Público

Política de Segurança Cibernética e da Informação

LEV DISTRIBUIDORA DE TÍTULOS E VALORES MOBILIÁRIOS LTDA
Av. Brigadeiro Faria Lima, 1234 – 5º andar – Jd. Paulistano – São Paulo - SP - CEP: 01451-001
www.lev.com.vc

Sumário

1. Objetivo

A Política de Segurança Cibernética e da Informação ("Política") tem o objetivo de estabelecer princípios e responsabilidades que visam garantir a proteção, manutenção da privacidade, integridade, disponibilidade e confidencialidade dos dados e dos sistemas utilizados na regular atividade da LEV Distribuidora de Títulos e Valores Mobiliários Ltda. ("LEV DTVM"). Esta Política estabelece orientações quanto a execução das ações relacionadas ao tratamento das informações e uso adequado de ativos e/ou informações relacionados a LEV DTVM, aplicando medidas eficientes que protejam a LEV DTVM e seus clientes, nos termos da Resolução do Conselho Monetário Nacional ("CMN") nº 4.893, de 26 de fevereiro de 2021 ("Resolução CMN 4.893/2021").

Nos termos do art. 7º da Resolução CMN 4.893/2021, o diretor responsável pela aplicação da presente Política, inclusive no que se refere à execução do plano de ação e de resposta a incidentes, é o Diretor de Tecnologia.

Nos termos da Lei nº 13.709/2018, Lei Geral de Proteção de Dados – LGPD, tem como um de seus pilares centrais a implementação de medidas de Segurança da Informação que podem trazer às entidades públicas e privadas, uma cultura de maior conscientização na área. A LGPD considera que, mais grave do que sofrer um ataque ou passar por um vazamento de dados, é não se prevenir e nem adotar as medidas e práticas necessárias e possíveis para a proteção dos seus dados e de todos os que são afetados por eventuais acessos não autorizados.

2. Abrangência

Esta Política tem como público-alvo todos os colaboradores da LEV DTVM, sendo estes: diretores, funcionários, gerentes e estagiários que tenham vínculo empregatícios ou estatutários, diretos ou indiretos, prestadores de serviços, fornecedores e parceiros que realizem atividades em nome da ou com a LEV DTVM ("Colaboradores").

3. Definições

Colaboradores: todos os colaboradores da LEV DTVM, incluindo sócios, diretores, empregados, consultores, estagiários e todos que, de alguma forma, auxiliam o desenvolvimento das atividades;

LEV DTVM: LEV Distribuidora de Títulos e Valores Mobiliários Ltda.;

Informação: é a reunião de todo conjunto de dados e conhecimento resultante do processamento, organização e/ou organização de dados, seja ela uma representação qualitativa ou quantitativa do conhecimento (humana ou máquina) recebido;

Informação Sensível: os dados cadastrais e demais informações que permitem a identificação de clientes, suas operações e operações de custódia;

Privilégio mínimo, princípio de menor privilégio: Este preza por delegar somente os privilégios necessários para que o elemento, seja ele um colaborador ou um sistema, execute sua função junto a LEV DTVM;

Segurança da Informação: conjunto de ações e controles que tem objetivo de garantir os aspectos de confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações contribuindo com o cumprimento dos objetivos estratégicos da LEV DTVM;

Confidencialidade: O acesso informação segue o princípio de privilégio mínimo, sendo disponibilizada e divulgada somente a indivíduos, entidades ou processos autorizados de acordo com a classificação do tipo de informação;

Integridade: Deve-se haver preservação da precisão, consistência e confiabilidade das informações e sistemas no ciclo de vida da informação, mantendo-se a preservação do estado original do dado e/ou informação;

Disponibilidade: O acesso à informação deve ser garantido a parte autorizada sempre que necessário;

Conformidade: Controles, auditorias e atividades regulares de revisão dos ativos de informação, seja por titulares ou seus substitutos e por funções independentes de controle e auditoria que monitorem a conformidade dos processos, diretrizes de acordo com as políticas definidas, a fim de reportar deficiências suspeitas ou conhecidas do plano de segurança da informação;

