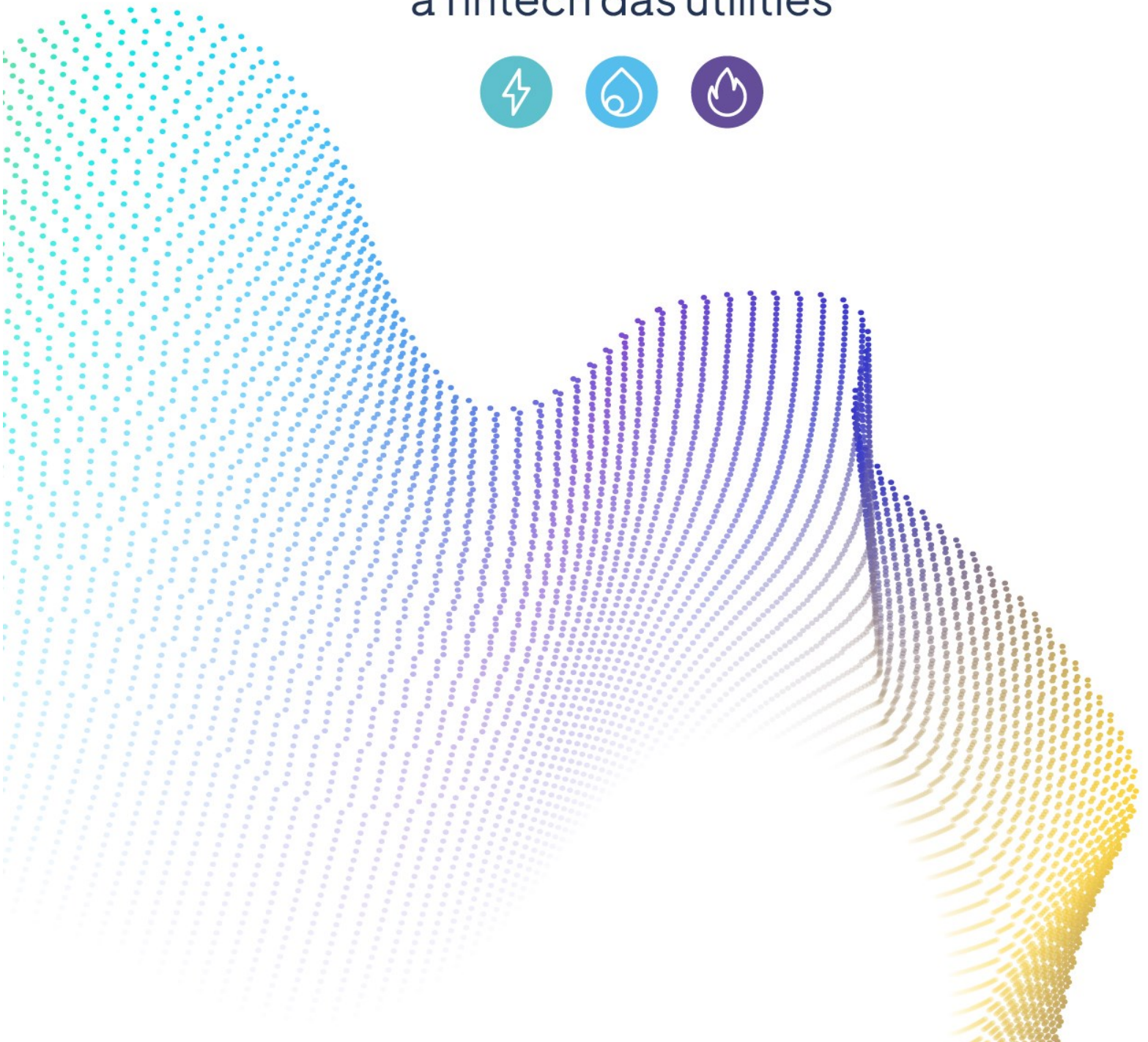
POLÍTICA INTERNA

SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Flexpag®

a fintech das utilities



1. OBJETIVO DA POLÍTICA

Esta Política de Segurança da Informação e Segurança Cibernética ("Política") tem o objetivo de estabelecer diretrizes que permitem a **FLEXPAG TECNOLOGIA E INSTITUIÇÃO DE PAGAMENTO S.A**. preservar e proteger as informações de seus clientes, funcionários, prestadores de serviços, partes interessadas e da própria FLEXPAG contra ameaças e riscos relacionados à segurança da informação e cibernética, bem como implementar controles e procedimentos que visam a reduzir a vulnerabilidade da FLEXPAG 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 FLEXPAG implementa e mantém esta Política formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade, a disponibilidade, a autenticidade e o não repúdio dos dados e dos sistemas de informação utilizados.

Esta Política será compatível com:

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

A FLEXPAG possui diretor responsável por esta Política e pela execução do plano de ação e de resposta a incidentes, assim como, um comitê para tratar de assuntos relacionados à segurança cibernética e privacidade dos dados.

2. ABRANGÊNCIA DA POLÍTICA

A Política se aplica a todos os administradores e diretores (coletivamente "Alta Administração"), funcionários e prestadores de serviço da FLEXPAG (coletivamente denominados simplesmente por "Colaboradores").

3. NORMAS APLICÁVEIS

RESOLUÇÃO BCB Nº 85/2021: Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil.

RESOLUÇÃO BCB Nº 150/2021: Consolida normas sobre os arranjos de pagamento, aprova o regulamento que disciplina a prestação de serviço de pagamento no âmbito dos arranjos de pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB), estabelece os critérios segundo os quais os arranjos de pagamento não integrarão o SPB e dá outras providências.

LEI FEDERAL Nº 13.709/2018: Lei Geral de Proteção de Dados Pessoais (LGPD).

