Política de Segurança Cibernética

São Paulo, 19 de dezembro de 2023

Versão: 3.1

flagship

SUMÁRIO

1. DEFINIÇÕES

a) Alta Administração: sócios, administradores e diretores da FLAGSHIP;

b) Ameaça: Evento ou atitude indesejável que potencialmente remove, desabita, danifica ou destrói um recurso ou um ativo da informação;

c) Ativo: Bem tangível ou intangível pertencente, administrado ou de responsabilidade da FLAGSHIP;

d) Ativo da Informação: Base de dados e arquivos, documentação de sistemas e aplicativos, manuais de instruções, procedimentos operacionais, de suporte e de negócios, planos de continuidade, gerenciamento de crise e recuperação, bem como as demais informações armazenadas, processadas e trafegadas dentro e fora do ambiente institucional;

e) Cloud / Nuvem: Rede integrada na Internet que oferece serviços de tecnologia com manutenção e recursos terceirizados;

f) Confidencialidade: Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;

g) Disponibilidade: Garantia de que as pessoas autorizadas terão acesso à informação e aos sistemas e aplicativos sempre que necessário;

h) Evento: É a ocorrência identificada em um sistema, serviço ou rede que indica uma possível violação da segurança da informação, ou uma situação desconhecida, que passa a ser relevante para a segurança dos ativos;

i) Incidente: Qualquer evento que não faz parte da operação normal de um serviço e que pode causar interrupção de serviços ou redução de sua qualidade;

j) Integridade: Garantia de que a informação somente será modificada por pessoas autorizadas a fazê-la seguindo as diretrizes estabelecidas pela FLAGSHIP;

k) Parceiros de Negócio ou/e Terceiros Estratégicos de Negócio: toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, que celebra contratos com a FLAGSHIP, com a finalidade de, mediante retribuição, colaborar com os negócios da FLAGSHIP;

l) Vulnerabilidade: São definidas como a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças

2. NORMAS APLICÁVEIS

Todos aqueles a quem esta Política for aplicável deverão observar as leis e normas abaixo indicadas (em conjunto **“Legislação Aplicável”**):

a) Resolução BCB Nº 85, de 8 de abril de 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;

b) Lei Geral de Proteção de Dados (LGPD) - Lei no 13.709, de 14 de agosto de 2018: Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

c) Norma ISO/IEC 27001:2013: ISO que dispõe sobre Sistemas de Gestão de Segurança da Informação;

d) Instrução Normativa Nº 412, de 26 de setembro de 2023: Estabelece os procedimentos operacionais para a comunicação aos titulares de dados pessoais em caso de ocorrência de incidente de segurança envolvendo banco de dados relacionado a componente ou a infraestrutura do Pix.

e) Política de Gestão de incidentes.

f) Política de Continuidade de Negócios;

g) Política de Gestão de Crise;

3. OBJETIVO DA POLÍTICA

Esta política descreve as diretrizes aplicáveis à Política de Segurança Cibernética da FLAGSHIP. As diretrizes aqui descritas visam garantir as melhores práticas a serem adotadas para mitigar os riscos relacionados à Segurança da Informação e Cibernética de modo a assegurar a confidencialidade, integridade e disponibilidade das informações geridas pela Instituição.

4. ABRANGÊNCIA DA POLÍTICA

A responsabilidade pelo cumprimento integral e efetivo dessas diretrizes cabe à Alta Administração, Clientes, Colaboradores, Estagiários, Parceiros de Negócio e Prestadores de Serviços/Fornecedores que apoiam a operação, sustentação e/ou armazenamento das informações e utilizam as instalações físicas e infraestrutura tecnológica da instituição.

5. PROCESSO DE REFERÊNCIA

Gerir Segurança da Informação e Cibernética.

6. DIRETRIZES

6.1. DECLARAÇÃO DA INSTITUIÇÃO

A FLAGSHIP está comprometida em assegurar a confidencialidade, integridade e disponibilidade dos ativos da informação, razão pela qual a estratégia está pautada na prevenção, correção e monitoramento do ambiente, bem como na avaliação e respostas aos incidentes de segurança.

