POLÍTICA DE SEGURANÇA, SIGILO DAS INFORMAÇÕES E SEGURANÇA CIBERNÉTICOS

Versão:
15/12/2025

EXANTE
ASSET MANAGEMENT

EXANTE
ASSET MANAGEMENT

SUMÁRIO

1. OBJETIVO

1.1. A presente Política de Segurança, Sigilo das Informações e Segurança Cibernética ("Política") tem por objetivo estabelecer diretrizes e padrões que assegurem a confidencialidade, integridade e disponibilidade das informações da Exante Asset Management Ltda. ("Exante Asset"). Visa padronizar procedimentos voltados à gestão de riscos cibernéticos, proteção de dados e prevenção de incidentes, promovendo a organização e o uso responsável das informações, bem como o aprimoramento contínuo da cultura de segurança dentro da instituição.

1.2. Complementarmente, a presente Política de Segurança, Sigilo das Informações e Segurança Cibernética observa os princípios do Código ANBIMA de Regulação e Melhores Práticas e as disposições das Resoluções Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021 ("Resolução CVM 21"), Resolução CVM nº 50, de 31 de agosto de 2021 ("Resolução CVM 50") e Resolução CVM nº 175, de 23 de dezembro de 2022 ("Resolução CVM 175"), que regem a atividade de gestão de recursos de terceiros. O documento reforça o compromisso da Exante Asset com a integridade do sistema financeiro, a transparência das operações e o cumprimento das normas aplicáveis ao mercado de capitais.

1.3. A Exante Asset tem como princípio basilar o exercício de suas atividades com boa-fé, transparência, diligência e lealdade, pautando-se na valorização e proteção de seus clientes e usuários. Em conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) e demais normativos aplicáveis, a Exante Asset desenvolveu esta Política de Privacidade com o objetivo de proteger os Dados Pessoais coletados, tratados e armazenados por meio de seus websites, domínios, canais digitais e demais meios de interação ("Canais"). A coleta de informações tem como finalidade aprimorar os serviços prestados, alinhando-os aos interesses e necessidades de cada Usuário, sempre sob os mais elevados padrões éticos e de governança.

1.4. Esta Política também define as responsabilidades da Administração na manutenção de um programa de segurança cibernética eficiente e atualizado, capaz de mitigar riscos decorrentes do aumento e sofisticação das ameaças digitais. O cumprimento de suas diretrizes visa proteger a empresa contra vazamentos de informações e fraudes, resguardar a privacidade de dados, garantir a disponibilidade de sistemas e assegurar a proteção da imagem e da marca Exante Asset. A gestão de riscos cibernéticos, alinhada aos objetivos corporativos, estabelece orientações aplicáveis a pessoas, processos e tecnologias, assegurando a integridade das informações da instituição, de seus colaboradores, clientes, fornecedores e parceiros de negócios.

1.5. A presente Política entrará em vigor em [XXX] de 2025 e vigorará por prazo indeterminado.

Exante Asset Management Ltda.
Ouvidora: +55 11 4550 6588
contato@exante.com.br

2. ABRANGÊNCIA

2.1 A Política de Segurança Cibernética em conjunto, com a legislação e regulamentação aplicável, disciplina a relação de todos os sócios, administradores, fornecedores, funcionários ou empregados da Exante Asset ("Colaboradores") entre si e com terceiros.

2.2 Posto isto, antes do início do exercício de suas funções perante à Exante Asset, os Colaboradores deverão receber uma cópia desta Política, bem como, firmar o Termo de Adesão abaixo, declarando se encontrar totalmente familiarizado a Política e os procedimentos aqui contidos, devendo estar sempre atento às situações que poderão ensejar condutas inadvertidas, por ele ou por qualquer outro Colaborador , isto é, condutas e/ou ações que pareçam ser uma violação direta ou indireta desta Política de Segurança Cibernética ou de qualquer lei ou regulamentação aplicável.

2.3 O Diretor de Compliance manterá em arquivo digital e físico, pelo prazo mínimo de 05 (cinco) anos, uma via do Termo de Adesão devidamente assinado por seus Colaboradores, bem como, disponibilizará uma cópia desta Política em sua sede e na rede mundial de computadores.

2.4 O descumprimento das regras estabelecidas nesta Política ou em normas e/ou regulamentações aplicáveis, será caracterizado como uma infração contratual e poderá resultar na imposição de penas de advertência, suspensão, desligamento ou exclusão por justa causa dos Colaboradores da Exante Asset.

2.5 A Exante Asset não assume a responsabilidade dos Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções de forma que, entretanto, caso a Exante Asset venha a ser responsabilizada ou sofra prejuízo de qualquer natureza por atos de seus Colaboradores, poderá exercer o direito de regresso em face dos responsáveis.

2.6 O Diretor de Compliance da Exante Asset é o responsável pela implementação dessa Política, incluindo uma revisão anual dos processos e procedimentos, manutenção e atualização da mesma.

2.7 Anualmente, todos devem reafirmar o cumprimento da presente Política. Em caso de eventuais dúvidas, o Colaborador deve contatar o Diretor de Compliance para receber treinamentos e/ou auxílio adequado.

3. DEFINIÇÕES E CONCEITOS

3.1. Usuário: Pessoa física ou jurídica que utiliza ou visita os Canais da Exante Asset, maior de 18 (dezoito) anos, ou emancipada e plenamente capaz, nos termos do Código Civil brasileiro.

Incluem-se, ainda, os absolutamente ou relativamente incapazes, desde que devidamente representados ou assistidos por seus responsáveis legais.

3.2. Dados Pessoais: Qualquer informação, fornecida ou coletada pela Exante Asset, que permita a identificação direta ou indireta de um Usuário, ainda que pública ou associada a outros dados já tratados. Incluem-se dados em formato físico ou digital, excluídas as informações meramente comerciais, como endereço, e-mail e número de telefone.

3.3. Finalidade: Propósito específico que motiva a coleta e o tratamento dos Dados Pessoais, devendo sempre ser legítimo, explícito e informado ao titular.

3.4. Necessidade: Princípio que fundamenta a coleta mínima de dados estritamente necessários para o atingimento da finalidade proposta, evitando o tratamento excessivo de informações.

3.5. Base Legal: Fundamentos jurídicos que legitimam a Exante Asset a realizar o tratamento de dados pessoais, conforme hipóteses previstas na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD).

3.6. Consentimento: Manifestação livre, informada e inequívoca pela qual o Usuário autoriza o tratamento de seus dados pessoais para finalidade específica previamente descrita.