4. TERMOS E DEFINIÇÕES

ACESSO: Ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique.

ANTIVÍRUS: é um software que identifica e protege os dispositivos de malwares, também conhecidos como vírus.

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.

AUTENTICIDADE: possibilidade de identificar e autenticar usuários, entidades, sistemas ou processos com acesso à informação.

BACEN: Banco Central do Brasil.

CONTROLE DE ACESSO: Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação.

CRIPTOGRAFIA: é um conjunto de técnicas pensadas para proteger uma informação de modo que apenas o emissor e receptor consigam compreendê-la.

FIREWALL: Dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.

GESTÃO DE ATIVOS: são as boas práticas utilizadas pela FLEXPAG em seu processo de controle de ativos tangíveis e intangíveis (equipamentos, contratos, marcas, ferramentas e materiais, know-how), que buscam alcançar um resultado desejado e sustentável para a operação.

HARDENING: Consiste na utilização de técnicas para prover mais segurança a servidores que disponibilizam serviços externos, como servidores Web, ou até mesmo serviços internos, como servidores de banco de dados, de arquivos, entre outros.

INFORMAÇÕES SENSÍVEIS: Que tem valor estratégico para o desenvolvimento das operações da FLEXPAG, ganhando tangibilidade por meio de transações financeiras, produção, entre outras formas, e que serão tratados com base no legítimo interesse da FLEXPAG, estritamente necessários para a finalidade pretendida nos termos desta Política.

INSTITUIÇÃO DE PAGAMENTO: para fins desta Política, é a FLEXPAG como 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.

MUDANÇA: adição, modificação ou remoção de qualquer item (hardware ou software) que possa afetar um ou mais serviços de TI.

NÃO REPÚDIO (IRREVOGABILIDADE): possibilidade de evitar o repúdio ou a negativa de autoria posterior de transações legítimas por parte de usuários.

