POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

03/06/2021

SUMÁRIO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

1. OBJETIVO

A presente Política de Segurança da Informação e Cibernética ("Política") tem como objetivo criar uma referência interna para a implantação de um ambiente tecnológico e informacional seguro, facilitando o controle da informação e processos relacionados, inclusive no tocante a atividades de contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, em linha com princípios de segurança da informação, com a regulamentação aplicável e com as melhores práticas de mercado.

As diretrizes da presente Política também visam proteger, de acordo com a LGPD, os dados pessoais tratados pela Vixi Exchange de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

2. APLICAÇÃO E VIGÊNCIA

Aplica-se aos Colaboradores e Terceiros da Vixi Exchange, a partir de **03/06/2021**.

3. DEFINIÇÕES

- **Colaborador(es):** todos os funcionários e empregados da Vixi Exchange, bem como todos que possuam cargo, função, posição, ou relação societária, empregatícia, comercial, profissional, contratual ou de confiança com a Vixi Exchange, assim como os estagiários e trainees;

- **Diretoria:** trata-se de grupo formado pelos membros da diretoria da Vixi Exchange. A Diretoria tem por função acompanhar os projetos da Companhia e seus respectivos resultados, bem como deliberar e direcionar os referidos projetos com base no melhor interesse da Companhia;

- **Lei de Sigilo Bancário:** a Lei Complementar nº 105, de 10 de janeiro de 2001;

- **LGPD**: a Lei nº 13.709, de 14 de agosto de 2018, conhecida como a Lei Geral de Proteção de Dados;

- **Política:** a presente Política de Segurança da Informação e Cibernética;
- **Terceiro(s):** fornecedores e prestadores de bens e serviços, representantes, agentes intermediários, procuradores, consultores técnicos, despachantes, colaboradores externos e/ou quaisquer outros terceiros que atuem em nome, benefício ou interesse da Vixi Exchange.

4. CONSIDERAÇÕES

4.1. RESPONSABILIDADES

4.1.1. Os Diretores e a área de Segurança da Informação da Vixi Exchange são responsáveis por garantir que o todos os Colaboradores, em suas respectivas áreas de negócios, estejam cientes de suas obrigações relativas à segurança da informação.

4.1.2. A segurança da informação visa a geração de valor aos *stakeholders*, bem como o fortalecimento da governança corporativa e do ambiente de controles internos.

4.1.3. A estrutura de segurança da informação da Vixi Exchange contempla os modelos definidos internamente, com técnicas de acompanhamento de riscos voltados à segurança da informação e pessoal especializado subordinado hierarquicamente aos departamentos ligados aos componentes corporativos de risco.

4.2. SEGURANÇA DA INFORMAÇÃO

4.2.1. A informação é um dos mais valorizados patrimônios no ambiente de negócios. Além da posse de uma informação estruturada e de qualidade ser um de seus objetivos estratégicos, a informação é um ativo fornecido pelos nossos clientes e parceiros que deve ser tratado com o mais alto nível técnico, de sigilo e de confidencialidade, observando a legislação vigente.

4.2.2. São exemplos de informações confidenciais:

- Informações de clientes que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (número de inscrição no Cadastro Nacional de Pessoas Físicas do Ministério da Economia - CPF, RG, endereço etc.), dados transacionais, situação financeira e movimentação de recursos;

- Informações sobre produtos e serviços que revelem vantagens competitivas da Vixi Exchange frente ao mercado;

- Todo o material estratégico da Vixi Exchange (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);

- Quaisquer informações da Vixi Exchange que não devam ser divulgadas ao meio externo antes da publicação pelas áreas competentes; e

- Todos os tipos de senhas a sistemas, redes, estações e outras informações utilizadas na autenticação, lembrando que são dados pessoais e intransferíveis.

4.2.3. Um fluxo de informação de qualidade é capaz de decidir o sucesso de um empreendimento, de um projeto e de uma avaliação. Entretanto, esse poder, somado à crescente facilidade de acesso, faz desse "ativo" um alvo de constantes ameaças internas e externas.

4.2.4. Quando não gerenciados adequadamente, esses riscos e ameaças podem causar consideráveis danos à Vixi Exchange, parceiros e clientes, prejudicando seu crescimento e vantagem competitiva.

4.2.5. Todos os Colaboradores da Vixi Exchange devem zelar pelas informações sob sua responsabilidade, atentando-se para os seguintes aspectos principais:

- **Integridade**: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;

- **Confidencialidade e Sigilo**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas, nos termos da LGPD e da Lei de Sigilo Bancário; e

- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

4.3. TRATAMENTO DAS INFORMAÇÕES

4.3.1. Categorizamos os tipos de informação a depender do seu uso, como:

- **Informação Pública**: pode ser acessada por Colaboradores, clientes, Terceiros e pelo público em geral.