3.7. Segurança da Informação: Conjunto de práticas e controles destinados a garantir a proteção de dados e informações da empresa, baseando-se nos pilares de Confidencialidade, Integridade, Disponibilidade, Autenticidade e Conformidade.

3.8. Confidencialidade: Princípio que assegura que as informações sejam acessadas apenas por pessoas autorizadas.

3.9. Integridade: Garante que as informações sejam exatas, completas e não alteradas indevidamente.

3.10. Disponibilidade: Assegura que os dados e sistemas estejam acessíveis a pessoas autorizadas sempre que necessário.

3.11. Autenticidade: Assegura que as informações sejam legítimas e originadas de fonte confiável.

3.12. Conformidade: Garante que os controles e políticas de segurança estejam em conformidade com as normas internas e externas aplicáveis.

3.13. Ativos: Todos os elementos de valor, tangíveis ou intangíveis, pertencentes, sob custódia ou responsabilidade da Exante Asset, incluindo dados, equipamentos, sistemas, processos, ambientes físicos e tecnológicos.

3.14. Ameaça: Qualquer evento, ação ou condição com potencial de comprometer a integridade, confidencialidade ou disponibilidade das informações e sistemas da empresa.

3.15. Ataque de Negação de Serviço (DoS/DDoS): Tentativa deliberada de tornar sistemas ou serviços indisponíveis por meio da sobrecarga de solicitações simultâneas.

3.16. Engenharia Social: Técnica de manipulação psicológica que visa induzir colaboradores ou usuários a revelar informações confidenciais, explorando falhas de comportamento humano.

3.17. Malware: Programa malicioso desenvolvido para causar danos, roubar informações ou comprometer sistemas, abrangendo vírus, trojans, worms e ransomwares.

3.18. Phishing: Fraude eletrônica que busca enganar o Usuário para obter informações confidenciais, geralmente por meio de e-mails, mensagens ou sites falsos.

3.19. Princípio do Privilégio Mínimo (POLP): Política que restringe o acesso de usuários, sistemas e aplicações apenas ao nível estritamente necessário para o desempenho de suas funções.

3.20. Need to Know: Princípio que determina que a informação seja acessível apenas àqueles que realmente necessitam conhecê-la para o desempenho de suas atividades.

3.21. Gestor: Colaborador com função de liderança, incluindo presidente, diretor, gerente, coordenador ou chefe de seção.

3.22. Boas Práticas de Segurança da Informação: Diretrizes reconhecidas internacionalmente, tais como ISO/IEC 27001, ISO/IEC 31000, NIST, OWASP, ISACA e SANS, utilizadas como referência para gestão de riscos e implementação de controles de segurança.

3.23. Ransomware: Tipo de malware que criptografa dados e exige pagamento de resgate para restabelecer o acesso.

3.24. Firewall: Sistema de segurança que monitora e controla o tráfego de rede, permitindo ou bloqueando comunicações de acordo com políticas de segurança predefinidas.

3.25. Gerenciamento de Riscos: Processo de identificação, análise, mitigação e monitoramento contínuo dos riscos que possam afetar a segurança da informação e os objetivos corporativos.

3.26. Trilha de Auditoria: Registro de todas as ações, eventos ou atividades realizadas em sistemas ou dados, destinado a assegurar rastreabilidade e transparência das operações.

3.27. Backup: Cópia de segurança de dados armazenada em ambiente distinto, visando à recuperação de informações em caso de incidente.

3.28. Wearables: Dispositivos eletrônicos vestíveis, como relógios, fones ou óculos inteligentes, que podem coletar e transmitir dados.

3.29. Zero-Day: Ataque que explora vulnerabilidades ainda não conhecidas ou corrigidas em softwares ou sistemas.

3.30. As diretrizes desta Política aplicam-se a todos os Usuários e potenciais Usuários dos serviços oferecidos pela Exante Asset Management Ltda., descrevendo de forma resumida e em conformidade com a legislação vigente, como a empresa poderá coletar, tratar, armazenar, compartilhar e eliminar dados pessoais obtidos por meio de seus canais de atendimento. Ao acessar ou utilizar tais canais, o Usuário declara ter mais de 18 (dezoito) anos, ser plenamente capaz e consentir expressamente com o tratamento de seus dados nos termos aqui previstos. Caso não atenda a esses requisitos ou não concorde com esta Política, o Usuário não deverá utilizar os serviços, websites ou quaisquer canais oficiais da Exante Asset.

4. COLETA E USO DE INFORMAÇÕES PESSOAIS

4.1. O Usuário dos websites, domínios, aplicativos, sistemas e demais canais digitais da Exante Asset declara estar ciente de que o fornecimento de informações ocorre de forma voluntária e consciente, sempre que realiza ações como o preenchimento de formulários, envio de currículos, contatos ou inserção de dados em campos disponibilizados pela empresa. Os Dados Pessoais informados serão utilizados exclusivamente para a finalidade específica que motivou o respectivo cadastro, em estrita conformidade com esta Política de Privacidade e com a legislação de proteção de dados aplicável.

Dados Pessoais	Finalidade	Base Legal	Consentimento
Nome, E-mail e Empresa	Para poder acessar conteúdo e receber material promocional, a Exante Asset precisará que o Usuário forneça seu Nome, E-mail e em qual Empresa trabalha. Os Dados Pessoais coletados	Consentimento	Estou de acordo e ciente em fornecer o meu Nome, E-mail e em qual Empresa eu Trabalho para acessar o material disponibilizado nos Canais, além de receber a Newsletter

	não serão utilizados para envio de qualquer tipo de SPAM.		Exante Asset. Estou ciente que meus dados serão utilizados internamente para fins promocionais pela Exante Asset e concordo em receber os e-mails da Exante Asset.
Nome, E-mail e Telefone	Caso o Usuário queira entrar em contato com a Exante Asset por meio da área "Fale Conosco" disponível no site, a Exante Asset precisará coletar Nome, E-mail e Telefone do Usuário para poder contatar o Usuário	Consentimento	Estou de acordo em fornecer meu Nome, E-mail e meu telefone para que a Exante Asset entre em contato comigo, bem como ciente de que esses dados poderão ser utilizados pela área Comercial da Exante Asset para o envio de e-mails
Nome, E-mail e Currículo	Para poder se candidatar a alguma das vagas anunciadas pela Exante Asset, o Usuário precisará fornecer para cadastro seu Nome e E-mail, e submeter o seu currículo para análise. OS dados serão utilizados para realização do processo seletivo	Legítimo interesse e Consentimento	Estou de acordo em fornecer meu Nome, E-mail e Demais informações contidas no meu currículo para a área de RH da Exante Asset, para me candidatar uma ou mais vagas disponíveis na Exante Asset e que eventualmente poderão ser utilizados em um processo seletivo e em um Contrato de Trabalho
Dado pessoal sobre origem racial ou étnica; convicção religiosa; opinião política; filiação sindical; dados referentes à saúde, dado genético ou biomédico	Caso algum Usuário submeta algum dado considerado como sensível nos termos do artigo 5º da LGPD, os dados serão coletados e eventualmente utilizados	Consentimento	Estou de Acordo com o tratamento dos dados pessoais sensíveis livremente fornecidos para a Exante Asset.