Todas as diretrizes, políticas e procedimentos deverão ser disponibilizados, de acordo com a sua classificação da informação, em local acessível aos colaboradores e, sempre que necessário aos demais públicos de relacionamento, devendo também ser protegidas contra quaisquer modificações intencionais ou não intencionais.

É terminantemente proibido o envio ou repasse por e-mail ou qualquer outro meio de comunicação de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo, bem como com opiniões, comentários ou troca de mensagens em redes sociais/fóruns, que possam difamar ou denegrir a imagem e afetar a reputação da FLAGSHIP.

6.2. ORGANIZAÇÃO E GESTÃO

.
A FLAGSHIP deverá constituir Comitê para tratar dos assuntos relativos ao processo de Gestão de Segurança da Informação e Cibernética. Este Comitê será responsável pela aprovação e manutenção das políticas e procedimentos que norteiam este processo.

Os usuários de negócios, técnicos e de suporte são responsáveis pelo desenvolvimento,
implementação de procedimentos detalhados, bem como pelo monitoramento dos controles sob a sua responsabilidade.

O Compliance deverá propor medidas disciplinares aos eventos que envolvam as diretrizes estabelecidas nesta política e a área de Gente e Gestão deverá aplicar as medidas disciplinares em resposta aos descumprimentos das Regulamentações vigentes, das Diretrizes e Normas institucionais

6.3. TREINAMENTO, CONSCIENTIZAÇÃO E MECANISMOS PARA DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA

A FLAGSHIP deverá ministrar educação continuada para o aculturamento das boas práticas, bem como adotar mecanismos para disseminação da cultura de segurança da informação e cibernética na Companhia, incluindo:

- Realização do programa de treinamento anual para colaboradores;

- Realização do programa de avaliação periódica de colaboradores para apuração do nível de conhecimento quanto ao tema segurança da informação e cibernética;

- Publicação deste documento no site da Instituição (público externo) e em ferramentas internas de comunicação institucional (público interno);

- A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos no site da Instituição (https://ipflagship.com.br/); e

- O comprometimento da administração com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

6.4. CLASSIFICAÇÃO DA INFORMAÇÃO

Todas as informações geradas pela FLAGSHIP devem passar por um processo avaliação e classificação da informação, garantindo que dados/informações com maior criticidade recebam controles apropriados. Portanto, a FLAGSHIP 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 FLAGSHIP. São exemplos de Informação Interna: normas, procedimentos e formulários da FLAGSHIP;

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 FLAGSHIP;

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.

6.5. GESTÃO DE RISCOS E VULNERABILIDADES

A FLAGSHIP possui processo de estruturado para gestão de riscos cibernéticos visando mitigar os possíveis impactos nos processos críticos da empresa. A gestão de riscos é fundamental para garantir a exatidão das atividades de controles e prevenção dos riscos relevantes do Processo de Gestão de Segurança da Informação e Cibernética e dos demais Processos de Suporte e de Negócios. Além disso, visa assegurar que medidas preventivas sejam implementadas para combater o risco de fraudes nos ambientes de infraestrutura, corporativo e de negócio.

A FLAGSHIP possui processo de Gestão de Vulnerabilidade nos ativos da informação, sistemas e aplicativos, de modo que os controles estabelecidos e implementados, como correções de Segurança e Testes Periódicos de Segurança, sejam suficientes para identificar e classificar as ameaças, bem como para propor medidas de tratamentos adequados diante da criticidade dos eventos.

6.6. GESTÃO DE INCIDENTES

Processos e procedimentos deverão ser estabelecidos para prevenir, identificar e responder adequadamente às violações de segurança e os incidentes de segurança.
Esses procedimentos deverão prever, no mínimo, a identificação, a classificação, o diagnóstico, a implementação de medidas corretivas imediatas, resolução definitiva, fechamento e monitoramento do Incidente, objetivando a mitigação e/ou eliminação dos riscos associados aos mesmos. Além disso, deverá ser emitido relatório anual que será aprovado e divulgado aos órgãos de governança da FLAGSHIP

6.7. INVENTÁRIO

A FLAGSHIP deverá manter inventário atualizado dos ativos da informação, contemplando no mínimo os recursos de hardware, software, aplicações de negócios, equipamentos de rede, instalações físicas, assim como fornecedores e/ou prestadores de serviços considerados relevantes.