- **Informação Interna**: somente pode ser acessada por Colaboradores. Possuem um grau de sensibilidade que pode comprometer a imagem da organização e/ou impacto negativo nos objetivos e resultados. O acesso não é restringido por controles internos.

- **Informação Confidencial**: pode ser acessada apenas por funcionários da organização que detenham autorização especial. A divulgação não autorizada pode causar impacto ao negócio, clientes, parceiros e/ou à reputação da Vixi Exchange. Acesso permitido apenas quando uma necessidade de trabalho tiver sido identificada e tal acesso for aprovado expressamente.

4.3.2. De forma geral, cabe a todos os Colaboradores e Terceiros associados à Vixi Exchange:

- Cumprir fielmente a presente Política;

- Proteger informações contra acessos indevidos, modificação, destruição ou divulgação não autorizados;

- Assegurar que os recursos tecnológicos, as informações e sistemas à sua disposição sejam utilizados apenas para as finalidades determinadas e aprovadas;

- Cumprir as leis e as normas que regulamentam a propriedade intelectual, bem como a LGPD e a Lei de Sigilo Bancário; e

- Não compartilhar informações confidenciais ou sigilosas de qualquer tipo.

4.4. INFORMAÇÕES NÃO ESTRUTURADAS – CONVERSAS EM LOCAIS PÚBLICOS

4.4.1. Os seguintes cuidados devem ser observados quanto ao tratamento de informações não estruturadas (voz e armazenadas fora de sistemas informatizados):

- Não se deve discutir ou comentar assuntos confidenciais da Vixi Exchange em locais públicos ou por meio de mensagens de texto particulares;

- A informação difundida oralmente também deve ser objeto de cautela, tanto no âmbito das dependências internas quanto externas;

- Sempre que os Colaboradores estiverem em locais públicos, faz-se necessária a adoção de práticas capazes de assegurar o sigilo das informações (ex.: não menção de nomes de clientes, parceiros e prospects);

- Outra cautela a ser tomada é a discrição e impessoalidade na referência a empresas e pessoas, bem como a não menção a questões sensíveis;

- De modo geral, objetivos, comentários, estratégias, orçamentos etc. devem ser discutidos em ambiente privado, tais como reuniões internas e/ou salas de chat privadas; e

- É vedada a obtenção de informações de forma ilícita (i.e., em descumprimento com as normas e regulamentações aplicáveis), com qualquer finalidade.

4.5. USO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO

4.5.1. O usuário autorizado é totalmente responsável pela correta posse e utilização de suas senhas e autorizações de acesso a sistemas, assim como pelas ações decorrentes da utilização.

4.5.2. O acesso e uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas explicitamente autorizadas e de acordo com a necessidade para suas funções, observando-se a regra de “mínimo acesso necessário”.

4.5.3. Periodicamente, os acessos concedidos devem ser revisados pelo Gestor de Segurança da Informação da Vixi Exchange.

4.5.4. Todos os Colaboradores devem adotar as seguintes práticas básicas:

- Manter atualizados nos servidores e redes compartilhadas os produtos dos trabalhos desenvolvidos no curso das atividades;

- Não manter cópias de seus arquivos em computador local;

- Utilizar senhas complexas que contenham caracteres compostos de letras, números e símbolos, evitando o uso de nomes, sobrenomes, números de documentos, telefones, datas que possam ser relacionadas com o usuário, alterando tais senhas periodicamente;

- Utilizar criptografia sempre que enviar ou receber dados contendo informações confidenciais/estratégicas, observada a necessidade de autorização desse compartilhamento;

- No uso de internet, certificar a procedência de qualquer website e a utilização de conexões seguras (criptografadas) ao realizar transações;

- Verificar a integridade de websites cujos acessos sejam necessários ao exercício da atividade;

- Digitar no navegador o endereço desejado e não utilizar links desconhecidos como recurso para acessar um outro endereço de destino;

- Não abrir arquivos ou executar programas anexados a e-mails, sem antes verificá-los com um antivírus; e

- Não utilizar o formato executável em arquivos compactados.

4.5.5. São expressamente proibidas pela presente Política as seguintes atividades:

- Introduzir códigos nos sistemas de TI, utilizar, facilitar ou permitir entradas de terceiros por quaisquer meios;

- Revelar códigos de identificação, autenticação e autorização de uso pessoal (ex.: conta, senhas, chaves privadas etc.) ou permitir o uso por terceiros de recursos autorizados por intermédio desses códigos;

- Divulgar ou comercializar produtos, itens ou serviços a partir de qualquer recurso dos sistemas de TI;

- Tentar interferir sem autorização expressa em um serviço ou transação;
- Alterar registro de evento dos sistemas;
- Modificar protocolos de comunicação de dados;
- Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades;
- Monitorar ou interceptar o tráfego de dados nos sistemas de TI;
- Violar medida de segurança ou autenticação, sem autorização de função competente;
- Fornecer informações a terceiros sobre usuários ou serviços disponibilizados nos sistemas de TI, exceto os de natureza pública ou mediante autorização expressa;
- Armazenar ou usar jogos em recursos pertencentes ao ambiente da Vixi Exchange; e
- Utilizar aplicativos não homologados e/ou com licença inativa ou não autorizada.