Segregação dos Deveres e Atividades: transações inerentes ao dia a dia não devem ter a totalidade do processo pela mesma pessoa obedecendo a matriz de segregação de função e os limites impostos a cada função. Como por exemplo, uma pessoa que cria a demanda de um pagamento, não pode aprová-la;

Incidentes: Os responsáveis e mantenedores dos ativos de informação devem monitorar sistemas e processos a fim de detectar quaisquer violações ou anormalidades de segurança. Deverão ser estabelecidos processos de acordo com a severidade para reação de forma sensível e efetiva.

4. Regulamentação Aplicável

- Lei 9.609, Lei de Propriedade Intelectual de 19 de fevereiro de 1998;
- Lei 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (“LGPD”);
- Resolução do CMN nº 4.893, de 26 de fevereiro de 2021;
- Resolução da Comissão de Valores Mobiliários (“CVM”) nº 35, de 26 de maio de 2021.3;
- Programa de Qualificação Operacional BM&FBOVESPA (PQO);
- Guia de Cibersegurança ANBIMA.

5. Diretrizes Gerais

Informação é Patrimônio

Toda e qualquer informação elaborada, adquirida, manuseada, armazenada e/ou descartada pelos Colaboradores são de propriedade patrimonial da LEV DTVM. Desta forma, toda e qualquer informação deve ser utilizada somente e exclusivamente para interesses corporativos e descartada de forma segura.

Responsabilidade

Todos os Colaboradores, em qualquer vínculo, função ou nível hierárquico são responsáveis pelas informações e ativos que sejam dispostos e tenham contato, sejam eles físicos, digitais a independer da medida de segurança implantada e responsabilizados legalmente por eles.

Do Acesso à Informação

Os acessos devem ser dispostos a partir da definição de matriz de segregação e função, partindo do princípio de privilégio mínimo e garantindo que o acesso seja aprovado de acordo com a função do Colaborador e que compreenda somente as atividades designadas para completude do seu trabalho no dia a dia.

Instalação e Utilização de Software

Somente softwares homologados e autorizados pela área de TI poderão ser instalados e utilizados. É proibido o uso de softwares ilegais ou em não-conformidade com a sua licença de uso, mesmo que gratuitos. A instalação deve ser feita somente pela área de Tecnologia e aprovado pelas instâncias na empresa.

Monitoramento de Ativos

A LEV DTVM pode monitorar acesso e utilização de seus ativos tecnológicos, desde equipamentos a sistema de informação, a fim de detectar e monitorar ações que não estejam de acordo com as políticas e diretivas da empresa.

Segurança no Descarte

Os equipamentos e mídias eletrônicas devem ser destruídos de modo a não permitir a recuperação dos dados contidos. Materiais impressos com informações sensíveis ou confidenciais devem ser triturados para o descarte.

Conformidade e Práticas de Segurança da Informação

A LEV DTVM pode auditar periodicamente, práticas relacionadas à segurança da informação, por meio de auditores internos ou externos, a fim de validar se as ações de seus Colaboradores estão de acordo com as políticas da instituição e com a legislação vigente.

Acesso Físico

A LEV DTVM possui áreas restritas, sendo permitida a entrada e/ou permanência em suas dependências somente aos Colaboradores autorizados. Liberar ou facilitar o acesso de pessoa não autorizada, ainda que Colaborador da LEV DTVM, é prática vedada.

6. Diretrizes de Confidencialidade

Todas as informações que se referem a sistemas, negócios, estratégias, operações, posições ou a clientes da LEV DTVM são confidenciais e devem ser tratadas como tal, sendo utilizadas apenas para desempenhar as atribuições na instituição e sempre em benefício dos interesses desta e de seus clientes.

