POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

DLOCAL

Data 27.08.2020

Versão 01

SUMÁRIO

A. ESCOPO DESSA POLÍTICA

1. Objetivo

Esta Política de Segurança da Informação e Segurança Cibernética ("Política") tem o objetivo de estabelecer diretrizes que permitem à DLOCAL BRASIL PAGAMENTOS LTDA. ("DLOCAL") preservar e proteger as informações de seus clientes, funcionários, prestadores de serviços, partes interessadas e da própria DLOCAL contra ameaças e riscos relacionados à segurança da informação e cibernética, bem como implementar controles e procedimentos que visam a reduzir a vulnerabilidade da DLOCAL a incidentes, e também dispõe sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

A DLOCAL deve implementar e manter esta Política formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

Esta Política será compatível com:

- O porte, o perfil de risco e o modelo de negócio da DLOCAL;
- A natureza das atividades da DLOCAL e a complexidade dos produtos e serviços oferecidos;
- A sensibilidade dos dados e das informações sob responsabilidade da DLOCAL.

A DLOCAL designará diretor responsável por esta Política e pela execução do plano de ação e de resposta a incidentes.

2. Abrangência

A Política se aplica a todos os administradores, diretores e conselheiros (coletivamente "Alta Administração"), funcionários e prestadores de serviço[1] da DLOCAL (coletivamente, inclusive a Alta Administração, denominados simplesmente por "Colaboradores").

3. Normas Aplicáveis

- Circular nº 3.909, de 16 de agosto de 2018, do Banco Central do Brasil.

[1] Quaisquer terceiros que atuem em nome da DLOCAL, tais como Auditoria Externa, Assessoria Jurídica, Tecnologia da Informação, Infraestrutura de TI, dentre outras.

4. Aprovação e Revisão

Esta Política foi aprovada e revisada pela Alta Administração e será revisada periodicamente. A Política também será alterada para contemplar quaisquer alterações regulatórias e outras obrigações legais.

5. Definições

- **Ativos**: todas as formas de criação, processamento, armazenamento, transmissão e exclusão de informações. Os Ativos podem ser documentos impressos, sistemas, *softwares*, banco de dados, arquivos digitais, dispositivos móveis etc..
- **Bacen:** Banco Central do Brasil.
- **Instituição de Pagamento:** para fins desta Política, é o emissor de moeda eletrônica, cuja atividade consiste em gerenciar a conta de pagamento de usuários, utilizada para o pagamento de transações pré-pagas.
- **Log:** registro de eventos de um sistema.
- **Segurança da Informação:** conjunto de conceitos, mecanismos e estratégias que visam a proteger os Ativos da DLOCAL.
- **Segurança Cibernética:** conjunto de tecnologias e processos desenvolvidos para proteger os sistemas internos, computadores, redes e dados da DLOCAL contra ataques, danos, ameaças ou acesso não autorizado.

B. PRINCÍPIOS

A DLOCAL tem o compromisso garantir a segurança e tratamento adequado das informações. Para tanto, nossas atividades se baseiam nos seguintes princípios:

- **Confidencialidade**: garantia de que somente pessoas autorizadas terão acessos às informações e apenas quando houver necessidade;
- **Integridade**: garantia de que as informações permanecerão exatas e completas e não serão modificadas indevidamente;
- **Disponibilidade**: garantia de que a informação estará disponível às pessoas autorizadas sempre que for necessário.

C. DIRETRIZES GERAIS

Com o objetivo de garantir os objetivos desta Política, os procedimentos de Segurança da Informação e Segurança Cibernética seguirão as seguintes diretrizes:

- Assegurar que não haja acessos indevidos, modificações, destruições ou divulgações não autorizadas das informações. Para tanto, o acesso do Colaborador deve ser pessoal, intransferível e restrito aos recursos necessários para realizar suas atribuições na DLOCAL.