5. PRINCÍPIO DA SEGURANÇA DA INFORMAÇÃO

5.1. Considera-se que os ativos de informação são os bens mais importantes no mercado financeiro, portanto, tratá-los com responsabilidade é o compromisso da Exante Asset. Dessa forma, a operação está fundamentada nos princípios de segurança da informação, cujo objetivos constituem a preservação da propriedade da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e compartilhamento de forma controlada, bem como o monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

Confidencialidade: garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

Integridade: garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;

Disponibilidade: garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

6. COMPARTILHAMENTO E DIVULGAÇÃO DE DADOS PESSOAIS

6.1. A Exante Asset não compartilha Dados Pessoais coletados em seus Canais sem o consentimento expresso do Usuário, exceto nas hipóteses previstas em lei. O compartilhamento poderá ocorrer exclusivamente quando necessário para a prestação dos serviços, para o cumprimento de obrigação legal, normativa ou judicial, ou quando indispensável à execução de contratos. Dados também poderão ser divulgados, na medida estritamente necessária, a órgãos governamentais, autoridades públicas, consultores ou terceiros autorizados, sempre com base legal adequada. Quando houver divulgação decorrente de obrigação legal ou judicial, a Exante Asset comunicará os Usuários afetados, salvo se houver vedação legal ou determinação judicial impedindo tal aviso.

7. RETENÇÃO, ARMAZENAMENTO E EXCLUSÃO DE DADOS

7.1. Os Dados Pessoais serão armazenados pela Exante Asset enquanto o cadastro do Usuário estiver ativo e/ou enquanto necessários à execução dos serviços, podendo abranger também Dados Sensíveis, quando aplicável. Após o término da relação ou mediante solicitação de exclusão, os dados serão eliminados, observados os prazos previstos na tabela de retenção mencionada no item 2 da Política. Em situações excepcionais, a Exante Asset poderá manter determinados dados mesmo após o pedido de exclusão, quando necessário para cumprir obrigações legais ou judiciais, prevenir fraudes, garantir segurança, resolver disputas ou exercer direitos, respeitando sempre os princípios da necessidade e da minimização.

8. BASES LEGAIS E DIREITOS DO USUÁRIO

8.1. A Exante Asset realiza o tratamento de Dados Pessoais apenas quando respaldada por base legal válida, incluindo consentimento, execução de contrato, cumprimento de obrigação legal ou regulatória, legítimo interesse e demais hipóteses previstas na LGPD. O Usuário poderá, a qualquer momento, negar ou revogar o consentimento concedido; contudo, caso esta seja a única base legal para o tratamento, a revogação poderá impedir a continuidade de determinados serviços. A Exante Asset garante ao Usuário o pleno exercício dos direitos previstos em lei, incluindo acesso, correção, exclusão, portabilidade, limitação do uso, ou oposição ao tratamento, mediante solicitação formal.

9. CLASSIFICAÇÃO DAS INFORMAÇÕES E DEVER DE SIGILO

9.1. Os Colaboradores da Exante Asset, em razão de suas funções, podem ter acesso a informações sigilosas, devendo analisá-las previamente para verificar sua natureza, impacto de eventual divulgação (“disclosure”), necessidade de compartilhamento ou restrição total de

acesso. Após essa análise, as informações deverão ser classificadas como Confidenciais, Públicas ou Difundidas. Consideram-se Informações Confidenciais todos os dados e documentos sensíveis relacionados à Exante Asset, seus Colaboradores, Clientes, Investidores, atividades de gestão, estratégias, operações, posições, contrapartes, fornecedores e demais informações não públicas. Em caso de dúvida, prevalece a regra de que a informação deve ser tratada como Confidencial.

9.2. Toda informação recebida ou produzida deve ser previamente analisada quanto à sua natureza, impacto de eventual divulgação e necessidade de compartilhamento, sendo obrigatoriamente classificada como Confidencial, Pública ou Difundida.

9.3. Consideram-se Informações Confidenciais todos os dados sensíveis de Colaboradores, Clientes e Investidores, bem como informações estratégicas, operacionais, financeiras, técnicas ou não públicas relativas às atividades da Exante Asset. Na dúvida, prevalece a presunção de confidencialidade. O sigilo deve ser mantido pelos Colaboradores durante a vigência do vínculo e após seu desligamento, sendo autorizado o acesso ou compartilhamento apenas por necessidade operacional, determinação legal/regulatória ou aprovação do Diretor de Compliance. Informações que permitam identificar Clientes devem permanecer em ambiente de acesso restrito.

9.4. São classificadas como Informações Públicas aquelas divulgadas legitimamente ou cuja divulgação seja exigida por determinação legal, judicial ou administrativa, ou previamente autorizada pelo Diretor de Compliance. Informações Difundidas são aquelas compartilhadas internamente entre Colaboradores exclusivamente para fins de execução de suas atividades, sempre em conformidade com esta Política.

9.5. As Informações Relevantes correspondem a dados capazes de influenciar a decisão de investimento ou a cotação de valores mobiliários de uma sociedade. Já as Informações Privilegiadas são informações relevantes ainda não disponibilizadas ao mercado ou divulgadas de forma incompleta. O uso indevido dessas informações configura infração regulatória (insider trading), sujeita a penalidades civis, administrativas e criminais, sendo obrigatória a comunicação imediata ao Diretor de Compliance em caso de suspeita de acesso a tais informações.

9.6. A obrigação de sigilo permanece mesmo após o desligamento do Colaborador, e todas as informações capazes de identificar Clientes devem permanecer em ambiente de acesso restrito. Informações Públicas são aquelas já disponíveis ao mercado, exigidas por determinação legal ou cuja divulgação tenha sido autorizada pelo Diretor de Compliance. Já as Informações Difundidas são aquelas compartilhadas internamente entre Colaboradores com necessidade legítima de acesso e conforme esta Política e o Manual de Compliance.

