POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Versão de: abril/2023

A presente Política de Segurança da Informação da EthQuo – Ethical Quotient Serviços de Compliance e Tecnologia Ltda. ("EthQuo") dispõe sobre:

- ✓ As diretrizes e práticas que nortearão o uso de ativos de informação da empresa, relativamente à sua confidencialidade, integridade e privacidade, abrangendo:
    - Geração, armazenamento, apresentação e utilização de informação, por colaboradores, clientes e terceiros, em ambientes digitais da EthQuo;
    - A proteção da informação em nossos sistemas e no tráfego externo, contra riscos e ameaças que possam causar danos ou interferir na continuidade do negócio.
- ✓ As obrigações que recaem sobre os sócios, prepostos, empregados e terceiros que atuem na EthQuo, relativamente à segurança da informação.

Não abrimos mão de um comportamento empresarial ético em todos os aspectos da nossa atuação profissional. Para maiores informações sobre nossos compromissos, políticas e diretrizes, consulte o nosso Código de Conduta em www.ethquo.com.

QUEM SOMOS

A EthQuo é uma empresa de tecnologia dedicada a apoiar as organizações no cumprimento de normas legais, regulamentos e políticas internas relativas à pesquisa e avaliação de informações sobre contrapartes de negócios (fornecedores, clientes, parceiros etc.) e terceiros em geral, que possam representar riscos de ordem patrimonial, reputacional, criminal ou regulatória para a empresa e seus administradores.

Essas normas legais, regulamentos e políticas internas formam o arcabouço de regras que norteiam as práticas diligência prévia (*due diligence*) de integridade de terceiros em geral, e são usualmente designadas por expressões como: levantamento de antecedentes de integridade, *background check*, Know Your Customer (KYC), Know Your Partner (KYP), dentre outras. Pela importância que alcançaram na proteção de valor das organizações, os processos de diligência de integridade de terceiros são considerados um dos mais significativos pilares das práticas de conformidade e, com efeito, têm sido fundamentais para a contínua evolução ética nos ambientes de negócio.

Os investimentos que fazemos em soluções para suportar os processos internos de *background check*, KYC e outras práticas de diligência de integridade de terceiros de nossos clientes são orientados pelo uso de tecnologia de ponta e técnicas robustas de segurança da informação,

com vistas a sustentar o cumprimento (*compliance*) de normas, regulamentos e políticas internas de governança de forma efetiva, apoiando as organizações em seu compromisso com a conformidade.

Como empresa de tecnologia do segmento de *compliance*, temos orgulho da contribuição que damos para as práticas que promovem a ética nos negócios, em busca de um mundo cada vez melhor. Se você, leitor, quiser saber um pouco mais sobre como nossas ferramentas suportam e dão efetividade às práticas de *compliance* de integridade de terceiros em nossos clientes, por favor nos procure através do e-mail contato@ethquo.com.

Fazemos referência à EthQuo através do uso de termos tais como "*site*", "nós", "nosso", "conosco". Palavras tais como "você", "seu" e expressões similares referem-se a nossos clientes, a usuários de nossa tecnologia atuando em nome de nossos clientes, a visitantes em nosso *site* ou a outros titulares de dados.

Os usuários de nossa tecnologia operam com base nas condições contratuais firmadas entre a EthQuo e nossos clientes e, por conseguinte, todos os usuários aderem às condições descritas a seguir, que compõem a nossa Política de Segurança da Informação. Por essas razões, se você for usuário dos produtos EthQuo, por favor, leia com atenção a presente Política de Segurança da Informação. Se houver quaisquer questões, procure-nos através do e-mail contato@ethquo.com.

DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

Definição de informação

Para os fins desta Política de Segurança da Informação, consideramos como "informação" toda base de conhecimento, conteúdo, mensagens trocadas, processo ou fato existente, em meio físico ou digital, que sejam de interesse ou que estejam de posse da EthQuo. Este conceito inclui quaisquer dados, materiais, procedimentos, especificações, inovações, atributos técnicos, modelos, projeções ou documentações de qualquer espécie que guardem conexão com o negócio da nossa empresa, bem como dados obtidos no curso normal da prestação de serviços a nossos clientes, mantidos sob nossa custódia por força contratual.