- Cada Colaborador, quando aplicável, receberá uma senha pessoal de acesso e ficará responsável por manter sua senha em sigilo para evitar acesso indevido às informações que estão sob sua responsabilidade. A DLOCAL adotará mecanismos que asseguram a complexidade, troca periódica e guarda de histórico de senhas.
- Qualquer risco à informação deverá ser imediatamente reportado pelo Colaborador por meio dos canais e procedimentos indicados pela DLOCAL.
- Assegurar que todas as informações sejam tratadas de maneira ética e sigilosa e que sejam adotadas medidas capazes de evitar acessos indevidos, modificações, destruições ou divulgações não autorizadas.
- Assegurar que as informações sejam utilizadas somente para a finalidade para a qual foram coletadas e que o acesso esteja condicionado à autorização.
- Assegurar que os procedimentos e controles adotados para reduzir a vulnerabilidade a incidentes e atender aos demais objetivos de Segurança Cibernética, tais como, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.
- Assegurar que os controles específicos, incluindo os voltados para a rastreabilidade da informação, garantam a segurança das informações sensíveis.
- Assegurar o registro, análise da causa e o impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades de uma Instituição de Pagamento.
- Assegurar a elaboração de cenários de incidentes considerados nos testes de continuidade dos serviços de pagamento prestados;
- Definir os procedimentos e controles voltados à prevenção e ao tratamento dos incidentes que devem ser adotados pelos prestadores serviços e terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da DLOCAL;
- Classificar os dados e as informações quanto à relevância;
- Definir os parâmetros a serem utilizados na avaliação da relevância dos incidentes;
- Assegurar os mecanismos para disseminação da cultura de segurança cibernética, incluindo:
    - A implementação de programas de capacitação e de avaliação periódica de pessoal;
    - A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos.

- Assegurar as iniciativas para compartilhamento de informações sobre os incidentes relevantes, com Instituições de Pagamento, instituições financeiras e demais instituições autorizadas a funcionar pelo Bacen.
- Assegurar o registro, análise da causa e do impacto, bem como o controle dos efeitos de incidentes de informações recebidas de empresas prestadoras de serviços a terceiros.
- Contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela DLOCAL e por esta Política.

D. PROCESSO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

A fim de assegurar que todas as diretrizes acima sejam cumpridas e que os princípios de Segurança da Informação e de Segurança Cibernética sejam devidamente seguidos, a DLOCAL adotará políticas e procedimentos para os processos elencados a seguir.

1. Gestão de ativos

Os Ativos devem ser inventariados e protegidos de acessos indevidos ou ameaças que possam comprometer o negócio. Para tanto, o acesso às salas com documentos físicos deve ser limitado, por meio de mecanismos de autenticação e autorização de acesso, destinados a impedir o acesso de indivíduos não autorizados.

Os Ativos devem ser utilizados tão somente para a finalidade devidamente autorizada. A DLOCAL deve assegurar proteção aos Ativos durante todo o seu ciclo de vida, a fim de garantir que os princípios da confidencialidade, integridade e disponibilidade sejam cumpridos integralmente.

2. Autenticação

A DLOCAL adotará mecanismos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas aos indivíduos autorizados, levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação.

3. Segmentação de rede

A DLOCAL deve adotar mecanismos internos para a segmentação de rede para proteger seus dados de ataques cibernéticos e determinar que todos os computadores conectados à rede corporativa não estejam acessíveis diretamente pela Internet.

Caso o Colaborador queira criar, alterar ou excluir regras nos *firewall* e ativos de rede deverá enviar uma requisição ao departamento de tecnologia da informação, que fará análise e aprovação.

4. Classificação da Informação

As informações devem ser classificadas segundo sua criticidade e sensibilidade para o negócio e seus clientes. Portanto, a DLOCAL deve adotar a seguinte classificação:

- **Informação Pública**: aquela que pode ser acessada por todos, sem restrição. São exemplos de Informação Pública: dados divulgados ao mercado e promocionais;
- **Informação Interna**: aquela que pode ser acessada somente por Colaboradores da DLOCAL. São exemplos de Informação Interna: normas, procedimentos e formulários da DLOCAL;
- **Informação Restrita**: aquela que pode ser acessada somente por Colaboradores que precisam dela para desempenhar suas atribuições. São exemplos de Informação Restrita: contratos e documentos estratégicos da DLOCAL.
- **Informação Confidencial**: aquela que pode ser acessada somente por Colaboradores que tenham permissão de acesso ou que necessitem dela para um propósito específico. São exemplos de Informação Confidencial: plano estratégico e informações de clientes.