Exante Asset Management Ltda.
Ouvidora: +55 11 4550 6588
contato@exante.com.br

10. INFORMAÇÕES RELEVANTES, PRIVILEGIADAS E PREVENÇÃO AO INSIDER TRADING

10.1. O Colaborador obriga-se a manter, durante a vigência de sua relação com a Exante Asset por prazo indeterminado após seu desligamento, absoluto sigilo sobre todas as Informações Confidenciais às quais tenha tido acesso, comprometendo-se a não utilizar, praticar, divulgar ou permitir o uso de tais informações, incluindo condutas caracterizadas como Insider Trading, Dicas ou Front Running, seja em benefício próprio, da Gestora ou de terceiros.

10.2. Consideram-se Informações Relevantes aquelas capazes de influenciar decisões de investimento ou a cotação de valores mobiliários de determinada sociedade. Já as Informações Privilegiadas correspondem a dados relevantes não divulgados ao mercado ou divulgados de forma parcial, tais como resultados financeiros, operações de M&A, alterações de controle e demais exemplos previstos na regulamentação aplicável, incluindo, mas não se limitando a Resolução CVM nº 44, de 23 de agosto de 2021 e normas subsequentes. O uso dessas informações para operações próprias ou de terceiros configura insider trading, prática expressamente vedada, sujeita a sanções civis, administrativas e criminais.

10.3. Sempre que houver suspeita de posse de Informação Confidencial, Relevante ou Privilegiada, o Colaborador deverá notificar imediatamente o Diretor de Compliance e abster-se de qualquer negociação ou divulgação. Compete ao Diretor de Compliance classificar ativos na lista de valores mobiliários restritos, atualizando-a conforme a informação se torne pública, deixe de ser relevante ou o evento potencial perca validade. Todas as reuniões com agentes de mercado devem ser registradas na agenda corporativa. Nomeações de Colaboradores para conselhos de administração ou diretorias de sociedades devem ser comunicadas de imediato ao Diretor de Compliance e ao Comitê, sendo o ativo da respectiva sociedade incluído na lista de ativos restritos, quando aplicável.

11. PROCEDIMENTOS INTERNOS, CONTROLES E RESPONSABILIDADES

11.1. Os Colaboradores devem manter absoluto sigilo sobre informações da Exante Asset, de seus investimentos, Clientes e operações, salvo quando a divulgação for expressamente autorizada pelo Diretor de Compliance, classificada como pública ou exigida por lei. Informações confidenciais devem ser copiadas ou impressas apenas para atender aos interesses da Exante Asset ou do próprio Cliente. Mesmo após o encerramento da relação contratual, como em caso de resgate integral, a Exante Asset continuará observando integralmente esta Política quanto às informações classificadas como Confidenciais.

11.2. Os Colaboradores devem comunicar imediatamente o Diretor de Compliance e o Comitê sobre qualquer restrição de negociação recebida de sociedades emissoras, mantendo os ativos restritos até a reabertura da janela de negociação. O cumprimento dessas diretrizes

protege a integridade das informações, preserva a segurança dos Clientes, reforça o compromisso regulatório e assegura a atuação ética e responsável da Exante Asset no mercado de capitais.

12. INFORMAÇÕES CONFIDENCIAIS

12.1. O acesso às informações confidenciais, incluindo dados pessoais, coletadas e armazenadas pela Exante Asset é restrito aos profissionais autorizados ao uso direto dessas informações, e necessário à prestação de seus serviços, sendo limitado o uso para outras tarefas, devendo respeitar, ainda, o disposto na Norma de Classificação da Informação contida na Política de Segurança da Informação da Exante Asset.

12.2. A Exante Asset poderá revelar as informações confidenciais nas seguintes hipóteses:

12.2.1. Sempre que estiver obrigado a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial;

12.2.2. Aos órgãos de proteção e defesa de crédito e prestadores de serviços autorizados pela Exante Asset a defender seus direitos e créditos;

12.2.3. Aos órgãos reguladores do mercado financeiro; e

12.2.4. Para instituições financeiras, desde que dentro dos parâmetros legais estabelecidos para tanto, podendo, nesta hipótese, o usuário, a qualquer tempo, cancelar sua autorização.

13. SEGURANÇA DAS INFORMAÇÕES

13.1. A Exante Asset adota controles físicos e tecnológicos rigorosos para proteger seus Colaboradores e garantir a segurança, confidencialidade e integridade das informações. O acesso às instalações é restrito e monitorado, sendo permitido apenas a Colaboradores autorizados e prestadores devidamente acompanhados. Áreas destinadas ao tratamento de informações sensíveis, bem como reuniões confidenciais, possuem acesso físico limitado e devem ser utilizadas em detrimento das salas individuais dos Colaboradores.

13.2. O departamento de tecnologia realiza testes periódicos de segurança, monitora vulnerabilidades e promove treinamentos regulares sobre uso adequado da infraestrutura tecnológica. O acesso à rede e aos sistemas ocorre mediante credenciais individuais, com níveis diferenciados de permissão conforme as funções desempenhadas. É obrigatório o uso de senhas fortes, a proteção de dispositivos corporativos e pessoais utilizados para fins profissionais, e a

proibição expressa de compartilhamento de senhas. Computadores e dispositivos devem ser bloqueados sempre que o Colaborador se ausentar e as senhas devem ser atualizadas periodicamente.

13.3. Incidentes envolvendo comprometimento de credenciais, perda ou roubo de dispositivos devem ser comunicados imediatamente ao Diretor de Compliance, que adotará as medidas necessárias, incluindo a desativação remota dos equipamentos. Dispositivos pessoais utilizados no ambiente corporativo devem cumprir integralmente a Política de Segurança da Informação e a Política de Segurança Cibernética da Exante Asset.

13.4. O uso de dispositivos pessoais para acesso a sistemas e informações corporativas somente será permitido mediante autorização prévia, registro formal e homologação técnica pela Equipe de Segurança. No regime de trabalho remoto, é obrigatório o uso de VPN e o cumprimento integral da Política de Regime Híbrido de Trabalho (Home Office). Os programas e configurações instalados em dispositivos pessoais deverão seguir os mesmos padrões da Exante Asset, contemplando, no mínimo: (i) risk assessment; (ii) ações de prevenção e proteção; (iii) monitoramento e testes; (iv) criação de backup; e (v) atualizações e manutenção preventiva e corretiva de segurança cibernética, garantindo que tais dispositivos sejam seguros, confiáveis e isentos de riscos, vírus ou malwares.

13.5. Armazenamento em Nuvem e Manuseio de Documentos: Colaboradores podem acessar serviços de armazenamento em nuvem a partir de computadores corporativos, observadas as seguintes condições:

i. É vedada a cópia de arquivos restritos da Exante Asset sem prévio e expresso consentimento do Diretor de Compliance;

ii. É permitida a cópia de documentos classificados como públicos; e

iii. Todas as anotações e materiais de trabalho devem ser transferidos, tão logo possível, para os servidores da Exante Asset.