Toda e qualquer informação em relação aos clientes deve ser mantida na mais estrita confidencialidade, não podendo ser divulgada sem o prévio e expresso consentimento, por escrito, do cliente, salvo na hipótese de decisão judicial específica ou extrajudicialmente, em razão de procedimento de fiscalização dos órgãos reguladores.

Os Colaboradores devem evitar manter em suas mesas papéis e documentos confidenciais e manter sigilo sobre senhas do computador, rede e sistemas. Os Colaboradores devem garantir que o acesso à área de trabalho seja feito somente por pessoal autorizado.

A LEV DTVM exige que seus Colaboradores atuem buscando a garantia da confidencialidade das informações às quais tiverem acesso. Assim, é recomendável que os Colaboradores não falem a respeito de informações obtidas no trabalho em ambientes públicos, ou mesmo nas áreas comuns das dependências da instituição.

O material com informações de clientes, suas operações e posições deverá ser mantido nas dependências da LEV DTVM, sendo proibida a cópia ou reprodução (física ou eletrônica) de tais materiais, salvo mediante autorização expressa da Diretoria.

Para fins de manutenção das informações confidenciais, os Colaboradores devem (i) bloquear o computador quando estiver ausente da sua estação de trabalho; (ii) manter anotações, materiais de trabalho e outros materiais semelhantes sempre trancados em local seguro; e (iii) jamais revelar a senha pessoal de acesso aos computadores ou sistemas eletrônicos.

7. Princípios de Segurança da Informação

Define-se os princípios para ações ou linhas de implementação quanto a gestão da segurança da informação:

- A segurança da informação é diretriz principal para a LEV DTVM e deve ser tratada em nível organizacional, de acordo com as diretrizes e processos críticos de negócio. A diretoria da LEV DTVM

está ciente da importância da manutenção e constante atualização dos procedimentos de segurança da informação, estando comprometida com a melhoria contínua dos procedimentos aqui indicados;

- Os riscos devem ser quantificados e toda e qualquer decisão deve ser fundamentado nos riscos de imagem, perda financeira, vantagem competitiva, responsabilidade civil e legal, observadas os impactos à conformidade, integridade, disponibilidade e confidencialidade;

- A criação de um ambiente positivo de segurança é procedimento contínuo, estruturado e baseado em comportamento humano, observando a conscientização e maturidade de toda a cadeia responsável pela continuidade do negócio da LEV DTVM, sejam eles ativos de software ou humano, a fim de garantir a diretivas e políticas definidas pela instituição.

8. Procedimentos de Segurança da Informação

8.1. Ameaças Cibernéticas

Os invasores podem utilizar vários métodos para os ataques cibernéticos, com o objetivo de: obter ganhos financeiros; roubar manipular ou adulterar informações; obter vantagens competitivas e informações confidenciais de empresas concorrentes; fraudar, sabotar ou expor a instituição invadida, podendo ter como motivo acessório a vingança; promover ideias políticas e/ou sociais; praticar o terror e disseminar pânico e caos.

8.2. Gestão de Riscos Cibernéticos

Os riscos cibernéticos são identificados por meio de processo estabelecido para avaliação de vulnerabilidades, ameaças e impactos sobre ativos da informação da LEV DTVM. Uma vez identificada uma vulnerabilidade, é proposto pelos responsáveis, a implementação de mecanismos de proteção adequados. Os riscos cibernéticos são mapeados entre incidentes relacionados à (i) malwares, (ii) invasão de sistemas da informação, (iii) engenharia social, (iv) mau uso de sistemas da informação, (v) gestão de acessos e ativos físicos e (vi) erros sistêmicos ou humanos e estão documentados na matriz de riscos e controles de tecnologia da informação.

9. Ações de Prevenção e Proteção

Os procedimentos e controles descritos abaixo buscam reduzir a vulnerabilidade da LEV DTVM às ameaças cibernéticas, detalhadas acima, atendendo aos objetivos de segurança cibernética da instituição, nos termos do inciso II do art. 3º da Resolução CMN 4.893/2021.