5. Controle de acesso

A DLOCAL deve adotar controles de acesso em toda infraestrutura para evitar que indivíduos não autorizados tenham acesso aos ambientes segregados e aos sistemas internos. Desta forma, a DLOCAL deve implementar mecanismos para a autenticação de usuários, manutenção de segregação de funções e rastreabilidade de acesso, de forma a garantir procedimentos internos adequados e consistentes.

6. Gestão de riscos

A DLOCAL possui processo para análise de vulnerabilidades, ameaças e impactos sobre os Ativos de informação para, diante de um incidente, adotar as medidas adequadas para minimizar os danos causados.

7. Gestão de fornecedores

A DLOCAL verifica o grau de comprometimento com relação a controles de Segurança da Informação e Segurança Cibernética de todos os seus prestadores de serviços, fornecedores, provedores e parceiros que processam e armazenam dados da DLOCAL, com a finalidade de verificar o nível de maturidade dos controles de segurança e o plano de tratamento de incidentes adotados.

A DLOCAL deve disponibilizar um canal para que seus prestadores de serviços, fornecedores, provedores e parceiros comuniquem incidentes de Segurança da Informação e Segurança Cibernética que estejam relacionados às informações da DLOCAL.

8. Segurança física do ambiente

A DLOCAL deve implementar sistema para controle de acesso dos Colaboradores, prestadores de serviços, fornecedores, provedores e parceiros aos locais restritos. Os equipamentos e instalações de processamento de informação crítica ou sensível devem ser mantidos em áreas seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

9. Backup e gravação de LOG

A DLOCAL deve adotar uma rotina de backup e restauração de dados para assegurar a disponibilidade das informações relevantes para o pleno funcionamento de suas atividades.

A DLOCAL também deve realizar gravação de logs de dados que permitam a rastreabilidade do acesso e a identificação do criador, data, meios de acesos e informações acessadas. As informações dos logs devem ser protegidas contra alterações e acessos não autorizados.

10. Proteção contra vírus, arquivos e softwares maliciosos

A DLOCAL deve adotar mecanismos para prevenir que vírus e outros tipos de software e condutas maliciosas (e.g., *phishing*, *spam* etc.) se propaguem nos computadores, sistemas e servidores internos ou exponham a DLOCAL a vulnerabilidades. Para tanto, os softwares de segurança, como o antivírus, devem estar instalados e atualizados em toda a rede interna da DLOCAL.

11. Testes de varredura para detecção de vulnerabilidade

A DLOCAL se preocupa em identificar e eliminar as vulnerabilidades de seus sistemas e servidores para assegurar a integridade do ambiente dos processos de negócio. Para tanto, deve promover monitoramento constante e condução de testes e varredura para detecção de vulnerabilidades, avaliação de riscos e determinação de medidas de correção adequadas.

12. Criptografia

Os Ativos de informação da DLOCAL devem possuir criptografia adequada, a fim de se garantir proteção em todo o ciclo de vida da informação, em conformidade com os padrões de segurança dos órgãos reguladores.

13. Plano de continuidade

A DLOCAL realiza plano de continuidade dos serviços prestados a partir da adoção de um conjunto preventivo de estratégias e planos de ação para garantir que os serviços essenciais da DLOCAL sejam devidamente identificados e preservados após a ocorrência de uma contingência.

Para tanto, a DLOCAL realizará o mapeamento de processos críticos, análise de impacto nos negócios e inventário dos cenários de crises cibernéticas relacionados aos incidentes de segurança.

Devem ser aplicados testes de continuidade de serviços de pagamento e realização testes periódicos para garantir a eficácia e segurança dos processos. O teste deve ser conduzido em um ambiente controlado que permita que a DLOCAL certifique a conformidade dos planos desenvolvidos com os objetivos da DLOCAL e requisitos legais.