6.8. TRANSFERÊNCIA DE INFORMAÇÃO

A transferência eletrônica ou física de informações entre a FLAGSHIP, colaboradores, estagiários, fornecedores, prestadores de serviços e parceiros de negócios deverá ser controlada de maneira planejada para assegurar a sua proteção na transmissão e no armazenamento adequado.

É vedada a utilização de aplicativos de comunicação não oficiais, tais como Whatsapp e Telegram, entre outros, para transferência de dados entre os representantes da FLAGSHIP e demais públicos de relacionamento.

As partes deverão firmar acordo por escrito prevendo cláusulas de proteção aos ativos da informação contra perda, extravio, divulgação e danos, aplicáveis de acordo com a classificação da informação e a natureza do relacionamento, seja ele comercial ou empregatício.

6.9. SEGURANÇA E CONTROLE DE ACESSO

Os colaboradores, estagiários, fornecedores e/ou prestadores de serviço devem ter acesso apenas às dependências físicas necessárias à natureza de seus serviços. 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.

Os visitantes, fornecedores e/ou prestadores de serviços eventuais e os clientes ao acessar qualquer dependência da FLAGSHIP deverão ser previamente identificados, autorizados e acompanhados por colaboradores durante a realização das suas atividades e/ou participações em reuniões.

A FLAGSHIP envidará seus melhores esforços para mitigar eventuais problemas relacionados à segurança em sua rede. Para tanto, se utilizará de ferramentas de segurança capazes de detectar e bloquear tentativas de intrusão em seu ambiente de rede e controlar os acessos que partem da sua rede.

O acesso remoto por colaboradores, estagiários, fornecedores e/ou prestadores de serviço à rede da FLAGSHIP só poderá ser feito mediante aprovação do líder imediato do colaborador ou do responsável pelo contrato de prestação de serviço.

Todas as solicitações de acesso devem seguir um fluxo documentado de aprovação. Aquelas realizadas em caráter de exceção, caso se tornem constantes, deverão ser documentadas e incluídas no fluxo padrão de aprovação.

Nenhuma exceção deve violar as normas e legislações vigentes no país e só deve ser encaminhada para análise e aprovação caso seja uma necessidade para o negócio.

Toda exceção aprovada deverá possuir controles apropriados, registro e justificativa, além de prazo para o retorno à normalidade.

6.10. PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

A FLAGSHIP utilizará recursos e ferramentas (antivírus e firewall), bem como manutenções periódicas de equipamentos e sistemas para a mitigação de ataques cibernéticos, tais como malwares, ransomware, phishing, engenharia social, entre outros, que possam ocasionar um incidente.

6.11. PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

A FLAGSHIP deverá realizar backups periódicos dos ativos da informação e armazená-los em ambientes físicos e/ou lógicos devidamente protegidos, para garantir a recuperação operacional e continuidade dos negócios.

Nenhuma informação importante para o negócio deve ser armazenada no disco local dos notebooks e desktops. Periodicamente os usuários deverão ser alertados sobre os riscos deste processo é imprescindível a utilização das ferramentas de armazenamento oficiais da Instituição, como por exemplo: Google Drive e demais servidores oficiais.

Toda a informação, incluindo backups, documentos, dados de colaboradores, estagiários, fornecedores e/ou prestadores de serviços, clientes e terceiros relacionados, correios eletrônicos e demais tipos de mídias de armazenamento físico deve respeitar indistintamente as diretrizes institucionais sobre retenção e descarte de informações.

Os dados pessoais dos titulares devem ser excluídos assim que atingirem as finalidades do consentimento ou findar-se o prazo de retenção predeterminado em razão da natureza da situação. Quando os dados forem retidos após o cumprimento da finalidade inicial, eles deverão ser minimizados / criptografados / anonimizados para proteger a identidade dos titulares em caso de um incidente envolvendo dados pessoais.

6.12. MALICIOSOS GERENCIAMENTO DE MUDANÇAS

As modificações e/ou aperfeiçoamentos dos sistemas de informação da FLAGSHIP deverão ser realizados através do processo de gerenciamento de mudanças. A análise deverá contemplar o impacto nos processos de suporte e negócios, bem como possíveis exposições da FLAGSHIP.