PCI DSS (*PAYMENT CARD INDUSTRY DATA SECURITY STANDARD*): Padrão de Segurança de Dados da Indústria de Pagamento com Cartão. O PCI DSS é composto por um conjunto de requerimentos e procedimentos de segurança cujo objetivo é proteger as informações pessoais dos titulares de cartão e, portanto, reduzir o risco de roubo de dados de cartão ou fraude.

SEGURANÇA DA INFORMAÇÃO: conjunto de conceitos, mecanismos e estratégias que visam a proteger os Ativos da FLEXPAG.

SEGURANÇA CIBERNÉTICA: conjunto de tecnologias e processos desenvolvidos para proteger os sistemas internos, computadores, redes e dados da FLEXPAG contra-ataques, danos, ameaças ou acesso não autorizado.

SUBCREDENCIADOR: para fins desta Política, é a FLEXPAG como participante de arranjos de pagamento, que possui autorização de uma ou mais credenciadoras para credenciar os Estabelecimentos e realizar a liquidação das transações, habilitando-os para realizar transações com cartões.

5. ATRIBUIÇÕES, RESPONSABILIDADES E COMPETÊNCIAS

5.1. ALTA ADMINISTRAÇÃO

Formada por todos os administradores e diretores (coletivamente "Alta Administração"), possuem como responsabilidades:

i. Prover recursos para a implementação, manutenção e melhoria da gestão da segurança da informação e segurança cibernética;
ii. Prover comprometimento e apoio à aderência a política de segurança cibernética e da informação de acordo com os objetivos e estratégias de negócio estabelecidas para organização;
iii. Fornecer às áreas de Tecnologia e Infraestrutura de Tecnologia da Informação direcionamento, apoio, recomendação e apontar restrições sempre que necessário.

5.2. DIRETORIA DE TECNOLOGIA

Presidente do Comitê De Segurança Cibernética e Privacidade dos Dados, responsável pela implementação, execução e manutenção da política, assim como, pela convocação das reuniões periódicas do Comitê**.**

5.3. COMITÊ DE SEGURANÇA CIBERNÉTICA E PRIVACIDADE DOS DADOS

Formado por colaboradores indicados pelas respectivas áreas da FLEXPAG, com o objetivo de compreender, obter informações e aconselhar o Diretor de Tecnologia e a alta administração a respeito de assuntos relacionados à segurança cibernética e privacidade dos dados. Assim deve:

i. Apoiar na disseminação e conscientização da segurança da informação;
ii. Solicitar ao Diretor de Tecnologia e à Alta Administração a disponibilização de recursos necessários para que ações de segurança da informação e privacidade dos dados sejam executadas;
iii. Acompanhar de perto as atividades do Diretor de Tecnologia na coordenação da atualização da Política, propondo, quando necessário, revisões e novas políticas complementares, bem como procedimentos que assegurem o controle das ações da política.

5.4. GESTORES DAS ÁREAS

Formado pelos colaboradores que exercem a gestão de área na FLEXPAG, responsáveis pela informação e privacidade dos dados em sua área de competência. Assim devem:

i. Gerenciar as informações sob sua competência;
ii. Autorizar os colaboradores a ter ou não acesso às informações sob sua competência;

iii. Informar o desligamento dos colaboradores de sua respectiva área ou setor;

iv. Indicar a classificação da informação sob sua competência, de modo a estabelecer como essas informações podem ser acessadas e administradas, garantindo a segurança da acessibilidade e disponibilidade destas. Garantir que seus subordinados tenham acesso e conhecimento desta política e demais normas e padrões de segurança da informação;

v. Avaliar periodicamente o grau de sigilo e segurança necessários para a proteção das informações sob sua responsabilidade e de sua equipe;

vi. Acionar as áreas competentes para a aplicação das penalidades, cabíveis aos Colaboradores que violarem o código de ética e conduta, a política de segurança cibernética e da informação e as normas da FLEXPAG;

vii. Autorizar acessos de seus colaboradores apenas quando forem realmente necessários.