Gestão da informação

A informação gerada originariamente pelas atividades operacionais da EthQuo, ou derivada de clientes ou terceiros, é protegida contra acesso e compartilhamento não autorizados de qualquer espécie e não é utilizada para nenhuma finalidade de marketing ou de qualquer forma comercializada. Tal informação é empregada no estrito atendimento aos nossos clientes, nos termos dos serviços acordados nos respectivos contratos. Para mais informações sobre nossas diretrizes e práticas de proteção de dados, consulte a nossa Política de Privacidade de Dados, em www.ethquo.com.

As atividades que envolvam geração, utilização, armazenamento, manutenção, distribuição e deleção de informação em quaisquer ambientes operacionais da EthQuo, físicos ou digitais, devem manter coerência com nosso propósito empresarial, nossos valores e práticas descritas em nosso Código de Conduta, devendo ser sempre adequadamente documentadas.

A Administração da EthQuo se reserva no direito de inspecionar e analisar informações mantidas ou armazenadas em quaisquer de seus ambientes físicos, digitais e em equipamentos de uso operacional. O compartilhamento de informações físicas ou digitais em âmbito interno na EthQuo ou com interlocutores externos de quaisquer espécies deve ser feito com o uso de recursos seguros.

A informação interna da EthQuo (de natureza comercial, de cadastro, técnica ou administrativa) será armazenada digitalmente pelo tempo requerido pela legislação em vigor. A informação de natureza operacional, resultante da prestação dos nossos serviços a clientes, será armazenada pelo prazo de duração dos respectivos contratos, sendo excluída em curto período de tempo após o término da contratação, para minimizar eventuais riscos de violação de privacidade de nossos clientes, ou de terceiros que tenham sido objeto de pesquisas de diligência prévia ou outros processamentos com o uso de soluções EthQuo.

O armazenamento das informações – interna e operacional – observa recursos e técnicas apropriadas e tem proteção contra sinistros, acessos não autorizados e perda definitiva de dados causada por incidentes, incluindo *back-ups* de ambientes, aplicações e bases de dados, infraestruturas redundantes, dentre outras.

Acesso à informação

A EthQuo utiliza servidores de *firewalls*, servidores de acesso à internet, serviços *anti-spam*, ferramentas antivírus ou *malwares* para proteção e controle da informação e de sua rede de comunicação interna e externa.

Caso terceiros externos à EthQuo (por exemplo, prestadores de serviços, auditores e outros) venham a ter acesso aos nossos sistemas e/ou à informação nele armazenada, sua atuação deverá ser na menor extensão e prazo possíveis, observando apenas o necessário para atendimento a demandas operacionais da EthQuo, a alguma solicitação específica previamente acordada com nossos clientes ou à determinação formal de alguma autoridade, sempre com registro da trilha de utilização, com documentação adequada e com estrita observância das diretrizes previstas nesta Política de Segurança da Informação.

Aplicações sistêmicas e propriedade intelectual

As aplicações EthQuo compõem o acervo de propriedades intelectuais da empresa e, quando aplicável, são registradas no INPI. Reservamo-nos todos os direitos a respeito de qualquer tecnologia associada a nossos serviços e plataformas digitais.

Todos os ativos de informação originários da EthQuo constantes em nosso *site* ou distribuídos por quaisquer mídias (físicas ou digitais), incluindo demonstrações de funcionamento (“demos”)

da nossa tecnologia, conteúdos, opiniões, compilações de dados para apresentações, documentos sobre aspectos funcionais ou de *design* de nosso software, informações institucionais sobre nós e nossa forma de atuação profissional, dentre outros, são de propriedade da EthQuo, e são protegidos pela lei de direitos autorais e, quando aplicável, pelas normas de registro de propriedade intelectual. Quando fizermos menção a algum material ou conteúdo não originado na EthQuo, sempre indicaremos a respectiva fonte e buscaremos, quando necessário, autorização prévia do respectivo titular.