- Gestão da Informação e Acessos Físicos e Lógicos

Todos os acessos, físicos ou lógicos, são submetidos ao princípio de menor privilégio. Todo acesso lógico e físico deve ser concedido e monitorado de forma que garanta o acesso somente a informação e funções necessárias para execução de seu trabalho.

- Autenticação e Uso de Senha

O colaborador é responsável por todos os atos executados através de suas credenciais, além de manter a confidencialidade dos dados e informações que tem acesso, também da troca periódica de senha de acordo com as definições de política de senha. É estritamente proibido o compartilhamento das credenciais. Também é dever do colaborador manter sua estação de trabalho bloqueada ao se ausentar da sua estação de trabalho.

- Gestão de Incidentes de Segurança da Informação

O monitoramento ativo do ambiente através de ferramentas de segurança da informação e de proteção de dados identifica possíveis ataques e sua natureza, notifica os times responsáveis e inicia um plano de ação para remediação sendo ela automática ou manual.

- Teste de Intrusão e Varredura de Vulnerabilidade

Serão realizados teste de intrusão, internos e externos, periodicamente validando a efetividade dos controles e políticas de segurança cibernética e da informação, identificando potenciais vulnerabilidades, definindo níveis de criticidade e potenciais impactos para posterior plano de ação e ações mitigatórias.

- Controle Contra Software Malicioso

Os ativos de tecnologia da LEV DTVM conectados à rede corporativa devem possuir uma solução de antivírus definida pela área de segurança da informação.

- Rastreabilidade

O escopo de acesso à LEV DTVM e seus ativos de informação deve possuir trilhas de auditorias automatizadas, capazes de registar eventos relacionados a autenticação de usuário, acesso à informação, ações executadas pelo usuário em todo o ciclo de vida de informação.

- Criptografia

As soluções de criptografia devem seguir as premissas e políticas da área de segurança da informação e em conformidade com os requisitos dos órgãos reguladores.

- Segmentação de Rede

Os servidores e computadores conectados às redes corporativas não devem ser acessíveis diretamente pela internet, o acesso a este deve ser feito através de uma conexão segura pelos métodos aprovados pelo time de segurança da informação.

As exceções a essa regra devem ser verificadas com o time de segurança da informação, que analisará e aprovará/rejeitará a solicitação a depender do requisito de negócio, do racional, dos fatores de risco e dos fatores mitigantes.

- Backup

A realização dos backups deve ser feita de forma periódica, a evitar possíveis perdas em decorrência de possíveis desastres. A periodicidade, retenção e tipo de backup devem estar alinhados à política de backup e regulamentação previstas e lei e/ou por órgãos reguladores.

- Continuidade dos Negócios

A LEV DTVM implementa o processo de continuidade de negócio de forma a garantir a redução de possíveis impactos e/ou perdas causados por incidentes que possam comprometer os processos críticos da organização. Este processo tange os processos críticos da LEV DTVM definidos pela Política de Continuidade de Negócio (PCN).

- Processamento, Armazenamento de Dados e Computação e Nuvem

A LEV DTVM assegura-se de um procedimento efetivo para aderência às regras previstas pela regulamentação em vigor, conforme Resolução CMN nº 4.893/2021.

- Prevenção de Intrusão

A LEV DTVM implementa controles de mitigação e sistemas de segurança da informação nos perímetros da rede e no ambiente de nuvem para limitar e conter o impacto de possíveis eventos de segurança cibernética.

- Prevenção de Vazamento de Informações

A LEV DTVM possui ferramentas e procedimentos para controlar a disseminação de informações sensíveis ou críticas enviadas para fora da rede da instituição. Os controles de vazamento de informações permitem a LEV DTVM proteger os dados de seus clientes e da instituição, monitorando, investigando e limitando o envio de dados não autorizados.

- Controles Específicos para Proteção de Informações Sensíveis

A LEV DTVM aplica controles de gestão de acessos, recuperação de dados, prevenção a vazamento de informações e continuidade de negócios para informações sensíveis visando manter a confidencialidade, integridade e disponibilidade destas informações.