5.5. EQUIPE TÉCNICA DE TI

Formada por colaboradores da área de Tecnologia da Informação e Infraestrutura de Tecnologia da Informação, a fim de:

i. Manter o ambiente tecnológico estável, operacional, atualizado, íntegro, disponível e monitorado;

ii. Elaborar e atualizar os procedimentos relativos à operacionalidade do ambiente tecnológico garantindo a segurança cibernética e a privacidade dos dados;

iii. Instalar e configurar os ativos de software e hardware necessários à operacionalidade do ambiente tecnológico;

iv. Relatar mensalmente ao Comitê ou representante indicado os incidentes de Segurança da Informação identificados, ocorridos no ambiente tecnológico;

v. Conduzir a gestão de incidentes de segurança da informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;

vi. Conduzir a definição de controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades;

vii. Propor projetos e iniciativas para melhoria do nível de segurança das informações;

viii. Conduzir a gestão dos acessos a sistemas e informações da Flexpag;

ix. Garantir a continuidade dos serviços tecnológicos de forma a atender aos requisitos essenciais do negócio;

x. Equipe responsável pelo tratamento dos incidentes: seguranca@flexpag.com
   - Wagner Sandres (Gerente de Infraestrutura);
   - Júlio Oliveira (Analista Cyber Security);
   - Erwin Julius (Gerente de Desenvolvimento);

xi. Responsável pela administração das contas dos usuários:
   - Júlio Oliveira (Analista Cyber Security) - seguranca@flexpag.com;

xii. Responsável pela monitoria de acesso aos dados de cartão:
   - Júlio Oliveira (Analista Cyber Security) - seguranca@flexpag.com.

5.6. USUÁRIOS

Clientes, funcionários, prestadores de serviços, partes interessadas ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura ou as informações da FLEXPAG, no que couber e que devem:

i. Cumprir as normas e procedimentos relacionados ao uso de informações e sistemas associados, em conformidade com o estabelecido nesta política;

ii. Informar, imediatamente, às áreas responsáveis, qualquer falha em dispositivo, serviço ou processo relacionado à Segurança da Informação e/ou privacidade dos dados, para que sejam tomadas ações urgentemente;
iii. Assinar 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
iv. Utilizar as informações como patrimônio da FLEXPAG e mantê-las seguras, íntegras e disponíveis, conforme sua classificação.

5.7. GENTE &GESTÃO

Verificar o histórico de candidatos a emprego, de acordo com a ética e leis vigentes.

Garantir que a política, normas e procedimentos da política de segurança cibernética e da informação sejam divulgados nos processos de admissão/integração de novos colaboradores e reciclagens a todos da alta administração, colaboradores, prestadores de serviços e parceiros de negócios da Flexpag.

5.8. FORNECEDORES E PARCEIROS DE NEGÓCIOS

Cumprir as determinações da política, normas e procedimentos publicados pela Flexpag.

Orientar os funcionários da empresa sobre o cumprimento das determinações da política, normas e procedimentos publicados pela Flexpag.
Cumprir com o acordo de confidencialidade.

6. PRINCÍPIOS

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

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

7. DIRETRIZES GERAIS

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

a) 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 FLEXPAG.
b) Cada Colaborador receberá uma senha pessoal de acesso e ficará responsável por mantê-la em sigilo, para evitar acesso indevido às informações que estão sob sua responsabilidade. A FLEXPAG deve adotar mecanismos que assegurem a complexidade, troca periódica e guarda de histórico de senhas.
c) Qualquer risco à informação deve ser imediatamente reportado pelo Colaborador por meio dos canais e procedimentos indicados pela FLEXPAG.
d) 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.
e) Assegurar que as informações sejam utilizadas somente para a finalidade para a qual foram coletadas e que o acesso esteja condicionado à autorização.