As atividades de desenvolvimento das aplicações da EthQuo são realizadas em ambientes específicos e separados dos ambientes de produção, seguindo boas práticas de documentação, sustentadas em artefatos e registros de códigos fonte e objetos em geral em repositório seguro, e que permitam que nossos sistemas sejam rapidamente recuperados, se necessário.

As aplicações não proprietárias somente serão instaladas em equipamentos da EthQuo e utilizadas por nossos sócios, prepostos, empregados ou terceiros contratados pela empresa mediante licença de uso firmada em nome da nossa empresa e com observância dos procedimentos de cópia (*download*) e das regras de utilização acordadas com a entidade proprietária do software.

Planejamento e controles

A Diretoria de Tecnologia da EthQuo, na pessoa de seu Chief Technology Officer (CTO), é responsável por estabelecer políticas de perfil de acesso e de uso dos sistemas proprietários da nossa empresa e de terceiros, compatíveis com os atributos funcionais e responsabilidades dos respectivos usuários. Os acessos e atividades realizados pelos usuários dos sistemas proprietários EthQuo e de terceiros serão monitorados e testados, para detecção e prevenção de fraudes ou danos acidentais aos sistemas e bases de dados.

É também responsabilidade da Diretoria de Tecnologia estabelecer um plano e executar atividades que garantam que o uso projetado dos sistemas e das infraestruturas digitais que os suportam é compatível com as demandas e outros requisitos de usuários internos, externos e clientes, considerando aspectos de disponibilidade, tráfego, performance, condições de acesso e usabilidade.

PRÁTICAS OPERACIONAIS

Regras gerais

1. A transmissão de informação a terceiros, bem como sua divulgação, reprodução, cópia, utilização ou exploração conceitual, somente é permitida se feita com a anuência dos Administradores da nossa empresa, de forma consistente com os propósitos da EthQuo, nos termos do nosso Código de Conduta, e desde que não infrinja quaisquer aspectos previstos na Lei Geral de Proteção de Dados e nos contratos firmados com contrapartes de negócio.

2. Caso algum sócio, preposto, empregado ou terceiro contratado pela EthQuo receba ou tenha contato com informação indevida, deverá comunicar imediatamente o ocorrido à Diretoria de Tecnologia e à Diretoria de Clientes e Mercados, para que as providências cabíveis sejam tomadas, sempre com a devida orientação jurídica. A comunicação a ambas as Diretorias deverá ser feita em quaisquer circunstâncias, ainda que a informação indevidamente recebida não seja relativa a clientes, prospecções, parceiros ou outro interlocutor de negócios da nossa empresa.

3. Os sócios, prepostos, empregados e terceiros contratados pela EthQuo, que tenham acesso a sistemas e informação mantidos por nossa empresa, serão instruídos quanto aos riscos previstos na presente Política de Segurança da Informação, relativos a acesso não autorizado, divulgação indevida, indisponibilidade e alterações impróprias, bem como quanto às consequências para a EthQuo e para os próprios indivíduos, nos âmbitos cíveis, criminais, patrimoniais, regulatórios, reputacionais e operacionais.

4. Todos os sócios, prepostos, empregados e terceiros contratados pela EthQuo, que tenham acesso a sistemas e informação mantidos por nossa empresa, deverão ter conhecimento de suas obrigações e responsabilidades para com a informação e sistemas da EthQuo, firmando Termo de Responsabilidade específico ou, quando for o caso, admitindo uma cláusula contratual com redação equivalente à do referido Termo de Responsabilidade. Toda ação havida que envolva ativos de informação da EthQuo, dentro ou fora de seus ambientes sistêmicos, terá como responsável o sócio, preposto, empregado ou terceiro contratado pela a EthQuo a quem se vinculem as credenciais de acesso associadas a tais ações.