4.5.6. As solicitações de acesso devem seguir as seguintes premissas:

- As solicitações de novas identificações de usuários e alterações de privilégios devem ser feitas por escrito e aprovadas pela área de Segurança da Informação, sendo mapeadas as suas necessidades conforme o escopo de trabalho de cada Colaborador;
- Em caso de alterações, os usuários devem fundamentar a necessidade das mudanças em seus privilégios e a relação de tais alterações com as atividades exercidas;
- Privilégios devem ser imediatamente revogados quando da finalização de projetos específicos, caso o profissional atuante esteja trabalhando como Colaborador ou parceiro. O mesmo deverá ser observado no desligamento ou fim da relação contratual, sendo o Colaborador desligado ou o parceiro inteiramente responsável pelas atividades e atos perpetrados durante a sua permanência;

- Os privilégios para todos os usuários dos serviços da rede deverão ser revisitados a cada 12 (doze) meses pela área de Segurança da Informação ou em periodicidade menor, caso haja necessidade.

4.5.7. Os Colaboradores devem observar as seguintes diretrizes no que tange às senhas de acesso:

- As senhas de acesso são os controles de segurança para os sistemas do ambiente de TI da Vixi Exchange e são pessoais, sigilosas e intransferíveis;

- Em caso de suspeita de exposição indevida, o fato deve ser comunicado imediatamente à área de Segurança da Informação e todas as senhas devem ser alteradas;

- Os usuários devem possuir orientação sobre a manutenção sigilosa das suas senhas de acesso e as responsabilidades envolvidas com seu mau uso;

- Em caso de comprometimento comprovado da segurança do ambiente de TI por algum evento não previsto, todas as senhas de acesso deverão ser modificadas;

- Da mesma forma, todas as alterações recentes de usuários e privilégios do sistema devem ser revisadas para detectar eventuais modificações não autorizadas de dados; e

- Todos os usuários precisam ser identificados antes de estarem aptos a realizar qualquer atividade em ambiente de TI.

4.5.8. Quanto ao uso de equipamentos e recursos de comunicação:

- Equipamentos corporativos, assim como os softwares da Vixi Exchange, devem ser disponibilizados e homologados pela área de Segurança da Informação;

- Equipamentos particulares, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes se não estiverem previamente autorizados;

- Os computadores com informações sensíveis e/ou classificadas deverão, obrigatoriamente, ser desligados ou bloqueados na ausência do Colaborador;

- Quando os equipamentos ou contas de Colaborador não estiverem em uso deverão ser imediatamente bloqueados ou desligados;

- É vedado o acesso não autorizado às caixas postais de terceiros e eventuais tentativas de acesso devem ser registradas em log;

- É vedado o envio de informações críticas para pessoas ou organizações não autorizadas, observando-se, quando aplicável, orientações para informações classificadas;

- É vedado o envio de material obsceno, ilegal ou não ético, propaganda, mensagem de entretenimento ou mensagens de qualquer natureza relacionadas com nacionalidade, raça, orientação sexual, religiosa, convicção política ou qualquer outro assunto que não tenha relação com o escopo de trabalho;

- Deve ser evitado o envio de mensagens simultâneas a todos os usuários da rede;

- Aplicativos de comunicação devem ser utilizados sempre baseados no bom senso e de acordo com os preceitos legais;

- Produtos resultantes do trabalho de usuários autorizados (coleta de dados e documentos, sistema, metodologia, resultados, dentre outros) são propriedade da Vixi Exchange. Em caso de extinção ou rescisão de contrato, esses usuários devem devolver todas as informações confidenciais geradas e manuseadas em decorrência da prestação dos serviços, ou emitir declaração de destruição;

- Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis. Documentos não devem ser abandonados após a sua impressão ou cópia; e

- Seguindo a melhor orientação legal, a Vixi Exchange reserva-se ao direito de monitorar equipamentos, correio eletrônico e ferramentas de comunicação corporativas sempre que necessário, independentemente de comunicação e/ou autorização prévia do Colaborador.