Os procedimentos e controles acima elencados deverão ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias eventualmente empregadas nas atividades da LEV DTVM.

10. Procedimentos Internos para Tratamento de Incidentes

No caso de incidentes relacionados a segurança de sistemas, processos e informações a equipe de tecnologia realizará registro em ferramenta de gestão de incidentes, avaliação dos danos, análise da causa e do impacto e definição dos processos e controles que serão utilizados para sanar o problema e evitar maiores exposições, no que tange a riscos de imagem e perdas financeiras.

Caso seja necessário, será ativado o modo contingência conforme os procedimentos descritos no Plano de Continuidade de Negócios e Recuperação de Desastres. Após a adoção de todas as medidas necessárias, o incidente será levado à Diretoria para avaliação e, se necessária, a tomada de medidas adicionais para mitigação do risco.

Os cenários de incidentes considerados nos testes de continuidade incluem ameaças de natureza humana, tecnológica, infraestrutura, natural e física, sendo que as ameaças de natureza tecnológica abordam cenários de ataques cibernéticos que comprometam a disponibilidade dos serviços críticos da LEV DTVM.

A Diretoria avaliará o grau de relevância considerando aspectos como comprometimento de dados de clientes e impacto ao sistema financeiro. Incidentes classificados como relevantes de acordo com a Política de Gerenciamento de Incidentes devem ser comunicados aos órgãos reguladores, incluindo as providências para o reinício das atividades e relato de como foi realizada a sua implementação.

O Plano de Continuidade de Negócios e Recuperação de Desastres, que abrange o plano de ação e de resposta a incidentes da LEV DTVM, ficará à disposição do BACEN e da CVM por, ao menos, 5 (cinco) anos.

Adicionalmente, em cumprimento ao disposto no inciso VII do art. 3º e no art. 22 da Resolução CMN 4.893/2021, a LEV DTVM se dispõe a compartilhar com as demais instituições financeiras reguladas pelas diretrizes do BACEN quaisquer incidentes que eventualmente venham a ocorrer, bem como os procedimentos de contingência adotados, mediante solicitação escrita de referidas instituições financeiras, e desde que respeitados o dever de sigilo e o princípio da livre concorrência.

A atividade de adequação às regras da Lei Geral de Proteção de Dados não se resume ao emprego de medidas tecnológicas e padrões de segurança. Inclui, também, a necessidade de elaboração, manutenção e revisão de documentos que, além de garantir a adequação à citada Lei, também são medidas que podem trazer maior organização e otimização aos processos internos, bem como, proteger a Entidade e sua reputação, seus servidores, usuários dos serviços prestados e parceiros.

Na Era Tecnológica, com a popularização dos computadores pessoais e a facilidade do acesso à internet, cada vez mais se observa a dependência de processos digitais para a manutenção de modelos de negócios ou cumprimento de obrigações legais. A praticidade, redução de custos e economia de tempo, advindas da informatização dos processos, traz consigo riscos de segurança que não devem ser negligenciados. Com tempo e recursos suficientes, qualquer sistema pode ser comprometido.

Levando isso em consideração, a criação de estratégias e planos para controle de danos é essencial, e é aí que entram os Planos de Respostas a Incidentes de Segurança em Dados Pessoais.

Incidente de segurança é “uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento”.

Resposta a Incidentes é o processo que descreve como uma organização deverá lidar com um incidente de segurança, seja ele um ataque cibernético, uma violação de dados, a presença de um aplicativo malicioso (como um vírus), uma violação das políticas e padrões de segurança da entidade, dentre outros. O objetivo é minimizar os danos que poderiam ser causados pelo incidente, reduzir o tempo de ação e os custos de recuperação.

