Política de Segurança da Informação

Abril/2023

Jatobá Gestora de Recursos Ltda.

Avenida Coronel Teixeira, 6225, 111º andar – Sala 1106 - Ponta Negra – Manaus – Amazonas 69037-000
www.jatobagestao.com.br + 55(92) 98166-66666

1. Objetivo

A presente Política de Segurança da Informação ("Política") estabelece as práticas e os cuidados mínimos necessários e aplicáveis a todos os colaboradores da Jatobá Gestora de Recursos ("Jatobá") no manuseio, guarda, descarte e transmissão de informação, dos clientes ou da empresa, respeitando as definições e conceitos estabelecidos das informações, garantia de que as informações sejam utilizadas apenas para a finalidade específica para que foram obtidas, a prevenção da adulteração das informações e a disponibilidade das informações para o desempenho das atividades da Jatobá e para envio as autoridades nos termos da regulamentação.

Um sistema de informações, transparente e eficaz, se constitui num ativo muito importante, sobretudo em empresas pertencentes ao mercado financeiro e de capitais. A Jatobá depende do correto manejo de informação para realizar negócios e atender suas obrigações operacionais, comerciais e estratégicas. Estes sistemas de informação, bases de dados, equipamentos, tecnologia e documentos em geral, sejam eles internos ou externos, devem ser protegidos.

Para efeito desta política, são considerados como "informação", todas as informações referentes aos clientes da Jatobá, informação da própria Jatobá e de seus colaboradores, informações para a continuidade de seus negócios e outras que tenham sido confiadas a Jatobá sob orientações expressas de confidencialidade. Seguindo os conceitos das boas práticas de controles e de segurança da informação, condizentes com o tamanho e com as atividades desenvolvidas pela Jatobá, a presente Política busca sua implementação de uma estrutura de controle formal, para assegurar a responsabilidade e a segurança no uso das informações. Este consiste em um passo essencial para estabelecer os níveis de controle e responsabilidade necessários para preservar a relação fiduciária mantida com os clientes e assegurar a observância da regulamentação em vigor.

Para fins desta Política estarão sujeitos aos cuidados aqui descritos as seguintes informações: (i) toda e qualquer informação relativa a clientes; (ii) informações sobre estratégia de negócios da Jatobá; (iii) informações pessoais sobre colaboradores da Jatobá; e (iv) outras informações que tenham sido confiadas a Jatobá sob obrigação expressa de confidencialidade.

Esta Política está em linha com o artigo 28 da Resolução CVM nº21 de 25 de fevereiro de 2021.

2. Responsabilidade

A presente Política é de responsabilidade do Diretor de Compliance a quem cabe as seguintes responsabilidades:

- Assegurar a disseminação da Política entre todos os colaboradores da Jatobá e esclarecer todas as eventuais dúvidas sobre a mesma;
- Conscientizar os colaboradores sobre a importância da observância das regras estabelecidas nesta Política e das potenciais consequências em caso de descumprimento;
- Dar conhecimento a todos os colaboradores sobre as alterações realizadas na Política;
- Assegurar o controle de informações confidenciais a que tenham acesso seus administradores e colaboradores;
- Realizar testes periódicos de modo a garantir que os procedimentos descritos nesta Política estejam sendo cumpridos.

É responsabilidade de cada colaborador o conhecimento da presente Política e a observância de suas disposições. Em caso de dúvida, o colaborador deverá recorrer ao Diretor de Compliance para esclarecimentos, abstendo-se de utilizar informações até que a dúvida seja esclarecida.

Na hipótese de compartilhamento de informações com prestadores de serviço, a Jatobá, por meio de seu Diretor de Compliance e de assessoria jurídica externa, conforme aplicável, deverá garantir que possui autorização do cliente, bem como que o prestador de serviço observe os procedimentos estabelecidos nesta Política.

3. Gestão de Acessos Físicos e Lógicos

i. Acesso Físico

As instalações da Jatobá ficam localizadas em prédio comercial com portaria e somente os colaboradores estão autorizados a acessar as dependências. O conjunto comercial no qual a Jatobá está instalada é mantido trancado e clientes e prestadores de serviços são recebidos na área comum. Excepcionalmente, clientes e prestadores de serviços podem ser acompanhados, por diretor, a visitar a área de trabalho devendo sempre ser acompanhado por um colaborador.

ii. Acesso Lógico

As informações eletrônicas e os sistemas internos deverão ser acessados mediante login e senha pessoal e intransferível. Tal acesso deve ser solicitado ao gestor da área do colaborador solicitante.