13.6. Instalação de Softwares e Administração de Sistemas: A instalação de qualquer software em computadores corporativos depende de aprovação prévia da Diretoria de Compliance. Toda e qualquer alteração em documentos, manutenções de hardware, controles de validade e destruição de informações devem seguir os mecanismos oficiais de conformidade.

13.7. Monitoramento, Logs e Segurança Operacional: A Exante Asset manterá mecanismos de rastreabilidade integral das ações dos usuários (logs de auditoria), bem como processos para garantir estabilidade operacional, atualizações constantes, correção de falhas, testes periódicos

de vulnerabilidade e disponibilidade, além da manutenção e testes contínuos dos Programas de Segurança da Informação, Segurança Cibernética, Continuidade de Negócios, Contingência, Recuperação de Desastres e Resposta a Incidentes.

13.8. Supervisão da Alta Administração: O Diretor de Compliance monitora regularmente todas as comunicações eletrônicas e confirma seu adequado armazenamento. A Exante Asset poderá monitorar toda e qualquer troca interna ou externa de e-mails, bem como acessos a sites e arquivos eletrônicos, reportando à alta administração avaliações de efetividade e vulnerabilidades para adoção tempestiva das medidas cabíveis.

13.9. A Exante Asset não proíbe que Colaboradores utilizem fóruns públicos, blogs ou redes sociais (como Facebook ou LinkedIn) em âmbito pessoal e fora do horário de trabalho. Contudo, a fim de mitigar riscos regulatórios, reputacionais e de divulgação indevida de informações, ficam estabelecidas as seguintes restrições, sem necessidade de prévia aprovação, exceto quando expressamente indicado:

i. É proibido qualquer contato, comunicação, resposta ou interação com Clientes ou Investidores, atuais ou potenciais, por meio de blogs, redes sociais ou plataformas equivalentes;

ii. Colaboradores devem remover imediatamente quaisquer endossos, depoimentos ou recomendações publicadas por Clientes ou Investidores em seus perfis pessoais;

iii. O Colaborador não poderá indicar vínculo profissional com a Exante Asset em qualquer fórum público quando houver risco de que outras informações disponíveis no mesmo ambiente possam prejudicar a reputação da instituição;

iv. É vedado publicar informações sobre a Exante Asset, seus negócios, operações, processos internos, produtos ou quaisquer Informações Confidenciais, Relevantes ou Não Públicas, sem a prévia e expressa aprovação do Diretor de Compliance, considerando que tais publicações podem ser caracterizadas como material publicitário em determinadas jurisdições;

v. É estritamente proibido identificar Clientes ou Investidores, bem como divulgar qualquer informação Não Pública ou Confidencial a eles relacionada, em fóruns públicos ou redes sociais;

vi. É proibida a ativação de recursos que permitam a redes sociais acessar contatos ou informações armazenadas nos sistemas corporativos da Exante Asset;

vii. Para fins desta política, considera-se "fórum público" qualquer ambiente no qual informações possam ser acessadas pelo público em geral ou por grupos restritos (ex.: amigos, grupos fechados, seguidores, assinantes, comunidades);

viii. As restrições acima também se aplicam a manifestações públicas em quaisquer meios de comunicação, tais como rádio, televisão, jornais, revistas, podcasts e veículos similares, quando não houver prévia aprovação do Diretor de Compliance.

13.10. A Exante Asset se reserva o direito de gravar, monitorar e escutar qualquer ligação realizada ou recebida por Colaboradores por meio das linhas telefônicas corporativas disponibilizadas para o exercício profissional, incluindo, mas não se limitando, às ligações da equipe de Controle e da Mesa de Operações. Tal monitoramento ocorre para fins regulatórios, de supervisão, auditoria e prevenção de riscos operacionais e reputacionais.

14. AVALIAÇÃO DE RISCOS, PROTEÇÃO E PREVENÇÃO

14.1. A Exante Asset adota medidas de avaliação de riscos, proteção e prevenção, regularmente revisadas de acordo com a legislação vigente, assegurando que:

14.1.1. Classificação e Proteção das Informações: Todas as informações são classificadas quanto ao nível de sigilo, valor, requisitos legais, sensibilidade e necessidade do negócio (Restrita, Confidencial, Interna ou Pública), garantindo confidencialidade, integridade, disponibilidade, autenticidade e conformidade, conforme o manual de classificação de informações. Cada nível de informação possui controles e níveis de serviço específicos, que são monitorados e avaliados continuamente.

14.1.2. Gestão de Riscos e Incidentes: Riscos e incidentes de segurança são reportados à Diretoria, considerando impactos financeiros, operacionais e reputacionais. Avaliações de risco incluem também atividades de prestadores de serviços terceirizados.

14.1.3. Uso e Propriedade de Informações e Sistemas: Informações, metodologias, tecnologias e documentos produzidos pelos Colaboradores em função de suas atividades são propriedade exclusiva da Exante Asset. Equipamentos, sistemas e informações devem ser utilizados prioritariamente para atividades profissionais, sendo permitido uso pessoal apenas quando não comprometer a política. Informações de clientes, colaboradores e produtos devem ser tratadas de forma ética e sigilosa, evitando uso, exposição ou transmissão indevida.

14.1.4. Conformidade e Segurança Cibernética: Procedimentos de backup, continuidade de negócios e recuperação de desastres são implementados e testados periodicamente.

Todos os processos respeitam a LGPD e regulamentações aplicáveis, garantindo proteção de dados pessoais e corporativos. Riscos, vulnerabilidades e incidentes são monitorados, registrados e comunicados à alta administração para tomada de ações corretivas tempestivas.

14.2. A Exante Asset assegura que o acesso às informações seja restrito apenas a pessoas autorizadas, com níveis hierárquicos definidos e concedido estritamente quando necessário ao exercício das atividades ou à tomada de decisão.

14.3. É vedado o uso de equipamentos pessoais para acessar sistemas ou informações corporativas sem prévia homologação, exceto em contingências autorizadas, sendo que tais dispositivos devem ser registrados, homologados e monitorados pela equipe de segurança, e seu uso registrado como incidente. Todas as ordens, negociações, aprovações e comunicações relacionadas a negócios devem ocorrer exclusivamente por canais corporativos autorizados.