14. Incidentes de segurança

a. Classificação de relevância dos incidentes

A DLOCAL classificará os incidentes de segurança segundo sua relevância e conforme a classificação das informações envolvidas e o impacto na continuidade dos negócios da DLOCAL.

b. Gestão de incidentes

Todos os incidentes ou suspeita de incidentes identificados por um Colaborador, cliente, prestador de serviços, fornecedor, provedor ou parceiro devem ser imediatamente comunicados à área responsável. A comunicação deverá ser feita por meio dos canais indicados pela DLOCAL. [caso a DLOCAL já tenhas esses canais, fornecer aqui os detalhes sobre o canal para comunicar incidentes – e-mail, telefone].

Os incidentes reportados serão classificados segundo o risco que representam para a DLOCAL e o impacto na continuidade dos negócios da DLOCAL. Além disso, devem ser devidamente registrados, tratados e comunicados.

A DLOCAL adotará procedimentos para mitigar os efeitos dos incidentes relevantes e a interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados.

Caso haja incidentes relevantes ou interrupção dos serviços relevantes, a DLOCAL comunicará o Bacen e adotará medidas necessárias para que as suas atividades sejam reiniciadas.

c. Plano de compartilhamento de incidentes

Sem prejuízo do dever de sigilo e da livre concorrência, a DLOCAL deve adotar iniciativas para o compartilhamento de informações sobre incidentes relevantes com outras Instituições de Pagamento por meio dos canais adotados pelas instituições.

As informações compartilhadas também estarão disponíveis ao Bacen.

d. Plano de ação e resposta a incidentes

A DLOCAL estabelecer deve estabelecer plano de ação e de resposta a incidentes visando à implementação desta Política, que abrange, minimamente:

- As ações a serem desenvolvidas para adequar as estruturas organizacional e operacional às diretrizes desta Política;
- As rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes.

e. Relatório anual de incidentes

A DLOCAL deve elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro. O relatório abordará:

- A efetividade da implementação das ações de adequação suas estruturas organizacional e operacional;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes desta Política;
- Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;
- Os resultados dos testes de continuidade dos serviços de pagamento prestados, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório anual de incidentes deve ser apresentado ao Conselho de Administração ou, na sua inexistência, à Diretoria da DLOCAL até 31 de março do ano seguinte ao da data-base.

15. Mecanismos de rastreabilidade

A DLOCAL deve adotar controles específicos para promover a rastreabilidade da informação, principalmente que busquem garantir a segurança das informações sensíveis.

16. Registro de impacto

A DLOCAL deve realizar registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da DLOCAL, que devem abranger inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

17. Treinamentos e conscientização

A DLOCAL preza por uma cultura de Segurança da Informação e Segurança Cibernética. Dessa forma, devem ser adotados políticas e procedimentos para a difusão dos princípios e diretrizes integrantes desta Política, garantindo-se a capacitação e conscientização para todos os seus Colaboradores.

A DLOCAL promoverá a ampla divulgação desta Política a todos os seus Colaboradores e o público em geral, bem como às empresas prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações, incluindo a prestação de informações aos usuários finais sobre medidas de precaução para a utilização dos produtos e serviços oferecidos.

Além disto, a Alta Administração da DLOCAL deverá difundir a cultura de Segurança da Informação e Segurança Cibernética para promover melhorias contínuas em seus processos internos, a fim de evitar quaisquer incidentes relacionado à Segurança da Informação e Segurança Cibernética.

18. Contratação de serviços de processamento e armazenamento de dados e computação em nuvem

a. Seleção de terceiros

O processamento e armazenamento de dados e computação em nuvem será realizado por meio de terceiros localizados no Brasil ou no exterior. A contratação de terceiros deve ser realizada por meio da aferição da capacidade do prestador de serviço para realizar as atividades em cumprimento com a legislação e regulamentação aplicável. Desta forma, a DLOCAL deve adotar procedimentos para verificação da capacidade do potencial prestador de serviço de forma a assegurar:

- O cumprimento da legislação e da regulamentação em vigor;
- O acesso da DLOCAL aos dados e às informações 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 aderência do prestador de serviço a certificações exigidas pela DLOCAL para a prestação do serviço a ser contratado;

- O acesso da DLOCAL 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;
- O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A identificação e a segregação dos dados dos usuários finais da DLOCAL por meio de controles físicos ou lógicos;
- A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da DLOCAL.