4.6. PROCESSAMENTO, ARMAZENAMENTO E COMPUTAÇÃO EM NUVEM

4.6.1. A Vixi Exchange deve manter em sua operação as premissas definidas por esta Política, assim como os controles para assegurar a confidencialidade, a integridade e disponibilidade dos dados e dos sistemas suporte em conformidade com a estrutura de negócios, perfil de risco e natureza das atividades da Vixi Exchange.

4.6.2. Aplicativos de comunicação devem ser utilizados sempre baseados no bom senso e de acordo com os preceitos legais.

4.6.3. Na contratação de Terceiros para atividades de processamento, armazenamento de dados e de computação em nuvem, a área de Segurança da Informação será responsável por conduzir um processo de *Due Diligence* do potencial parceiro contratado, a fim de averiguar (i) sua capacidade técnica e operacional, (ii) a segurança e integridade de seus sistemas, e (iii) a possibilidade de cumprimento integral das disposições da presente Política.

4.7. TRATAMENTO DE EVENTOS DE SEGURANÇA DA INFORMAÇÃO

4.7.1. A responsabilidade da comunicação de eventos de segurança da informação para as áreas competentes é atribuída a todos Colaboradores da Vixi Exchange.

4.7.2. Toda a comunicação de eventos que impactem negativamente as premissas da segurança de informação deverão ser comunicadas oportunamente à área Segurança da Informação.

4.7.3. Cabe à área de Segurança da Informação a coleta dos dados e evidências dos eventos que impactam negativamente a segurança da informação da Vixi Exchange.

4.7.4. Todas as evidências coletadas devem ser devidamente arquivadas e direcionadas à área de Compliance da Vixi Exchange por meio magnético e/ou em diretório com restrição de acessos.

4.7.5. A área de Segurança da Informação deve aplicar a análise com base na causa-raiz do evento, assim como documentar em relatório internos as características do evento.

4.7.6. Não será permitida a realização da análise por parte dos agentes envolvidos ou por quem identificou o evento.

4.7.7. Deverá ser destacado nos relatórios internos o plano de ação para mitigar os eventos identificados pela entidade, assim como as datas para a implementação das melhorias por parte das áreas envolvidas.

4.7.8. Cabe à área da Segurança da Informação realizar o monitoramento da implantação dos planos de ação e à área de Compliance certificar sua eficácia.

4.7.9. Todas as análises de eventos deverão ser suportadas por classificação de acordo com o impacto esperado, conforme a seguir:

- **Alto (Impacto Grave)**: Evento que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre a receita ou clientes ou que comprometa a continuidade dos negócios da Vixi Exchange;

- **Médio (Impacto Significativo)**: Evento que afeta sistemas ou informações não críticas, sem impacto negativo à receita ou clientes, decorrente de erros não intencionais ou fragilidade nos processos; e

- **Baixo (Impacto Mínimo)**: Possível evento, sistemas não críticos, investigações de incidentes ou de Colaboradores, investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho forense detalhado.

4.7.10. São classificados como eventos negativos ou adversos:

- Qualquer evento adverso confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, bem como estruturas físicas e lógicas associadas, que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;

- Indisponibilidade do ambiente tecnológico por ataques maliciosos;

- Incidentes de segurança ou situações de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

- Tentativas internas ou externas de ganhar acesso não autorizado a sistemas, a dados ou até mesmo comprometer o ambiente de TI;

- Violação da política de segurança;

- Uso ou acesso não autorizado a um sistema;

- Modificações em um sistema, sem o conhecimento ou consentimento prévio do gestor responsável; e

- Compartilhamento de senhas.

4.8. VIOLAÇÕES À POLÍTICA

4.8.1. Violações de segurança devem ser informadas à área de Segurança da Informação.

4.8.2. Toda violação ou desvio será devidamente investigado para a determinação das medidas necessárias, visando a correção da falha ou reestruturação de processos.

4.8.3. Abaixo algumas violações que podem resultar em sanções administrativas, cíveis e criminais:

- Uso ilegal de software;

- Introdução de vírus ou programa malicioso (intencional ou não);

- Tentativas de acesso não autorizados a dados e sistemas;

- Compartilhamento de informações confidenciais/sensíveis do negócio; e

- Divulgação de informações de clientes, parceiros ou operações contratadas.

4.8.4. A não-conformidade com as diretrizes desta Política e a violação de normas derivadas sujeita os infratores às penas de responsabilidade civil e criminal nos termos previstos em lei, sem prejuízo da imediata rescisão do contrato de prestação de serviços do colaborador envolvido.

4.8.5. É de responsabilidade do usuário conhecer e cumprir a legislação, em especial a obrigação de sigilo prevista no artigo 5º, XII, da Constituição Federal, a Lei n. 12.737/2012 (tipificação criminal de delitos informáticos), as disposições do Marco Civil da Internet (Lei n. 12.965/2014), a LGPD e a Lei de Sigilo Bancário.

***