f) Assegurar que os procedimentos e controles adotados para reduzir a vulnerabilidade a incidentes de segurança e atender aos demais objetivos de Segurança Cibernética, tais como: autenticação, criptografia, prevenção e detecção de intrusão, prevenção de vazamento de informações, realização periódica de testes e varreduras para detecção de vulnerabilidades, proteção contra softwares maliciosos, rastreabilidade, controles de acesso, segmentação da rede de computadores e manutenção de cópias de segurança dos dados e das informações.

g) Assegurar que os controles específicos, incluindo os voltados para a rastreabilidade da informação, garantam a segurança das informações sensíveis.

h) Assegurar o registro, análise da causa e o impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da FLEXPAG.

i) Assegurar a elaboração de cenários de incidentes considerados nos testes de continuidade dos serviços de pagamento prestados;

j) 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 FLEXPAG;

k) Classificar os dados e as informações quanto à relevância;

l) Definir os parâmetros a serem utilizados na avaliação da relevância dos incidentes;

m) Assegurar mecanismos para disseminação da cultura de segurança cibernética, incluindo a implementação de programas de capacitação e de avaliação periódica de pessoal;

n) Prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos.

o) Assegurar iniciativas para compartilhamento de informações sobre os incidentes relevantes, com Instituições de Pagamento, instituições financeiras e demais instituições autorizadas a funcionar pelos órgãos reguladores.

p) 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.

q) Contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela FLEXPAG e por esta Política.

8. PROCESSO DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

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

8.1. GESTÃO DE ATIVOS

Trata da definição dos padrões para que os ativos de tecnologia da informação da FLEXPAG, estabelecendo as responsabilidades para a proteção e divulgação da gestão dos ativos da informação, por meio da manutenção de inventários, além de assegurar que o ciclo de vida dos ativos seja realizado e gerenciado para garantir a Segurança da Informação e o atendimento às legislações, normas e boas práticas recomendadas.

8.2. AUTENTICAÇÃO E USO DE SENHAS

Estabelecer um padrão de configuração sistêmica para criação e utilização de senhas fortes, no intuito de evitar que pessoas mal-intencionadas as descubram e se passem por outras pessoas, acessando contas de correio eletrônico, ambiente de rede, sistemas, entre outros e bloqueiem, alterem, deletem ou capturem informações privilegiadas da FLEXPAG, como se proprietário fosse e isso venha a comprometer o

negócio, os parceiros ou a integridade de todos que direta ou indiretamente utilizam os sistemas, infraestrutura ou informações da FLEXPAG.

8.3. SEGMENTAÇÃO DE REDE – *HARDENING*

Tem como objetivo definir padrões de segurança e de conformidade técnica através de um processo periódico de identificação de padrões seguros de tecnologia no ambiente computacional da FLEXPAG, conforme padrões estabelecidos pelo PCI (*Payment Card Industry*).

8.4. CLASSIFICAÇÃO DA INFORMAÇÃO

i. **Informação Pública:** aquela que pode ser acessada por todos, sem restrição. São exemplos de Informação Pública: dados divulgados ao mercado e promocionais;

ii. **Informação Interna:** aquela que pode ser acessada somente por Colaboradores da FLEXPAG. São exemplos de Informação Interna: normas, procedimentos e formulários da FLEXPAG;

iii. **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 FLEXPAG.

iv. **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.

8.5. CONTROLE DE ACESSO

Trata-se de controles de identificação, autenticação e autorização para salvaguardar as informações da FLEXPAG, a fim de evitar a quebra da segurança da informação e

quaisquer acessos não autorizados que implique em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Os controles de autorização, identificação e autenticação garantem que apenas usuários autorizados tenham acesso ou façam uso dos sistemas de informação da Flexpag.