Na avaliação da relevância do serviço a ser contratado, a DLOCAL também deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado. Todos os procedimentos devem ser documentados.

Ademais, a DLOCAL deve adotar recursos e medidas necessários para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações e uso dos recursos providos pelo potencial prestador de serviços.

b. Execução de aplicativos pela internet

No caso da execução de aplicativos por meio da internet, a DLOCAL deve assegurar que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

c. Serviços de computação em nuvem

Os serviços de computação em nuvem disponibilizados à DLOCAL, sob demanda e de maneira virtual, deverão incluir um ou mais serviços conforme descritos abaixo:

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à DLOCAL implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela DLOCAL ou por ela adquiridos;
- Implantação ou execução de aplicativos desenvolvidos pela DLOCAL, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços;
- Execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

A DLOCAL é responsável, em conjunto com o prestador de serviços, pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada pela DLOCAL ao Bacen, nos termos da legislação em vigor.

d. Contratação de serviços de computação em nuvem no exterior

Em caso de contratação de serviços de processamento, armazenamento de dados e de computação em nuvem no exterior, a DLOCAL deverá observar os seguintes requisitos:

- Existência de convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países onde os serviços serão prestados;
- Verificação de que a prestação dos serviços não causará prejuízos ao seu regular funcionamento nem embaraço à atuação do Bacen;
- Definição dos países e regiões em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados. Essa definição deverá ocorrer antes da contratação dos serviços;
- Previsão de alternativas para a continuidade dos serviços de pagamento prestados, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

Caso não haja convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países em que os serviços serão prestados, a DLOCAL solicitará autorização do Bacen para a contratação do serviço. O prazo para solicitar autorização é de 60 dias anteriores à contratação. Caso haja alterações contratuais que impliquem em modificação das informações, a DLOCAL deverá solicitar autorização 60 dias antes da alteração contratual.

A DLOCAL deve assegurar que a legislação e a regulamentação nos países em que os serviços serão prestados não restrinjam ou impeçam o acesso da DLOCAL e do Bacen aos dados e às informações. A comprovação do atendimento aos requisitos e o cumprimento desta exigência deverão ser documentados.

e. Contrato de prestação de serviços

A DLOCAL deve assegurar que os contratos de prestação de serviços de processamento, armazenamento de dados e computação em nuvem prevejam:

- A indicação dos países e da região em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados;
- A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
- A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos usuários finais;

- Em caso de extinção do contrato, a obrigatoriedade de transferência dos dados ao novo prestador de serviços ou à DLOCAL, bem como a exclusão dos dados pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos.
- O acesso da DLOCAL às informações fornecidas pela empresa contratada; bem como as informações relativas às certificações e aos relatórios de auditoria especializada e informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A obrigação da empresa contratada notificar a DLOCAL sobre a subcontratação de serviços relevantes para a DLOCAL;
- A permissão de acesso do Bacen aos contratos e acordos firmados para a prestação de serviços, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso aos dados e informações;
- A adoção de medidas pela DLOCAL, em decorrência de determinação do Bacen;
- A obrigação de a empresa contratada manter a DLOCAL permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

Em caso de decretação de regime de resolução da DLOCAL pelo Bacen, o contrato de prestação de serviços deve prever:

- A obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, acordos, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso, que estejam em poder da empresa contratada;
- A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços. A notificação deverá ocorrer com 30 dias de antecedência da data prevista para a interrupção dos serviços prestados e deverá determinar que:
    - A empresa contratada se obriga a aceitar eventual pedido de prazo adicional de 30 dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;
    - A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da DLOCAL.

f. Comunicação ao Bacen

A comunicação ao Bacen deve conter as seguintes informações:

- O nome da empresa a ser contratada;
- Os serviços relevantes a serem contratados;
- No caso de contratação no exterior, indicação dos locais onde os serviços serão prestados e os dados armazenados, processados e gerenciados.