5. Terceiros contratados que vierem a utilizar equipamentos próprios na prestação dos serviços só poderão acessar sistemas e informação mantidos pela EthQuo depois de analisados os riscos das respectivas atividades. Nesses casos, a Diretoria de Tecnologia deverá manter registro dos riscos identificados e medidas de segurança adotadas para eliminá-los ou minimizá-los.

6. Terceiros contratados que vierem a utilizar software que não seja proprietário da EthQuo deverão apresentar documentação comprobatória das respectivas licenças de uso ou firmar Termo de Responsabilidade garantindo que o uso da tecnologia em questão encontra-se devidamente autorizada, isentando a EthQuo de eventuais danos associados a um eventual uso com infração de quaisquer normas ou direitos dos respectivos titulares do software.

7. Todos os clientes, fornecedores, parceiros e demais interlocutores da EthQuo que venham a ter acesso a sistemas e informação da nossa empresa deverão ser informados da existência desta Política de Segurança da Informação e concordar em pautar o seu relacionamento com a EthQuo em conformidade com a sua redação.

8. Todos os indivíduos que vierem a ter acesso à informação e sistemas mantidos pela EthQuo deverão ser previamente identificados como usuários, de forma individualizada, com atribuição de um *login* específico e senha exclusiva, pessoal e intransferível. Essa identificação deverá constar em todas as trilhas de *logs* dos sistemas.

9. Não é permitido a nenhum usuário compartilhar dados de acesso (*login* e senha) aos sistemas da EthQuo com terceiros, mesmo que estes também sejam usuários cadastrados, em nenhuma circunstância. Em caso de emergências, a Diretoria de Tecnologia deverá ser contactada.

10. As senhas cadastradas terão duração máxima de 1 (um) ano e não poderão ser reutilizadas. Os arquivos de dados de senhas deverão ser criptografados e armazenados área específica do ambiente sistêmico da EthQuo, de acesso restrito aos perfis de Administradores do sistema.

11. O ambiente sistêmico da EthQuo deve contar com controles que permitam detectar tentativas de acesso não autorizado, com registros que identifiquem usuário, equipamento, data e hora, aplicações utilizadas, dados consumidos e atividades realizadas. Os controles em questão devem estar preparados para gerar relatórios detalhados.

12. Os ambientes sistêmicos de produção e de homologação/desenvolvimento devem ser segregados, de modo a impedir acessos indevidos e incidentes ou problemas que ameacem a disponibilidade, acesso ou tráfego regular dos sistemas e da informação.

13. Os arquivos, conteúdos e demais ativos de informação produzidos a partir da interação corporativa, institucional ou comercial com clientes, fornecedores, parceiros e outros *stakeholders*, bem como aqueles pertinentes à relação entre a EthQuo e seus sócios, prepostos, empregados e terceiros contratados, devem ser mantidos em nossos servidores, sendo vedada a manutenção em unidades de armazenamento de computadores ou em mídias de armazenamento de dados removíveis, exceto para fins tráfego transitório de dados (*downloads*) autorizado pela Diretoria de Tecnologia e apenas pelo tempo necessário para exportação para nossos servidores.

14. O armazenamento de informação em nossos sistemas deve estar suportado em técnicas de criptografia em unidades de disco e as transmissões de dados via internet devem observar as versões mais atuais de protocolos seguros para as respectivas conexões.

15. A Diretoria de Tecnologia fará a gestão dos recursos, ferramentas e meios necessários para assegurar o armazenamento seguro de informação, controle de acessos, proteção e criptografia. Sem embargo, não é responsabilidade da Diretoria de Tecnologia realizar *back-up* de informação armazenada de forma local em equipamentos ou segundo diretrizes e práticas que não se alinhem à presente Política.

16. A Diretoria de Tecnologia fará um inventário anual de sistemas proprietários e de terceiros e respectivas versões (software), bem como dos equipamentos próprios ou cedidos em uso para a EthQuo (hardware), de modo a manter controle sobre os acervos digital e físico que suportam as nossas operações, definindo ações para minimizar ou eliminar eventuais riscos identificados.