14.4. Equipamentos cedidos pela Exante Asset devem ser controlados conforme esta Política, garantindo segurança em qualquer local de uso. Cópias de segurança de documentos, arquivos eletrônicos e caixas de mensagens corporativas devem ser mantidas em locais externos para recuperação em caso de contingência ou desastre, e os processos de gestão documental devem obedecer ao ciclo de vida da informação, incluindo níveis de acesso e serviço compatíveis. Documentos devem ser armazenados de forma segura quando não utilizados ou durante ausências prolongadas (Clean Desk). Senhas e logins devem ser individualizados, sendo vedado o compartilhamento ou uso coletivo, e mecanismos de autenticação devem assegurar a identidade do usuário antes da liberação de acesso, podendo incluir biometria, tags ou certificação eletrônica.

14.5. O tratamento de dados pessoais segue integralmente os princípios da LGPD, garantindo finalidade, adequação, necessidade, transparência, segurança e responsabilização, vedando uso discriminatório ou ilícito. Informações devem ser armazenadas apenas pelo período necessário para atender finalidades legais, regulamentares ou contratuais, sendo eliminadas de forma segura após o término desse prazo, em meios físicos ou eletrônicos.

15. VAZAMENTO DE INFORMAÇÕES CONFIDENCIAIS, RESERVADAS OU PRIVILEGIADAS

15.1. Em caso de suspeita ou ocorrência de vazamento de informações confidenciais, reservadas ou privilegiadas, inclusive oriundos de ações involuntárias, o Colaborador deve registrar e comunicar imediatamente o fato à área de Risco e Compliance. Esta, em conjunto com as áreas de suporte, adotará as seguintes providências:

i. comunicar imediatamente à Diretoria da Gestora;

Exante Asset Management Ltda.
Ouvidora: +55 11 4550 6588
contato@exante.com.br

ii. bloquear senhas, acessos, servidores ou quaisquer recursos necessários para evitar novos vazamentos;

iii. avaliar a amplitude do vazamento e identificar potenciais riscos e impactos;

iv. elaborar plano de recuperação do evento; e

v. reavaliar e ajustar as medidas de segurança vigentes para prevenir recorrências.

Exante Asset Management Ltda.
Ouvidora: +55 11 4550 6588
contato@exante.com.br

16. POLÍTICA DE SEGURANÇA CIBERNÉTICA

16.1. Os principais ataques cibernéticos que podem impactar a Exante Asset incluem:

16.1.1. Malware: softwares maliciosos projetados para corromper computadores, redes e dados:

i. Vírus: danifica sistemas, softwares e bancos de dados;

ii. Cavalo de Troia (Trojan): disfarçado em outro software, cria portas para invasão;

iii. Spyware: coleta e monitora informações do usuário;

iv. Ransomware: bloqueia sistemas ou criptografa dados, exigindo resgate.

16.1.2. Engenharia Social: manipulação para obter informações confidenciais, senhas ou dados financeiros:

i. Pharming: redireciona usuários para sites fraudulentos;

ii. Phishing: envio de e-mails falsos simulando remetentes confiáveis;

iii. Vishing: ligações telefônicas fraudulentas;

iv. Smishing: mensagens de texto fraudulentas;

v. Acesso pessoal: captação de informações em locais públicos.

16.1.3. Ataques de negação de serviço (DoS/DDoS) – sobrecarga de sistemas para torná-los indisponíveis.

16.1.4. Invasões (APT – Advanced Persistent Threats) – ataques sofisticados visando vulnerabilidades específicas.

16.2. Conceitos de Segurança da Informação

i. Ameaça: potencial causador de incidente indesejado com impacto nos objetivos do negócio.

ii. Ativo: qualquer recurso de valor para a empresa, tangível ou intangível, incluindo dados, sistemas, equipamentos e processos.

iii. Blackdoor (Backdoor): vulnerabilidade que permite acesso remoto não autorizado, geralmente via Trojan.

iv. Backup: cópia de segurança de dados para recuperação em contingência.

v. Confidencialidade: garantia de acesso apenas a pessoas autorizadas.

vi. Integridade: garantia de que informações não sejam modificadas indevidamente.

vii. Disponibilidade: garantia de acesso às informações e sistemas conforme necessidade e autorização.

viii. Conformidade: garantia de que controles estão funcionando de acordo com objetivos estabelecidos.

ix. Controle: recurso ou medida para mitigação, eliminação ou transferência de riscos.

x. Cryptojacking: malware que usa recursos de dispositivos para mineração de criptomoedas.

xi. Decoy: software falso que coleta informações do usuário.

xii. DMA (Direct Memory Access): ataque que acessa diretamente a memória RAM.

xiii. DNS: sistema que mapeia nomes de domínio a endereços IP.

xiv. Eavesdropping: interceptação e roubo de dados.

xv. Firewall: sistema que controla o tráfego de rede e bloqueia acessos não autorizados.

xvi. Gerenciamento de Risco (Risk Management): identificação, avaliação e resposta a riscos.

xvii. Gerenciamento de Superfície de Ataque (ASM): análise e monitoramento contínuo das vulnerabilidades e vetores de ataque.

xviii. Hardening: medidas para reduzir a superfície de ataque, eliminando funções e portas desnecessárias.

xix. Instant Messaging (IM): aplicativos de mensagens em tempo real.

xx. IP (Internet Protocol): endereço que identifica dispositivos na rede.

xxi. Logs: registros de eventos e atividades do sistema.

xxii. Man-in-the-Middle (MitM): interceptação de comunicação entre usuário e servidor.

xxiii. Nuvem (Cloud): serviços, aplicações ou infraestrutura acessíveis via internet, podendo ser pública, privada ou híbrida.

xxiv. Phishing / Spoofing / Smishing / Vishing: técnicas de fraude e manipulação de informações.

xxv. Principles “Least Privilege” e “Need to Know”: acesso restrito apenas ao necessário para o desempenho da função.

xxvi. Ransomware: bloqueio de sistemas ou criptografia de dados mediante resgate.

xxvii. Spam: comunicação não solicitada enviada em massa.

xxviii. Trojan / Worms / ZeroDay: softwares maliciosos que exploram vulnerabilidades conhecidas ou recém-descobertas.

xxix. Wearables: dispositivos vestíveis conectados a sistemas corporativos.

xxx. Trilha de Auditoria: registro completo das ações realizadas pelos usuários em sistemas.

17. SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA

17.1. A Exante Asset adota práticas e controles de segurança da informação alinhados às normas internacionais ISO/IEC 27001, ISO/IEC 31000, OWASP, NIST, ISACA e SANS, bem como às melhores práticas de mercado, garantindo a proteção de informações, ativos e sistemas corporativos, conforme exigido pela legislação vigente e pelas diretrizes regulatórias.