O prazo para comunicação é de 10 dias, contados a partir da contratação dos serviços. Caso haja alterações contratuais que impliquem em modificação das informações, a comunicação ao Bacen deverá ocorrer em 10 dias contados da alteração contratual, salvo na hipótese prevista no item 18 “d”.

19. Continuidade dos serviços de pagamento

No tocante à continuidade dos serviços de pagamento prestados, a DLOCAL deve assegurar:

- O tratamento dos incidentes relevantes relacionados com o ambiente cibernético;
- Os procedimentos a serem seguidos no caso de interrupção de serviços de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a substituição da empresa contratada e o reestabelecimento da operação normal da DLOCAL;
- Os cenários de incidentes considerados nos testes de continuidade de serviços de pagamento prestados.
- O tratamento para mitigar os efeitos dos incidentes relevantes da interrupção dos serviços de processamento, armazenamento de dados e de computação em nuvem contratados;
- O prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos;
- A comunicação tempestiva ao Bacen das ocorrências de incidentes relevantes e das interrupções dos serviços, que configurem uma situação de crise pela DLOCAL, bem como das providências para o reinício das suas atividades.

A DLOCAL deve instituir mecanismos de acompanhamento e de controle visando a assegurar a implementação e a efetividade desta Política, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Os mecanismos de acompanhamento e controle devem incluir a definição de processos, testes e trilhas de auditoria, bem como a definição de métricas e indicadores adequados e a identificação e a correção de eventuais deficiências.

20. Arquivamento de informações

A DLOCAL deve armazenar, pelo prazo de 5 anos, as seguintes informações:

- O documento relativo à política de Segurança Cibernética;
- A ata de reunião do Conselho de Administração, se existente, e de reunião da Diretoria da DLOCAL;
- O documento relativo ao plano de ação e de resposta a incidentes;
- O relatório anual;
- A documentação sobre os procedimentos desta Política;
- A documentação no caso de serviços prestados no exterior;
- Os contratos de prestação de serviços mencionados nesta Política;
- Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e controle, a partir da implementação dos mecanismos mencionados.

E. DECLARAÇÃO DE RESPONSABILIDADE

Os Colaboradores e prestadores de serviço da DLOCAL devem aderir formalmente a um termo em que se comprometem a agir de acordo com esta Política. Ademais, todos os contratos da DLOCAL devem possuir cláusula que assegure a confidencialidade das informações.

F. DISPOSIÇÕES GERAIS

Esta Política está acompanhada de um Termo de Adesão à Política de Segurança da Informação e Segurança Cibernética e Termo de Adesão às Alterações da Política de Segurança da Informação e Segurança Cibernética, que deverão ser assinados por todos os Colaboradores, prestadores de serviços, fornecedores, provedores e parceiros.

Esta Política está disponível em local acessível a todos Colaboradores, em linguagem clara e acessível. É possível acessá-la no site www.dlocal.com

ANEXO I

TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Eu, _____, inscrito no CPF sob o n. _____, declaro ter conhecimento desta Política Segurança da Informação e Segurança Cibernética, bem como das diretrizes contidas nas demais políticas, normas e procedimentos internos da [DLOCAL].

Declaro ainda ter conhecimento de que, diante de um incidente de segurança ou ameaça de incidente, devo comunicar imediatamente à área responsável por meio do [incluir mecanismo de reporte].

_____ /_____ /_____

Data

_____

Assinatura

ANEXO II

TERMO DE ADESÃO ÀS ALTERAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Eu, _____, inscrito no CPF sob o n. _____, declaro ter conhecimento das alterações da Política Segurança da Informação e Segurança Cibernética, bem como das diretrizes contidas nas demais políticas, normas e procedimentos internos da [DLOCAL].

Declaro ainda ter conhecimento de que, diante de um incidente de segurança ou ameaça de incidente, devo comunicar imediatamente à área responsável por meio do [incluir mecanismo de reporte].

_____ /_____ /_____

Data

_____

Assinatura