17. A Diretoria de Tecnologia manterá um portfólio recomendado de ferramentas e aplicativos de terceiros que atendam às demandas operacionais da EthQuo, incluindo ferramentas de produtividade, gestão de processos, auditoria de segurança da

informação e afins. Sempre que se mostrar mais adequado às demandas do negócio, tais ferramentas ou aplicativos deverão ser previamente instalados nos equipamentos próprios ou cedidos em uso para a EthQuo.

18. A Diretoria de Tecnologia manterá um plano que permita acessar recursos de processamento alternativos (*back-up*) e recuperação (*restore*), no caso de perda ou ameaça de violação de informação ou de sistemas, próprios ou de terceiros, de posse da EthQuo. O plano deverá considerar protocolos distintos de recuperação de informação, sistemas, ambientes e infraestrutura, de modo a garantir continuidade de operações cotidianas em caso de incidentes, de situações de catástrofe e por requerimentos legais, levando em conta:

    - A periodicidade e regularidade dos procedimentos de *back-up* e teste de integridade de dados;
    - O tempo de preservação dos dados e controle de versões, quando aplicável;
    - As características dos dados, dos respectivos titulares e criticidade de acesso;
    - A localização de servidores de *back-up*, capacidade, garantia de disponibilidade de infraestrutura e comunicação, segurança, dentre outros aspectos técnicos.

19. A Diretoria de Tecnologia programará testes anuais, para avaliação da efetividade do plano de *back-up* e recuperação de informação e sistemas.

20. Não é permitida:

    - A instalação ou utilização de nenhum software ou objeto de qualquer tipo em sistemas da EthQuo, que não tenha sido autorizada pela pessoa física ou jurídica proprietária, exceto nos casos de software de autoria da própria EthQuo. Esta regra aplica-se, inclusive, a softwares de código aberto, gratuito ou para fins de demonstração;
    - A utilização de ativos protegidos por direitos autorais, cuja cessão não tenha sido autorizada pelo respectivo titular;
    - A prática de quaisquer outros atos envolvendo informação e sistemas, no ambiente operacional da EthQuo, que possa insinuar infração a propriedades intelectuais de terceiros ou outra forma de pirataria.

21. As conexões de acesso remoto devem ser estabelecidas por meio de VPN (*Virtual Private Network*) corporativa ou desbloqueio de restrição por IPs, mediante regra de *firewall*.

22. Os equipamentos portáteis (*notebooks*, *tablets*, *smartphones* e outros) de uso operacional da EthQuo devem ser protegidos contra acessos não autorizados, especialmente no caso de furtos ou roubos.

23. Dispositivos de uso pessoal não são permitidos para uso operacional, com conexão às redes internas da EthQuo.

24. Os servidores de acesso à internet devem ser segregados, protegidos por *firewalls*.

25. O acesso a *websites* e outros ambientes digitais na internet, através de equipamentos de uso operacional da EthQuo, por parte dos sócios, prepostos, empregados e terceiros contratados pela empresa, deve se dar em consonância com as necessidades do negócio, com responsabilidade, ética e alinhamento aos valores da EthQuo.

26. A Diretoria de Tecnologia deve adotar procedimentos e tecnologias que permitam monitorar o uso e rastrear os acessos a endereços na internet, feitos através de equipamentos de uso operacional da EthQuo. Quando observadas características de navegação na internet não alinhadas com esta Política, os respectivos endereços digitais deverão ser imediatamente bloqueados.

27. Todos os arquivos mantidos ou baixados em equipamentos de uso operacional pela EthQuo devem ser submetidos a sistemas antivírus e outros *malwares* periodicamente atualizados.

28. Não é permitido acessar sistemas corporativos da EthQuo com dispositivos cujas aplicações ou configurações nativas de segurança tenham sido alteradas, salvo após prévia autorização por parte da Diretoria de Tecnologia, em caráter temporário e pelo tempo estritamente necessário.