11. Tratamento e Controle de Dados

Princípios para Tratamento de Dados:

- Finalidade: É essencial que o tratamento de dados pessoais tenha uma finalidade específica que deve ser informada para o titular e o tratamento daquele dado deve se restringir a tal finalidade;
- Necessidade: A coleta daquele dado deve ser necessária para a finalidade ao qual ele se destina. Sempre coletar o mínimo de dados necessários, ou seja, coletar apenas aqueles efetivamente imprescindíveis;
- Transparência: Assegurar aos titulares informações claras, precisas e de fácil acesso a seus dados;
- Segurança: É a utilização de medidas técnicas para garantir a segurança dos dados pessoais evitando situações de incidentes de segurança;
- Prevenção: A necessidade de adoção de medidas para prevenir a ocorrência de danos aos titulares dos dados pessoais;
- Adequação: O tratamento dos dados pessoais tem que ser compatível com a finalidade para a qual eles foram coletados;
- Livre Acesso: Permitir de forma simples e gratuita o acesso dos titulares aos dados coletados, bem como a todas as informações sobre o tratamento de tais dados;e
- Qualidade dos dados: Garantir aos titulares a exatidão dos dados, mantendo esses sempre atualizados e verídicos.

12. Classificação das Informações e Dados

Esta norma descreve os processos de tratamento aplicáveis a todas as informações da LEV DTVM, independentemente dos meios nos quais elas se apresentam como, por exemplo, documentos em papel,

gravação de voz ou de outros tipos, relatórios impressos, fitas magnéticas, discos removíveis e pendrives, meio de armazenamento ótico, listagem de programas, documentação de sistemas etc.

Todas as informações e dados coletados devem ser classificados de acordo com a norma interna de classificação da informação, garantido que sejam seguidos os controles definidos para cada nível de criticidade.

A LEV DTVM adota categorias para classificação das informações, as categorias são:

RÓTULOS DE CONFIDENCIALIDADE

A informação deve ser classificada quanto ao grau de confidencialidade a está requerido através dos seguintes rótulos:

CONFIDENCIAL

Trata-se de informações críticas que podem caracterizar vantagens competitivas e estratégicas da LEV DTVM.

São informações que, se divulgadas a pessoas não autorizadas, podem causar danos extremos e significativos aos negócios e/ou à imagem da LEV DTVM.

CONFIDENCIAL COM INFORMAÇÕES SENSÍVEIS – LGPD

Trata-se de informações sobre dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, se divulgadas a pessoas não autorizadas, podem expor a empresa à riscos classificados como altos.

CONFIDENCIAL COM INFORMAÇÕES PESSOAIS - LGPD

Trata-se de informações relacionada a pessoa natural identificada ou identificável, se divulgadas a pessoas não autorizadas, podem expor a empresa à riscos classificados como médios.

INTERNA

Pode ser de conhecimento de quaisquer áreas internas da LEV DTVM.

Trata-se de informações que podem caracterizar por exemplo: metodologias; processos; procedimentos e políticas da LEV DTVM que, se divulgadas a pessoas não autorizadas, podem expor a LEV à riscos classificados como baixos.

PÚBLICA

Pode ser de conhecimento público por não oferecer ameaças aos negócios e à imagem da LEV DTVM.

Todas as informações, independentemente de sua classificação, podem ser compartilhadas com reguladores caso sejam solicitadas.

As informações classificadas como confidenciais e/ou sensíveis devem ser armazenadas em sistemas e diretórios com identificação e controle de acesso de modo a permitir o correto tratamento destas informações.

O tratamento das informações é realizado de acordo com sua classificação prevendo controles de Gestão da Informação e Acessos Físicos e Lógicos, Autenticação e Uso de Senha, Criptografia, Segmentação de Rede, Backup, Continuidade dos Negócios e Prevenção de Vazamento de Informações conforme descritos anteriormente neste documento.