6.13. USO ACEITÁVEL DE RECURSOS TECNOLÓGICOS E MONITORAMENTO DE LOGS

Os recursos físicos, bem como os serviços de tecnologia oferecidos aos colaboradores e terceiros pela FLAGSHIP, devem ser utilizados de forma profissional, ética e legal, e seguir as diretrizes estabelecidas pela instituição.

O profissional entende que os equipamentos, a conta e a rede corporativa fornecida pela FLAGSHIP são exclusivos para o desempenho das suas atividades produtivas e é de conhecimento, desde já que, as informações trafegadas, produzidas e/ou armazenadas não estarão protegidas pelo princípio da intimidade, nem de privacidade pessoal.

A utilização de senhas tem a finalidade de verificar a identidade do usuário, assegurando que a pessoa é quem diz ser e, liberando os acessos permitidos necessários para execução das suas atividades. É extrema importância a utilização da senha para registrar as atividades executadas, garantir a integridade das ações e proteger os acessos de pessoas não autorizadas.

A senha é de uso pessoal e intransferível, sendo o colaborador, o estagiário, o fornecedor e/ou prestador de serviço o único responsável pelas ações realizadas, portanto em hipótese alguma a senha deve ser compartilhada, dentro ou fora da instituição.

É obrigatória a gravação de logs ou trilhas de auditoria do ambiente computacional, para todas as plataformas, de forma a permitir identificar as interações dos usuários e os ativos da informação. Essas informações devem ser protegidas contra modificações e acessos não autorizados.

A FLAGSHIP deverá estabelecer procedimento de monitoramento de eventos de log para analisar atividades suspeitas ou exceções aos comportamentos normais na execução das atividades do dia a dia. Esse procedimento deverá prever a identificação, registro e análise do evento, bem como as respectivas atribuições de responsabilidades e medidas corretivas necessárias.

6.14. DESENVOLVIMENTO SEGURO

O processo de desenvolvimento de sistemas da FLAGSHIP deve seguir as boas práticas de desenvolvimento seguro. Os ambientes de produção devem ser segregados dos demais ambientes e com acesso via aplicação por usuários previamente autorizados ou por ferramentas homologadas.

6.15. COMPUTAÇÃO EM NUVEM

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, no País ou no exterior, deverá atender rigorosamente à legislação vigente, incluindo análises, condições precedentes e requisitos contratuais e nela estabelecidas.

6.16. COMPUTAÇÃO EM NUVEM

A FLAGSHIP deverá utilizar, sempre que necessário, controles de criptografia e de gerenciamento de chaves atrelado às diretrizes institucionais de classificação dos ativos da informação para recebimento e compartilhamento de dados requisitos contratuais e nela estabelecidas.

6.17. CONTINUIDADE DE NEGÓCIOS E GESTÃO DE CRISES

A gestão de continuidade de negócios é realizada pela FLAGSHIP por meio de estratégias, soluções tecnológicas e processos descritos no Plano de Continuidade de Negócios (PCN), com objetivo de evitar e/ou mitigar os impactos decorrentes de falhas de segurança e desastres de grandes proporções.

6.18. GESTÃO DE TERCEIROS

A FLAGSHIP estabelece diretrizes para prestação de serviços em suas dependências e para contratação e/ou aquisição de serviços. São realizadas diligências adicionais nos terceiros considerados relevantes, pois armazenam e processam dados considerados críticos em estruturas tecnológicas inclusive aquelas não pertencentes à FLAGSHIP.

Os contratos de terceirização e acordos comerciais não podem impedir que a FLAGSHIP administre e proteja seus ativos da informação.

A FLAGSHIP 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 FLAGSHIP.

6.19. PROPRIEDADE INTELECTUAL

Quaisquer invenções, criações, obras e aperfeiçoamentos que tenham sido ou venham a ser criados ou realizados pelos colaboradores, estagiários, fornecedores e/ou prestadores de serviço decorrentes de suas atividades profissionais e contratuais, respectivamente, pertencem exclusivamente à FLAGSHIP, salvo se o contrato de prestação de serviços, dispuser o contrário. É vedado aos profissionais qualquer cópia, divulgação, posse ou revenda. A instalação de quaisquer programas nos computadores/notebooks deve ser objeto de prévia e expressa autorização do gestor imediato do profissional ou aquele responsável pelo contrato, em conjunto com a TI.