Após aprovação, cabe ao Diretor de Compliance avaliar a solicitação e conceder o acesso solicitado.

Anualmente, no mês de fevereiro, o Diretor de Compliance deverá avaliar a pertinência dos acessos concedidos e se os mesmos deverão ser mantidos ou alterados. O diretor de Compliance deverá, nesta oportunidade verificar se os controles de acesso estabelecidos estão em funcionamento. Na hipótese de detecção de algumas irregularidades, o Diretor de Compliance deverá apresentar aos demais diretores relatório com o problema identificado e com o plano de correção. Caso seja detectada alguma irregularidade na conduta de determinado colaborador a diretoria deverá, em conjunto, determinar os procedimentos a serem adotados.

Na hipótese de desligamento de algum colaborador, todos os acessos são imediatamente bloqueados.

iii. Políticas de Senhas

A senha é de uso pessoal e intransferível.

O eventual uso ou acesso indevido é de total responsabilidade do detentor e titular da senha que deve tomar todos os cuidados necessários para salvaguardá-la;

O compartilhamento de senhas somente será permitido em casos de indisponibilidade para uso individual e se aprovado prévia e formalmente;

Toda e qualquer senha, de acesso físico ou lógico, deverá ser imediatamente bloqueada em caso de desligamento; quanto às características e complexidade, a senha; deve possuir, no mínimo, 8(oito) caracteres e entre letras, números e caracteres especiais, se necessários;

Após 3 (três) tentativas, em caso de insucesso, ser automaticamente bloqueado; e sendo nova, o usuário deverá, obrigatoriamente, alterá-la seguindo os critérios acima citados.

4. Armazenamento e Tratamento de Dados e Informações

Cada Colaborador da Jatobá é responsável direto pela guarda e verificação da integridade dos arquivos, documentos, planilhas, relatórios, e demais documentos que utilize para a construção de suas atividades.

O armazenamento de informações de clientes, confidenciais ou relevantes, devem permanecer em locais (físicos ou lógicos) de acesso restrito, seguros e organizados quando não estiverem sendo manuseados.

Não é recomendado o uso do e-mail para o armazenamento de informações relevantes. Estas deverão ser arquivadas na rede corporativa para assegurar o efetivo procedimento de backup dos dados em caso de contingência ou incidente.

O envio de informações e documentos em meio físico para locais externos deve ser necessariamente protocolado (entrada e saída) e arquivado para fins comprobatórios e de rastreamento, quando necessário.

Relatórios de auditorias, órgãos regulados ou fiscalizadores são de propriedade da Jatobá, e consequentemente, estritamente confidenciais.

i. Backup de Dados e Informações da Jatobá

A prática e as rotinas diárias de backup visam assegurar a disponibilidade das informações geradas ou utilizadas pela Jatobá, inclusive e prioritariamente aplicáveis aos negócios da Jatobá.

O período de armazenagem de informações, antes do descarte definitivo, deve respeitar os períodos exigidos por leis, normas e regulamentos aplicáveis aos negócios da Jatobá.

Para assegurar a segurança, organização e periodicidade de guarda dos dados, a Jatobá possui procedimento de backup que compreendem: cópia, armazenamento e recuperação de suas informações e de seus clientes.

ii. Prevenção contra Invasões

A prevenção contra riscos de invasões e exposições indevidas das informações eletrônicas é realizada através do equipamento de segurança de rede FORTINET, modelo FortiGate 50E Fortiwifi-50E. Possui proteção contra as ameaças avançadas, incluindo firewall, antivírus, controle de aplicativos, IPS, VPN e Web Filtering. Executa varredura de vulnerabilidade de rede ajudando na proteção dos ativos de rede e identificado as falhas de segurança.

iii. Uso de Recursos de Tecnologia

A Jatobá é proprietária do direito de uso de todos os recursos de tecnologia colocados à disposição dos colaboradores, bem como todas as informações criada e gerada durante as atividades profissionais ou nas dependências da empresa.

Os recursos de tecnologia da Jatobá abrangem: computadores desktops, notebooks, impressoras, e 1 servidor todos em rede elétrica estabilizada, link dedicado de internet, central telefônica e um modulo de gravação, periféricos, telefonia e mídia em geral.

É expressamente proibida, portanto, a utilização de quaisquer recursos de tecnologia que não sejam de propriedade da Jatobá, tais como: recursos de multimidia, monitores, notebooks, HD externo, pen drivers e demais mídias removíveis, impressoras, etc...