8.6. GESTÃO DE RISCOS E VULNERABILIDADES

A Flexpag estabelece as regras relacionadas às atividades de identificação, avaliação, documentação, gestão, comunicação e remediação de vulnerabilidades. Além disso, contempla ações e boas práticas que devem ser observadas para se evitar que vulnerabilidades estejam presentes nos ativos da Flexpag. A revisão, a avaliação, a aplicação e a verificação das atualizações de ativos de informação auxiliam a mitigar as vulnerabilidades no ambiente de Tecnologia da Informação e Telecomunicações, bem como os riscos associados a tais vulnerabilidades.

8.7. GESTÃO DE FORNECEDORES

A FLEXPAG deve verificar 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 seus dados, com a finalidade de verificar o nível de maturidade dos controles de segurança e o plano de tratamento de incidentes adotados.

A FLEXPAG disponibiliza um canal para que seus prestadores de serviços, fornecedores, provedores e parceiros, comuniquem incidentes de Segurança da Informação e Segurança Cibernética, através do e-mail seguranca@flexpag.com .

8.8. BACKUP E GRAVAÇÃO DE LOG

A FLEXPAG adota padrões para geração, manuseio, armazenamento e descarte de registros (logs) de segurança e atividades de monitoração. Durante a execução de procedimentos em sistema, ocorrem eventos, que são ações de um usuário, como acesso, download ou troca de informações. Dessa forma para registro desses acontecimentos são usados os arquivos de logs.

O gerenciamento de logs é necessário em virtude da necessidade de controle de informações úteis, armazenando de modo seguro o arquivo que guarda todos os registros de logs.

8.9. PROTEÇÃO CONTRA VÍRUS, ARQUIVOS E SOFTWARES MALICIOSOS – ANTIVÍRUS

A FLEXPAG adota regras para o uso de solução de antivírus nos equipamentos de propriedade da Flexpag, com o intuito de detectar programas maliciosos. Para tanto, a Flexpag deve assegurar que todos os computadores que estão na rede da Flexpag possuam os softwares de proteção contra códigos maliciosos instalados e atualizados.

8.10. ATUALIZAÇÃO DE SEGURANÇA NO PARQUE TECNOLÓGICO

A FLEXPAG adota processo de atualização periódica de segurança no parque tecnológico, de forma a prevenir vulnerabilidades que possam ocasionar brechas de segurança para ataque de vírus e outros tipos de software, que se propaguem nos computadores, sistemas e servidores da FLEXPAG.

São implementados processos de Gerenciamento de Mudança, focados em reduzir riscos e maximizar a capacidade da Flexpag integrar novas ferramentas ao ambiente de trabalho, com vistas a assegurar que todas as solicitações de mudanças sejam registradas, autorizadas, documentadas e controladas.

8.11. TESTES DE VARREDURA PARA DETECÇÃO DE VULNERABILIDADE

A FLEXPAG 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 periódica de testes e varredura para detecção de vulnerabilidades, avaliação de riscos e determinação de medidas de correção adequadas.

8.12. CRIPTOGRAFIA

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

9. PLANO DE CONTINUIDADE

A FLEXPAG adota um plano de continuidade dos serviços prestados a partir da implementação de um conjunto preventivo de estratégias e planos de ação para garantir que os serviços essenciais da FLEXPAG sejam devidamente identificados e preservados após a ocorrência de um sinistro.

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

Periodicamente, são aplicados testes de continuidade nos sistemas críticos da FLEXPAG, para garantir a eficácia e segurança dos processos. O teste deve ser conduzido em um ambiente controlado que permita que a FLEXPAG se certifique da conformidade dos planos e processos desenvolvidos para atender os critérios mínimos de segurança e proteção de dados e requisitos legais.

10. INCIDENTES DE SEGURANÇA

10.1. CLASSIFICAÇÃO DA RELEVÂNCIA DO INCIDENTE

A FLEXPAG deve classificar os incidentes de segurança, segundo sua relevância, conforme a classificação das informações envolvidas e o impacto na continuidade dos negócios.