29. O uso de tecnologia de correio eletrônico (e-mail) em comunicação interna ou externa, sempre que feita em nome da EthQuo ou com referência à nossa empresa, ainda que através de equipamentos que não sejam de uso operacional da EthQuo, por parte dos sócios, prepostos, empregados e terceiros contratados pela empresa, deve se dar em consonância com as necessidades do negócio, com responsabilidade, ética e alinhamento aos valores da EthQuo.

30. A Diretoria de Tecnologia deve adotar procedimentos e tecnologias que permitam monitorar o uso e o conteúdo transmitido através de e-mail, quando através de equipamentos de uso operacional da EthQuo. Quando observadas características de uso ou aspectos de conteúdo não alinhados com esta Política, os respectivos acessos deverão ser bloqueados.

31. Nos e-mails enviados por sócios, prepostos, empregados e terceiros contratados pela EthQuo que se comuniquem através de endereço de e-mail da empresa, deve-se adotar a seguinte mensagem:

> "Esta mensagem e seus anexos podem conter informações confidenciais, privilegiadas, de divulgação restrita ou com dados pessoais sensíveis, cujo sigilo é protegido por lei. Caso a mensagem tenha chegado ao seu conhecimento por engano ou erro do remetente, não utilize o conteúdo, anexos, informação ou contexto da mensagem recebida para nenhum fim; em o fazendo, você poderá estar incorrendo em uso indevido de informações privadas. Solicitamos, gentilmente, que apague a mensagem e avise imediatamente ao remetente. O conteúdo desta mensagem e seus anexos não representam necessariamente a opinião e a intenção da EthQuo, não implicando em qualquer obrigação ou responsabilidade imediata da nossa parte.

32. Quando um sócio, preposto, empregado ou terceiro contratado pela EthQuo deixar de desempenhar funções operacionais, técnicas ou executivas na empresa, o respectivo e-mail corporativo será descontinuado. Os e-mails e arquivos pessoais poderão ser exportados, com acompanhamento da Diretoria de Tecnologia. A conta de e-mail descontinuada terá os respectivos conteúdos redirecionados para um outro sócio, preposto ou empregado designado para esses fins, a quem caberá instruir a respeito do canal de comunicação que deverá ser utilizado pelos interlocutores, em substituição à conta de e-mail descontinuado, conforme o caso.

Plano de continuidade do negócio

A EthQuo mantém um plano de continuidade do negócio (*Business Continuity Plan* – BCP), contemplando a recuperação e restauração de processos críticos, com foco nos níveis de serviços a clientes, relacionamentos com autoridades e fluxo financeiro de pagamentos e recebimentos.

O BCP deverá ser acionado em situações de indisponibilidade do ambiente sistêmico e outros recursos chave que suportem a informação e as aplicações operacionais, proprietárias ou de terceiros, que dão sustentação ao negócio.

A Diretoria de Tecnologia é responsável pela concepção, implementação e testes do BCP aprovado. O plano será periodicamente revisado, no mínimo em bases anuais, com vistas a assegurar sua atualidade e efetividade, dando especial atenção a novos processos, interdependência entre sistemas, contratos, nível de serviço acordado com clientes em geral e fornecedores críticos, capacitação das equipes de operação, histórico de eventos e boas práticas divulgadas.

Reporte e resposta a Incidentes

A Diretoria de Tecnologia é responsável por elaborar, publicar e revisar o plano de resposta a incidentes de cibersegurança.

O plano deve detalhar as etapas de investigação, entendimento e resposta a serem cumpridas imediatamente após identificado ou reportado um incidente. O plano deve também incluir a caracterização do incidente, seus potenciais impactos e medidas remediativas em curso e outras a serem aplicadas, bem como um protocolo de comunicação com terceiros (clientes, fornecedores, titulares de dados, entidades, autoridades etc.) potencialmente afetados.