O bom e correto uso dos recursos de tecnologia é responsabilidade de todos os colaboradores da empresa.

iv. Utilização do E-mail e Telefonia

O funcionário deve prezar pela boa e responsável utilização de sua conta de e-mail corporativo. É permitida a utilização do email para fins pessoais e outros assuntos não relacionados às atividades profissionais e aos negócios da Jatobá.

A empresa entende que um dos principais meio de invasão criminosa de sistema é por meio do acesse ou clique do usuário em arquivos ou sites não confiáveis, desta forma, busca conscientizar seus colaboradores sobre a necessidade de verificação rigorosa dos e-mails recebidos. Todos os colaboradores estão obrigados a serem diligentes e evitarem acesso a arquivos e sites que possam colocar em risco a integridade dos sistemas da Jatobá, bem como as informações armazenadas.

O correio eletrônico não pode ser utilizado, sem autorização prévia e controle específico, para envio ou recepção de mensagens que contenham arquivos executáveis, ou ainda outros mecanismos que possam conter vírus e, portanto, causar algum dano aos equipamentos da Jatobá ou seus destinatários.

É expressamente proibido o uso do e-mail corporativo para participação em blogs, redes sociais, serviços de webmail ou mensageria, cadastramento em sites para fins pessoais.

Cabe ressaltar que é proibido o envio, recepção ou encaminhamento de mensagens com teor ofensivo, ideologias políticas, religiosas ou raciais, pornografia, apologia às drogas, terrorismo, dentre outros considerados impróprios.

Quanto às assinaturas de e-mail, somente é permitido o uso do padrão interno previamente definido (inclusive formato e ordem das informações).

V. Informações privilegiadas

As consequências do uso de informações privilegiadas podem ser graves, tanto para o colaborador quanto para a gestora.

Informações privilegiadas podem incluir, mas não se limitam, a informações relacionadas com propostas ou contratos de fusão e aquisição, modificação na situação financeira, previsões ou projeções financeiras, oferta ou transações de títulos e valores mobiliários, licitações, informações sobre crédito, alterações de dividendos, desinvestimentos, processos de falência, litígios substanciais, alterações na administração, desenvolvimento de produtos, anúncios de lucros, novos comunicados ou outros eventos significativos a respeito de um emitente.

Importante esclarecer que informações privilegiadas também podem se referir a eventos futuros ou passados.

Algumas regras básicas quanto ao cuidado no tratamento de informações privilegiadas, são:

I – É vedado, ao funcionário, compra, venda ou recomendação de títulos e valores mobiliários de um emissor ou cotas de um fundo de investimento para qualquer conta própria, de cliente, de funcionário ou outra quando estiver de posse de informações relevantes e não disponíveis ao publico (“informações privilegiadas”), devendo realizar todas as atividades de investimentos de acordo com as leis, normas e regulamentos aplicáveis;

II – É expressamente proibida a compra, venda, recomendação ou comercialização, de qualquer tipo, valor mobiliário ou cotas de fundos de investimentos, tanto pessoalmente quanto em

nome de outros, na eventualidade do funcionário possuir informações privilegiadas relacionadas a tal título/fundo;

III – Os colaboradores estão orientados a indicar, como "informação confidencial", todas as informações privilegiadas relevantes e não disponíveis ao público; e

IV – Todas as informações privilegiadas que forem obtidas durante o exercício pleno e responsável das atividades não deverão ser consideradas conforme previsto nesta Política e nas leis e normas em vigor.

5. Incidentes

Diante de uma eventual suspeição de fraude ou incidente que comprometa a segurança das informações da Jatobá ou no caso de ocorrência de um "vazamento" de informações ou incidente de segurança, o funcionário deve registrar e comunicar o fato imediatamente à área ao Diretor de Compliance.

6. Código de Ética e Conduta

O Código de Ética e Conduta da Jatobá estabelece as diretrizes gerais e profissionais de conduta esperadas de todos os colaboradores em suas relações entre si, com clientes, prospects, concorrentes, fornecedores, prestadores de serviços e com toda a sociedade.

A plena observância das diretrizes constantes ao longo do Código é premissa fundamental também para minimização dos riscos inerentes à segurança de nossas informações.

7. Penalidades

A não observância do disposto nesta política será considerada como falta grave de acordo com o Código de Conduta e Ética da Jatobá. O colaborador poderá sofrer sansões, conforme o grau de gravidade, a serem definidas em conjunto pelos diretores da Jatobá e poderão compreender: advertência, revisão das responsabilidades, suspensão ou demissão, além de penalidades legais aplicáveis.