13. Contratação de Serviços de Processamento e Armazenamento de Dados e Computação em Nuvem

A contratação de serviços relevantes em nuvem, ou de quaisquer prestadores de serviços que venham a manusear dados ou informações sensível e/ou que sejam relevantes para a condução das atividades da LEV DTVM, deve considerar os requisitos mínimos que a contratada deve atender durante a prestação dos serviços, que são:

- Cumprimento da legislação e da regulamentação referência à segurança cibernética e tratamento de dados em vigor, incluindo, mas não se limitando a, Resolução CMN nº 4.893/2021 e a LGPD;
- Os procedimentos e controles para acesso aos dados e às informações fornecidos pela LEV DTVM a serem processados ou armazenados pelo prestador de serviço;
- A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
- A sua aderência a certificações exigidas para a prestação do serviço a ser contratado;
- Acesso da contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
- Provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A identificação e a segregação dos dados dos clientes por meio de controles físicos/lógicos, em conformidade com a legislação e regulamentação de segurança à informação e tratamento de dados; e
- A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes.

A avaliação do cumprimento destes requisitos pelo prestador de serviços será realizada previamente a contratação e será devidamente documentada e arquivada. Após a contratação do prestador de serviços, a LEV DTVM comunicará o BACEN, em até 10 (dez) dias, nos termos do art. 14 da Resolução 4.893/2021.

Na avaliação do cumprimento dos requisitos acima elencados, a LEV DTVM considerará a criticidade do serviço e a sensibilidade dos dados e das informações que serão processados, armazenados e gerenciados, levando em conta a classificação elencada no item 12 desta política.

Adicionalmente, caso a contratação de serviços seja no exterior deve observar os seguintes requisitos:

- Existência de convênio para troca de informações entre o regulador e as autoridades supervisoras dos países onde os serviços poderão ser prestados;
- A instituição contratante deve assegurar que a prestação dos serviços referidos não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do regulador;
- A instituição contratante deve definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e
- A instituição contratante deve prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

O instrumento contratual deve ainda prever todas as cláusulas exigidas pela regulamentação em vigor do BACEN e da CVM. Adicionalmente, o contrato, bem como quaisquer documentos relacionados à contratação de terceiros, deve permanecer à disposição do BACEN e da CVM pelo prazo mínimo de 5 (cinco) anos a partir de sua extinção.

14. Atribuições e Responsabilidades

Segue abaixo tabela com a matriz de atribuições e responsabilidades da LEV DTVM:

Grupo	**Responsabilidade**
Segurança da Informação	Gerenciar, coordenar, orientar, avaliar, monitorar e implementar atividades, projetos e ações relacionadas à segurança cibernética e da informação com base no interesse da empresa;
Colaboradores	• Conhecer e cumprir as normas e orientações estabelecidas nesta Política e demais Regulamentos que compõem esta Política; • Informar as situações que comprometam a segurança das informações nas unidades organizacionais aos responsáveis do time de Segurança da Informação; • Toda informação criada, modificada no exercício das funções e qualquer informação contida em mensagens do correio eletrônico corporativo deve ser tratada como referente ao negócio da instituição; • Garantir o não compartilhamento de acessos nomeados sejam eles senha, token, ou qualquer outro tipo de acesso; • Garantir que os requisitos de Segurança da Informação constem nas aquisições e/ou implementações tecnológicas.

15. Compromisso e Penalidades

A garantida do cumprimento desta política está estabelecida formalmente com os colaboradores da empresa.

O descumprimento desta política é considerado uma falta grave, podendo acarretar sanções previstas em lei, bem como advertência, suspensão ou demissão conforme previsto em regulamentos internos e nas cláusulas contratuais.

16. Treinamento, Atualização e Divulgação

De modo a garantir o pleno conhecimento de todos os Colaboradores sobre as medidas para segurança da informação da LEV DTVM, todo Colaborador receberá, no momento da contratação, cópia desta Política. Adicionalmente, a LEV DTVM estará disponível, a qualquer tempo, a esclarecer quaisquer dúvidas que o Colaborador venha a ter acerca do conteúdo e da aplicabilidade desta Política.