17.2. <u>Avaliação de Riscos e Proteção de Informações</u>

17.2.1. Todas as informações da Exante Asset são classificadas quanto ao nível de sigilo, valor, requisitos legais, sensibilidade e necessidade do negócio (Restrita, Confidencial, Interna ou Pública), com o objetivo de assegurar confidencialidade, integridade, disponibilidade, autenticidade e conformidade. Cada nível de informação requer controles específicos, monitoramento contínuo e avaliação periódica quanto à efetividade das medidas aplicadas.

17.2.2. Riscos e incidentes de segurança devem ser reportados à Diretoria, considerando seus impactos financeiros, operacionais e reputacionais. Informações, metodologias, tecnologias e documentos produzidos pelos colaboradores no exercício de suas funções são de propriedade exclusiva da Exante Asset. Equipamentos, sistemas e informações devem ser utilizados prioritariamente para atividades profissionais, sendo permitido o uso pessoal desde que não viole esta Política. Avaliações de risco incluem também atividades desenvolvidas por prestadores de serviços terceirizados.

17.3. Proteção e Prevenção

17.3.1. O acesso às informações é restrito a pessoas autorizadas, seguindo hierarquias de acesso e os princípios de Least Privilege e Need to Know, sendo concedido apenas quando necessário para o exercício das atividades ou tomada de decisões.

17.3.2. É vedado o uso de equipamentos pessoais para acessar sistemas ou informações corporativas sem homologação prévia, exceto em situações de contingência autorizadas. Equipamentos e dispositivos pessoais devem ser registrados, homologados e monitorados pela equipe de segurança, sendo que toda utilização deve ser registrada como incidente.

17.3.3. Ordens, negociações, aprovações e comunicações relacionadas a negócios devem ser realizadas exclusivamente pelos canais corporativos autorizados. Equipamentos fornecidos pela Exante Asset devem ser controlados de acordo com esta Política, garantindo a segurança das informações independentemente do local de uso.

17.3.4. A Exante Asset mantém cópias de segurança de documentos, arquivos eletrônicos e caixas de mensagens corporativas em locais externos, assegurando a recuperação em caso de contingência ou desastre. Processos de gestão documental seguem o ciclo de vida da informação, com níveis de acesso e serviços compatíveis, e todos os documentos devem ser armazenados de forma segura quando não estiverem em uso ou durante ausências prolongadas (Clean Desk).

Exante Asset Management Ltda.
Ouvidora: +55 11 4550 6588
contato@exante.com.br

17.3.5. Senhas e logins são individualizados, sendo vedado compartilhamento ou uso coletivo. Mecanismos de autenticação asseguram a identidade do usuário antes da liberação de acesso, podendo incluir biometria, tags ou certificação eletrônica. O tratamento de dados pessoais segue integralmente os princípios da LGPD, garantindo finalidade, adequação, necessidade, transparência, segurança e responsabilização, sendo vedado qualquer uso discriminatório ou ilícito. Informações devem ser armazenadas apenas pelo período necessário ao cumprimento das finalidades legais, regulamentares ou contratuais, sendo eliminadas de forma segura após o término desse prazo.

17.4. Vazamento de Informações

17.4.1. Em caso de suspeita ou ocorrência de vazamento de informações confidenciais, reservadas ou privilegiadas, voluntário ou involuntário, o colaborador deve comunicar imediatamente a área de Risco e Compliance. A ação deve incluir:

i. Comunicação imediata à Diretoria;

ii. Bloqueio de senhas, acessos, servidores ou recursos necessários para evitar novos vazamentos;

iii. Avaliação da amplitude do vazamento e potenciais impactos;

iv. Elaboração de plano de recuperação;

v. Reavaliação das medidas de segurança existentes para prevenir novas ocorrências.

17.5. Ameaças e Tipos de Ataques Cibernéticos

17.5.1. A Exante Asset reconhece os principais tipos de ataques cibernéticos e suas características, incluindo:

i. Malware: vírus, cavalos de Tróia, spyware, ransomware;

ii. Engenharia social: phishing, pharming, vishing, smishing e acesso em locais públicos;

iii. Ataques de negação de serviço (DoS/DDoS) e botnets;

iv. Invasões sofisticadas (APT – Advanced Persistent Threats);

v. Cryptojacking, Decoy, DMA, Man-in-the-middle (MitM), Spoofing e Zero Day;

vi. Ransomware, worms, trojans, entre outros.

17.5.2. O conceito de ameaça refere-se a qualquer causa potencial de incidente que possa impactar os objetivos do negócio, sejam elas internas ou externas, intencionais ou não.

17.6. Controles Gerais de Segurança e Cibersegurança

17.6.1. A Exante Asset adota controles mínimos de cibersegurança para proteção de dados, sistemas e infraestrutura, incluindo:

i. Ferramentas seguras de backup e armazenamento;

ii. Sistemas de proteção e prevenção de malwares, firewalls, antivírus, filtros de spam e controle de periféricos;

iii. Perfis de acesso diferenciados para administradores;

iv. Assinaturas digitais em processos críticos;

v. Atualização contínua de sistemas e softwares;

vi. Inclusão de requisitos de segurança em novas aplicações e softwares;

vii. Monitoramento e registro de atividades (logs e trilhas de auditoria);

viii. Centros de processamento e armazenamento de dados com controle rigoroso de acesso;

ix. Contratos de manutenção e suporte 24x7 para servidores.

17.7. Boas Práticas

17.7.1. A Exante Asset garante a aplicação de boas práticas internacionais em segurança da informação, incluindo classificação de informações, controles de acesso hierárquicos, monitoramento de atividades, proteção de dados pessoais, autenticação robusta de usuários, proteção de dispositivos e sistemas corporativos, testes contínuos de vulnerabilidades e planos de contingência e recuperação de desastres.

17.8. Risk Assessment

17.8.1. A Gestão de Riscos é feita inicialmente por meio de uma avaliação de riscos e posterior implementação de controles baseados nos riscos, levando em consideração o ambiente de controle da Exante Asset, suas atividades, processos e clientes.

17.8.2. A avaliação de riscos deve ser atualizada de forma a identificar novos riscos, ativos e processos.

17.8.3. A avaliação de riscos segue a metodologia do Risco Operacional, conforme respectiva política.

17.8.4. A gestão de riscos deve contemplar monitoramento e testes com o objetivo de detectar as ameaças e reforçar os controles, bem como criação de ("plano de resposta") que é o planejamento prévio para tratamento e recuperação de incidentes, incluindo um plano de comunicação.

17.9. Tratamento de Incidentes de Segurança da Informação

17.9.1. A Exante Asset adota um plano formal de tratamento de incidentes envolvendo áreas multidisciplinares (TI, Risco, Jurídico, Compliance, Comunicações e Governança Corporativa) para assegurar respostas rápidas e consistentes.