10.2. 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 FLEXPAG.

Os incidentes reportados devem ser classificados segundo o risco que representam e o impacto na continuidade dos negócios, além de, serem devidamente registrados, tratados e comunicados.

A FLEXPAG deve adotar procedimentos, para mitigar os efeitos dos incidentes e 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 FLEXPAG deve comunicar aos órgãos reguladores e adotar medidas necessárias para que as suas atividades sejam reiniciadas.

10.3. PLANO DE COMPARTILHAMENTO DE INCIDENTES

Sem prejuízo do dever de sigilo e da livre concorrência, a FLEXPAG 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 devem estar disponíveis aos órgãos reguladores.

10.4. PLANO DE AÇÃO E RESPOSTA À INCIDENTES

A FLEXPAG estabelece através do plano de ação e de resposta a incidentes visando à implementação desta Política, que abrange, minimamente:

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

10.5. RELATÓRIO ANUAL DE INCIDENTES

A FLEXPAG 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:

i. A efetividade da implementação das ações de adequação suas estruturas organizacional e operacional;
ii. 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;
iii. Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;
iv. 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 FLEXPAG até 31 de março do ano seguinte ao da data-base.

11. MECANISMO DE RASTREABILIDADE

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

12. REGISTRO DE IMPACTO

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

13. TREINAMENTO E CONSCIENTIZAÇÃO

A FLEXPAG preza por uma cultura de Segurança da Informação e Cibernética e Privacidade dos Dados. Dessa forma, devem ser adotados programas de treinamentos e conscientização relacionados as políticas e procedimentos para a difusão dos princípios e diretrizes integrantes desta Política, para todos os colaboradores.

Periodicamente a FLEXPAG deve promover 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 deverá difundir a cultura de Segurança da Informação e Cibernética e privacidade dos dados para promover melhorias contínuas em seus processos internos, a fim de evitar quaisquer incidentes relacionados à segurança.

14. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

14.1. 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 FLEXPAG deve adotar procedimentos para verificação da capacidade do potencial prestador de serviço de forma a assegurar:

i. O cumprimento da legislação e da regulamentação em vigor;
ii. O acesso da FLEXPAG aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
iii. A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
iv. A aderência do prestador de serviço as certificações exigidas pela FLEXPAG para o serviço contratado;
v. O acesso da FLEXPAG 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;
vi. O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

vii. A identificação e a segregação dos dados dos usuários finais da FLEXPAG por meio de controles físicos ou lógicos;

viii. A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da FLEXPAG.

Na avaliação da relevância do serviço a ser contratado, a FLEXPAG 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 FLEXPAG 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.

14.2. EXECUÇÃO DE APLICATIVOS PELA INTERNET

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

14.3. SERVIÇO DE COMPUTAÇÃO EM NUVEM

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

i. Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à FLEXPAG implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela FLEXPAG ou por ela adquiridos;

ii. Implantação ou execução de aplicativos desenvolvidos pela FLEXPAG, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços;
iii. 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 FLEXPAG 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.

14.4. 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 FLEXPAG deverá observar os seguintes requisitos:

i. Existência de convênio para troca de informações entre os órgãos reguladores e as autoridades supervisoras dos países onde os serviços serão prestados;
ii. Verificação de que a prestação dos serviços não causará prejuízos ao seu regular funcionamento nem embaraço à atuação dos órgãos reguladores;
iii. Definição dos países e regiões em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados. Essa definição deve ocorrer antes da contratação dos serviços;
iv. 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.