A LEV DTVM providenciará treinamento aos Colaboradores que tenham acesso a dados e a informações sensíveis referente às matérias desta Política e das inovações na área de segurança cibernética e proteção de dados a serem adotadas pela instituição com frequência, no mínimo, anual a todos os Colaboradores. O respectivo treinamento será composto por uma parte conceitual e por outra dedicada à avaliação dos conhecimentos adquiridos. Para aprovação, os Colaboradores devem obter, no mínimo, 70% (setenta por cento) de acertos. Caso contrário, será exigido que o Colaborador participe novamente do treinamento.

A LEV DTVM pode escolher deixar de aplicar o treinamento em prestador de serviço que demonstre possuir procedimentos de segurança da informação e de treinamento adequados e compatíveis com esta Política.

Adicionalmente, a LEV DTVM informará seus clientes, através do seu website, acerca das precauções necessárias na utilização de produtos e serviços financeiros, disseminando suas diretrizes de segurança cibernética e proteção de tratamento de dados. As orientações abrangerão, de forma simples e resumida, no mínimo: (i) as práticas adotadas quanto aos controles de acesso lógico aplicados aos clientes e à proteção da confidencialidade das Informações Sensíveis; e (ii) cuidados a serem tomados pelos clientes com segurança cibernética no acesso aos sistemas da LEV DTVM.

17. Termo de Ciência e Confidencialidade

Colaboradores, quando de sua contratação, devem assinar o Termo de Confidencialidade presente no anexo à esta Política, pelo qual se obrigam, entre outras coisas, a proteger a confidencialidade das informações.

18. Framework de Segurança da Informação

A Política é organizada sob a forma de um framework, composto das seguintes políticas internas:

- Classificação das Informações;
- Plano de Continuidade de Negócios e Recuperação de Desastre;
- Gerenciamento de senhas;
- Uso da Internet e Correio Eletrônico;
- Gerenciamento de Ativos de Software e Hardware;
- Proteção Contra Vírus, Malware e Ransomware;
- Framework de Risco de TI;
- Gerenciamento de incidentes e problemas;
- Gerenciamento de Vulnerabilidades;
- Controle de Acesso e matriz de segregação de função/atividade;
- Gestão de acesso físico;
- Armazenamento e Recuperação de dados;
- Gestão de Mudanças;
- Acesso Remoto;
- Matriz de Riscos e Controles – Tecnologia da Informação.

19. Manutenção de Informações e Registro

Manter o termo de adesão à esta Política pelo prazo mínimo de 5 (cinco) anos.

Esta Política deverá ficar à disposição do BACEN e da CVM pelo prazo mínimo de 5 (cinco) anos.

20. Vigência e Atualizações

Esta Política entra em vigor na data de sua publicação e permanece vigente por prazo indeterminado, devendo ser testada e revisada, no mínimo, a cada 1 (um) ano.

Não obstante as revisões estipuladas, este documento poderá ser alterado sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.

21. Controle de Versões

Informações Básicas

Título	Política de Segurança Cibernética e da Informação
Versão	4
Aprovador	Diretoria
Data da elaboração	01/04/2022
Data da aprovação	30/04/2024
Data da próxima revisão	30/04/2025
Área proprietária da política	Segurança da Informação

Histórico de Versões

Versão	Motivo da Alteração	Data	Autor	Departamento
1	Versão Inicial	01/04/2022	Rodrigo Belani	Tecnologia da Informação
2	Revisão para adequação a Res. CMN 4.968	31/10/2022	Elio Makuda	Tecnologia da Informação
3	Revisão	05/04/2023	Henrique Lopes	Segurança da Informação
4	Revisão adequação termos da LEI Nº 13.709, de 14 de agosto 2018 e Classificação da Informação.	30/04/2024	HMD – Alessandro Hamada	Segurança da informação

Aprovações

Aprovações:	Marcelo Cerize	Daiane Pereira	Bruno Freitas	Anelise Cerizze
Data: 30/04/2024	Diretor	Diretora	Diretor	Diretora