17.9.2. Comunicação e Responsabilidades: Incidentes críticos são comunicados imediatamente aos colaboradores relevantes, com definição clara de papéis, contatos externos e órgãos reguladores.

17.9.3. Classificação e Resposta: Incidentes são classificados por gravidade, com respostas escalonadas, incluindo redundância de equipamentos, acesso remoto ou uso de instalações de contingência físicas ou na nuvem.

17.9.4. Segurança em Contingências: Medidas de controle de acesso e segurança são mantidas em todas as instalações e serviços de contingência.

17.9.5. Documentação: Todos os eventos e ações são documentados detalhadamente, servindo como evidência para auditorias e investigações.

17.9.6. Proteção de Dados Sensíveis: Dados pessoais e sensíveis são protegidos por criptografia, anonimização ou pseudonimização, em conformidade com a LGPD, garantindo uso autorizado e seguro.

17.10. Backups, Plano de Contingência e Continuidade de negócio

17.10.1. Plano de contingência e de continuidade dos principais sistemas e serviços deverá ser implantado e testado no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

17.10.2. Os mesmos controles de segurança e controle de acesso devem ser aplicáveis nas instalações do site de contingência.

17.10.3. Deve haver backup e que os mesmos sejam testados anualmente.

17.11. Testes de Controles

17.11.1. A efetividade da Política de Sigilo de Informações, a Política de Segurança das Informações e da Política de Segurança Cibernética deverão ser verificadas por meio de testes periódicos dos controles existentes

17.11.2. Um plano de teste deve ser efetuado pelo responsável pela área de tecnologia da informação assegurando que:

i. recursos humanos e computacionais estejam adequados ao porte e as áreas de atuação;

ii. adequado nível de confidencialidade e acessos as Informações Confidenciais;

iii. segregação física e lógica;

iv. recursos computacionais, de controle de acesso físico e lógico, estejam protegidos;

v. manutenção de registros que permita a realização de auditorias e inspeções.

17.12. Propriedade Intelectual

17.12.1. Tecnologias, marcas, metodologias e quaisquer informações que pertençam as Exante Asset não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho.

17.13. Rastreamento

Exante Asset Management Ltda.
Ouvidora: +55 11 4550 6588
contato@exante.com.br

17.13.1. Sem prejuízo do disposto neste Política de Segurança Cibernética, é permitido o uso pessoal dos equipamentos de informática e de comunicação utilizados pelos Colaboradores para a realização das atividades profissionais.

17.13.2. Sem prejuízo do disposto nesta Política de Segurança Cibernética, ressaltamos novamente que como tais recursos, como e-mails, sistemas, computadores, telefones e gravação de voz pertencem à Exante Asset, são rastreáveis e sujeitos a monitoramento, bem como podem se tornar públicos em caso de auditoria e/ou exigência judicial.

17.13.3. O acesso interno às informações e gravações deve ser previamente autorizado pelo *"head da área"* e copiado o Diretor de Compliance.

17.14. Termo de Adesão

17.14.1. Os Colaboradores devem aderir formalmente a um termo, comprometendo-se a agir de acordo esta Política de Segurança Cibernética.

17.15. Treinamento

17.15.1. Os Colaboradores que tenham acesso a Informações Confidenciais ou participem de processo de decisão de investimento deverão obrigatoriamente participar de programas de treinamento inicial e de reciclagem continua.

17.15.2. Os treinamentos serão ministrados pelo Diretor de Compliance.

17.16. Programa de Treinamento Inicial

17.16.1. É aquele ministrado ao tempo da contratação de novos Colaboradores, antes da execução de suas atividades na Exante Asset.

17.16.2. O ("Programa de Treinamento Inicial") terá por objetivo principal apresentar aos novos Colaboradores a atividade desenvolvida pela Exante Asset, seus princípios Éticos e de investimento, bem como prestar esclarecimentos sobre as disposições constantes desta Política e das demais normas internas adotadas pela empresa, inclusive no que diz respeito às funções exercidas pelo Diretor de Compliance.

17.16.3. Ademais, o Programa de Treinamento Inicial visa a assegurar a completa informação e esclarecimento dos novos Colaboradores acerca dos procedimentos e controles a

Exante Asset Management Ltda.
Ouvidora: +55 11 4550 6588
contato@exante.com.br

serem adotados para garantir o bom uso das instalações, equipamentos e arquivos da Exante Asset, bem como para o devido cumprimento das normas desta Política.

17.17. Programa de Reciclagem Contínua

17.17.1. ("Programas de Reciclagem Contínua") serão realizados periodicamente e envolverão a participação dos Colaboradores em cursos, palestras e treinamentos sobre temas relacionados à atividade desenvolvida Exante Asset, objetivando promover a constante atualização do conhecimento dos Colaboradores sobre a legislação, regulamentação e auto-regulamentação aplicável e sobre quaisquer outros temas relevantes ao exercício de suas funções e às atividades da sociedade.

17.18. Responsabilidades

17.18.1. Os Colaboradores devem atender às diretrizes e procedimentos estabelecidos nesta Política, informando qualquer irregularidade ao Diretor de Compliance.

17.18.2. O canal de comunicação e denúncia para o assunto é o Comitê.

17.18.3. A Área de Tecnologia da Informação é responsável pela implementação dos procedimentos e controles técnicos inerentes a esta Política de Segurança Cibernética, bem como pelos testes de controle, podendo ser realizados por terceiros, de forma independente.

17.18.4. O Responsável pelo Compliance deve garantir o atendimento a esta Política de Segurança Cibernética, bem como a difusão de uma cultura de segurança na Exante Asset.

Exante Asset Management Ltda.
Ouvidora: +55 11 4550 6588
contato@exante.com.br

18. TERMO DE ADESÃO

POLÍTICA DE SEGURANÇA, SIGILO DAS INFORMAÇÕES E SEGURANÇA CIBERNÉTICOS

DE ACORDO: Declaro que li, compreendi e concordei com todas as políticas integrantes do presente Política de Segurança, Sigilo das Informações e Segurança Cibernéticos ("Política"). Declaro ainda que não tive conhecimento de quaisquer circunstâncias que não foram reportadas ao Comitê ou Diretor de Compliance ("Diretor de Compliance") que poderiam vir a conflitar com este Política de Segurança Cibernética, seja de natureza pessoal ou familiar, bem como referente a qualquer outro Colaborador. Afirmo ter conhecimento das responsabilidades relativas à Política, conforme descrito neste documento.

Data

_____

Colaborador

Exante Asset Management Ltda.
Ouvidora: +55 11 4550 6588
contato@exante.com.br