14.5. CONTRATO DE PRESTAÇÃO DE SERVIÇOS

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

i. A indicação dos países e da região em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados;
ii. A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
iii. A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos usuários finais;
iv. Em caso de extinção do contrato, a obrigatoriedade de transferência dos dados ao novo prestador de serviços ou à FLEXPAG, 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.
v. O acesso da FLEXPAG 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;
vi. A obrigação da empresa contratada notificar a FLEXPAG sobre a subcontratação de serviços relevantes para a FLEXPAG;
vii. A permissão de acesso dos órgãos reguladores 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;
viii. A adoção de medidas pela FLEXPAG, em decorrência de determinação dos órgãos reguladores;

ix. A obrigação da empresa contratada manter a FLEXPAG 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 FLEXPAG pelos órgãos reguladores, o contrato de prestação de serviços deve prever:

i. A obrigação da 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;
ii. A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção da 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:
iii. 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;
iv. A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da FLEXPAG.

15. CONTINUIDADE DOS SERVIÇOS DE PAGAMENTO

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

i. O tratamento dos incidentes relevantes relacionados com o ambiente cibernético;
ii. 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 FLEXPAG;
iii. Os cenários de incidentes considerados nos testes de continuidade de serviços de pagamento prestados;
iv. O tratamento para mitigar os efeitos dos incidentes relevantes da interrupção dos serviços de processamento, armazenamento de dados e de computação em nuvem contratados;
v. O prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos;
vi. A comunicação tempestiva ao Bacen e eventuais órgãos reguladores das ocorrências de incidentes relevantes e das interrupções dos serviços, que configurem uma situação de crise pela FLEXPAG, bem como das providências para o reinício das suas atividades.

A FLEXPAG 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.

16. ARQUIVAMENTO DE INFORMAÇÕES

A FLEXPAG deve armazenar, pelo prazo de 5 (cinco) anos, as seguintes informações:

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

17. DECLARAÇÃO DE RESPONSABILIDADE

Os Colaboradores e prestadores de serviço da FLEXPAG devem aderir formalmente a um termo em que se comprometem a agir de acordo com esta Política. Ademais, todos os contratos da FLEXPAG devem possuir cláusula que assegure aos princípios de segurança da informação estabelecidos nesta política.

18. DISPOSIÇÕES GERAIS

Esta Política foi aprovada e revisada pela Alta Administração e será revisada anualmente. A Política também será alterada a qualquer momento, para contemplar quaisquer alterações regulatórias e outras obrigações legais.

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 Cibernética e Proteção de Dados, 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, sempre que necessário, acessá-la através dos canais oficiais da Flexpag.

O não cumprimento das regras estabelecidas nesta norma poderá acarretar a aplicação de medidas disciplinares ou contratuais.

Todo e qualquer comentário relativo aos procedimentos descritos nesta Política devem ser encaminhados à Área de Compliance da FLEXPAG, através do e-mail compliance@flexpag.com.

19. CONTROLE DE APROVAÇÕES E ALTERAÇÕES DO DOCUMENTO

Histórico do Documento Normativo		
Responsável pela Elaboração:		
Área de Compliance em conjuntos com a Barcellos Tucunduva Advogados		
Responsável pela Revisão:		
Área de Compliance – Flávia Lima		
Responsáveis pela Aprovação:		
Diretoria Executiva	Mariana de Almeida Chaves de Souza	
	Henrique Almeida Chaves	
Versão	Alterações	Data
01	Emissão Inicial	24/03/2021
01	Atualização da Política	09/11/2022

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 de Segurança da Informação e Cibernética e Proteção de Dados, bem como das diretrizes contidas nas demais políticas, normas e procedimentos internos da FLEXPAG.

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 e-mail *seguranca@flexpag.com*, pelo *Canal de Ética* ou através do fone 0800 033 0314 das 9h às 17h de segunda a sexta.

_____ /_____ /_____

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 de Segurança e Cibernética e Proteção de Dados, bem como das diretrizes contidas nas demais políticas, normas e procedimentos internos da FLEXPAG.

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 e-mail *seguranca@flexpag.com*, pelo *Canal de Ética* ou através do fone 0800 033 0314 das 9h às 17h de segunda a sexta.

_____ /_____ /_____

Data

_____

Assinatura