POLÍTICA DE SEGURANÇA CIBERNÉTICA

Versão:
15/10/2021

EXANTE
ASSET MANAGEMENT

EXANTE
ASSET MANAGEMENT

SUMÁRIO

Exante Asset Management Ltda.
Ouvidora: +55 11 4550 6580
ouvidoria@exante.com.br

1. OBJETIVO

1.1. Esta política tem por objetivo disciplinar e padronizar política de segurança cibernética ("Política de Segurança Cibernética").

1.2. Esta Política de Segurança Cibernética abrange todos os princípios necessários para aderir ao disposto no Código Anbima de Regulação de Melhores Práticas para Administração de Recursos de Terceiros vigente ("Código ANBIMA") que dispõe sobre a atividade de gestor de recursos de terceiros, bem como, o credenciamento na categoria de gestor de recursos e consultor de compliance da Exante Asset Management Ltda. ("Exante Asset"), nos termos da Instrução CVM nº 558.

1.3. A Exante Asset tem como princípio basilar exercer suas atividades com boa-fé, transparência, diligência e lealdade, dispendendo no exercício de suas atividades, todo o cuidado que toda pessoa prudente e diligente costuma dispensar à administração de seus próprios negócios.

1.4. Com a finalidade de garantir a proteção, a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações de sua propriedade e/ou sob sua guarda, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, definindo as regras que representam, em nível estratégico, os princípios fundamentais incorporados pela Exante Asset para o alcance dos objetivos de segurança da informação.

1.5. Essa Política demonstra o compromisso da Exante Asset e de sua Alta Administração em zelar e tratar as informações de seus clientes, de forma a proporcionar plena satisfação quanto à segurança e privacidade de suas informações. Demonstramos também o compromisso com os aspectos regulatórios e estratégicos da Exante Asset, estando assim, em conformidade com as principais regulamentações vigentes.

1.6. A presente Política de Segurança Cibernética entrará em vigor em janeiro de 2021 e vigorará por prazo indeterminado.

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.

Exante Asset Management Ltda.
Ouvidora: +55 11 4550 6580
ouvidoria@exante.com.br

2.2 Posto isto, antes do início do exercício de suas funções perante à Exante Asset, os Colaboradores deverão receber uma cópia desta Política de Segurança Cibernética, bem como, firmar o Termo de Adesão abaixo, declarando se encontrar totalmente familiarizado a Política de Segurança Cibernética 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 de Segurança Cibernética em sua sede e na rede mundial de computadores.

2.4 O descumprimento das regras estabelecidas nesta Política de Segurança Cibernética 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 de Segurança Cibernética, incluindo uma revisão anual dos processos e procedimentos, manutenção e atualização da mesma.

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

3. PRINCÍPIO DA SEGURANÇA DA INFORMAÇÃO

3.1 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.

Exante Asset Management Ltda.
Ouvidora: +55 11 4550 6580
ouvidoria@exante.com.br

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.

4. INFORMAÇÕES CONFIDENCIAIS

4.1 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.

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

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

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

4.2.3 Aos órgãos reguladores do mercado financeiro; e

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

5. POLÍTICA DE SEGURANÇA CIBERNÉTICA

5.1. Ataques cibernéticos / Cibersegurança

Os ataques cibernéticos mais comuns são:

5.1.1. Malware – softwares desenvolvidos para corromper os computadores e redes, como:

i. Vírus: software que causa danos à máquina, rede, softwares e Banco de Dados;

ii. Cavalo de Troia: aparece dentro de outro software criando uma porta para a invasão do computador;

iii. Spyware: software malicioso para coletar e monitorar o uso de informações; e

iv. Ransomware: software malicioso que bloqueia o acesso aos sistemas e base de dados, solicitando um resgate para que o acesso seja reestabelecido.

5.1.2. Engenharia social: são os métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito, como exemplo:

i. Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;

ii. Phishing: links vinculados por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

iii. Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

iv. Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes, a fim de captar qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

v. Ataques de DDoS (*distributed denial of services*) e *botnets* – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição.

Exante Asset Management Ltda.
Ouvidora: +55 11 4550 6580
ouvidoria@exante.com.br

vi. Invasões (*advanced persistent threats*) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

5.2. Controles Gerais de Segurança da Informação e Cibersegurança

5.2.1. A Exante Asset deve adotar controles mínimos de Cibersegurança, que devem ser garantidos por meio de tecnologia da informação, sendo eles:

5.2.2. Proteção dos dados armazenados, contendo ferramenta segura de backup, conforme necessário; bancos de dados e dispositivos de rede devem ser enviados para um sistema de segurança dedicado que seja rigorosamente controlado para preservar a integridade, a confidencialidade e a disponibilidade do conteúdo;

5.2.3. Uso de assinaturas digitais para alguns processos/Colaboradores críticos;

5.2.4. Atualização dos sistemas operacionais e softwares utilizados na instituição;

5.2.5. Prevenção de ameaças com firewalls, antivírus, perfis de acesso específico para os administradores das máquinas, filtros de spam, controle para uso de periféricos (pendrives, CDs e HDs), DLP, FireEye e filtros de uso de internet;

5.2.6. Inclusão das preocupações de segurança durante as fases de desenvolvimento de novos sistemas, softwares ou aplicações;

5.2.7. Controles de auditoria, tais como sistemas de gerenciamento de senhas, logs e trilhas de acesso;

5.2.8. Controle de acesso e um centro de processamento e armazenamento de dados;

5.2.9. Contrato de manutenção com Suporte 24x7 dos Servidores.

5.3. Risk Assessment

5.3.1. 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.

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

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

5.3.4. 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.

5.4. Tratamento de Incidentes de Segurança da Informação

5.4.1. Os riscos e incidentes da Política de Segurança da Informação e da Política de Segurança Cibernética deverão ser reportados ao Diretor Compliance, que analisará caso a caso e adotará as medidas cabíveis.

5.5. Backups, Plano de Contingência e Continuidade de negócio

5.5.1. 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.

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

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

5.6. Testes de Controles

5.6.1. 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

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

a) recursos humanos e computacionais estejam adequados ao porte e as áreas de atuação;
b) adequado nível de confidencialidade e acessos as Informações Confidenciais;
c) segregação física e lógica;
d) recursos computacionais, de controle de acesso físico e lógico, estejam protegidos;

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

5.7. Propriedade Intelectual

5.7.1. 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.

5.8. Rastreamento

5.8.1. 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.

5.8.2. 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.

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

5.9. Termo de Adesão

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

5.10. Treinamento

5.10.1. 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.

5.10.2. Os treinamentos serão ministrados pelo Diretor de Compliance.

5.11. Programa de Treinamento Inicial

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

5.11.2. 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.

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

5.12. Programa de Reciclagem Contínua

5.12.1. ("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.

5.13. Responsabilidades

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

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

5.13.3. 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.

5.13.4. 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 6580
ouvidoria@exante.com.br

6. TERMO DE ADESÃO

Política de Segurança Cibernética

DE ACORDO: Declaro que li, compreendi e concordei com todas as políticas integrantes do presente Política de Segurança Cibernética ("Política de Segurança Cibernética"). 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 6580
ouvidoria@exante.com.br