Os sócios, prepostos, empregados e terceiros contratados pela EthQuo são responsáveis por reportar prontamente à Diretoria de Tecnologia sobre qualquer evento, situação e fato ocorrido ou suspeito, que possa caracterizar incidente relacionado com segurança da informação ou violação das diretrizes e práticas previstas nesta Política.

Qualquer outra pessoa que tome conhecimento de evento, situação, fato ocorrido ou suspeito, que possa caracterizar incidente relacionado com segurança da informação ou violação das diretrizes e práticas previstas nesta Política, poderá reportá-lo através do e-mail contato@ethquo.com, sob a referência "Segurança da Informação".

Treinamento sobre Segurança da Informação e sobre esta Política

A Diretoria de Tecnologia será responsável aplicar treinamento sobre Segurança da Informação, incluindo o conteúdo desta Política, mantendo-o permanentemente atualizado. As sessões de capacitação deverão contemplar *workshops* para aferição de conhecimento, devendo ser ministradas a todos os sócios, prepostos, empregados e terceiros contratados pela EthQuo ao menos uma vez por ano.

O material de treinamento deve ser mantido atualizado e disponível para consulta dos sócios, prepostos, empregados e terceiros contratados pela EthQuo, a qualquer momento.

Novos sócios, prepostos, empregados ou terceiros, quando admitidos ou contratados por nossa empresa, deverão obrigatoriamente se dedicar a uma sessão de autoinstrução, tendo como base o material do treinamento.

OBRIGATORIEDADE E RESPONSABILIZAÇÃO

Todas as diretrizes e práticas previstas nesta Política de Segurança da Informação são de observância obrigatória por parte dos sócios, prepostos, empregados e terceiros contratados pela EthQuo.

As condutas previstas na presente Política ou esperadas em razão de suas diretrizes devem prevalecer para além do término das relações contratuais entre a EthQuo e seus sócios, prepostos, empregados e terceiros contratados pela empresa, devendo os respectivos instrumentos contratuais dispor sobre tal condição, quando não decorra diretamente de texto de lei, bem como prever penalidades aplicáveis em caso de descumprimento.

OUTRAS DISPOSIÇÕES

Mudanças neste Documento

Em caso de modificação dos termos constantes na presente Política de Segurança da Informação, publicaremos as respectivas alterações em nosso *site* e manteremos as versões anteriores arquivadas, para leitores interessados poderem compará-las.

Disposições complementares

Ao manter uma relação profissional, comercial ou institucional com a EthQuo, você deverá atuar com observância das diretrizes contidas nesta Política de Segurança da Informação.

Na eventualidade de alguma diretriz contida nesta Política de Segurança da Informação se tornar inválida, em virtude de conflito com alguma lei que venha a ser instituída ou outras razões, as demais disposições continuarão em pleno vigor e efeito.

A interpretação, conformidade e aplicação desta Política de Segurança da Informação serão regidas pelas leis federais do Brasil e todos os nossos serviços devem ser considerados como prestados no território brasileiro. Em caso de discussão judicial, deverá ser utilizado o foro da justiça da Cidade de São Paulo, Estado de São Paulo, prevalecendo sobre qualquer outro, independentemente do motivo.

Os títulos que adotamos nas seções desta Política de Segurança da Informação têm a finalidade de oferecer uma indicação conveniente dos conteúdos nelas contidos, mas o significado ou a interpretação de quaisquer de suas disposições não depende do título que adotamos, e sim dos textos transcritos nas respectivas seções.

Para devida publicidade, esta Política de Segurança da informação estará disponível digitalmente no *site* da EthQuo (endereço eletrônico www.ethquo.com).

A EthQuo protege a informação e os sistemas por ela mantidos.

Raise your company's ethical quotient

***

Atualizações:

Data	Causa da atualização	Resumo das alterações
22 de junho de 2022	Criação	Não aplicável.
29 de agosto de 2022	Atualização	Correções de erros ortográficos e gramaticais.
4 de abril de 2023	Correções	Correções em termos técnicos e ajustes visuais.