É vedada a instalação de qualquer tipo de software ou programa que possua direitos autorais restritos, sem a contratação das respectivas licenças de utilização.

6.20. EMPRESAS E EVENTUAIS ENTIDADES DO GRUPO ECONÔMICO

Devem avaliar as diretrizes e requisitos estabelecidos nesta política e demais documentos correlatos, reportando periodicamente à Compliance e Controles Internos os riscos identificados, bem como a necessidade de revisão de processos, adequando seus procedimentos de segurança internos conforme seu segmento de negócio e perfil de riscos.

7. CANAIS DE COMUNICAÇÃO

O Departamento de Compliance centralizará as comunicações e interações com órgãos reguladores, entidades de classes, parceiros de negócios, entre outros, através dos canais de comunicação oficiais da instituição, para alcance dos mais diferentes públicos de relacionamento

A FLAGSHIP deverá assegurar canal de comunicação com atendimento integral, eficiente e autônomo para recepcionar demandas e orientar sobre situações que possam colocar em risco a segurança dos ativos da informação e a continuidade dos negócios. Sempre que necessário, os incidentes deverão ser compartilhados com as partes interessadas e órgãos reguladores.

8. VIOLAÇÕES E SANÇÕES

A identificação de qualquer desvio das diretrizes estabelecidas nesta política deverá ser reportada, tempestivamente, ao Departamento de Compliance que analisará e deliberará sobre as penalidades de acordo com a gravidade do evento e seus respectivos impactos. O descumprimento de quaisquer diretrizes estabelecidas nesta política está sujeito à sanção disciplinares, medidas administrativas e/ou criminais, sem prejuízo de outras penalidades ou medidas cabíveis de acordo com a legislação vigente.

9. RELATÓRIOS

Os registros coletados e classificados indicando a implementação efetiva das ações estabelecidas em resposta à incidentes da FLAGSHIP, servirão de insumo para o reporte periódico, à Diretoria, após aprovações dos demais órgãos de governança.

10. ESTRUTURA E RESPONSABILIDADES

10.1. DIRETORIA

a) Aprovar as diretrizes estabelecidas neste documento e exigir seu cumprimento por todos os departamentos da instituição.

10.2. COMITÊ DE RISCOS

a) Assessorar a Diretoria no desempenho de suas atribuições relacionadas à adoção de políticas e medidas voltadas à disseminação de segurança de informação e cibernéticas, bem como da disseminação da cultura de riscos, identificação e mitificação de riscos e conformidade com normas aplicáveis;

10.3. CONTROLES INTERNOS E COMPLIANCE

a) A Gestão de Riscos, Controles Internos e Compliance é independente no exercício de suas atribuições e funções, possui comunicação direta com a Alta Administração e acesso a quaisquer informações necessárias no âmbito de suas responsabilidades;

b) O Monitoramento e as avaliações periódicas deverão ser conduzidos pela Gestão de Riscos, Controles Internos e Compliance a fim de verificar a conformidade com as políticas e procedimentos internos, legislações e regulamentações vigentes, bem como avaliar a efetividade dos controles

10.4. SEGURANÇA DA INFORMAÇÃO

a) Oferecer supervisão ao negócio através da medição da conformidade;

b) Elaborar, criar e manter as políticas de Segurança, os controles e treinamentos relacionados à Segurança da Informação.

10.5. TI

a) Manter o parque tecnológico disponível e atualizado com os padrões de segurança implementados, dentro dos prazos compatíveis com os níveis de riscos da FLAGSHIP;

b) Garantir o desenvolvimento e implantação de procedimentos detalhados, bem como o monitoramento da conformidade com essas diretrizes e normas correlatas

.

10.6. GERENTE E GESTORES

a) Em conjunto com TI deverá adotar mecanismos que garantam a proteção dos ativos da informação sob sua responsabilidade contra alteração, destruição, divulgação e cópia não autorizada, seja ela acidental ou intencional.

10.7. TIME DE G&G (GENTE & GESTÃO)

a) Manter controles de Segurança sobre todas as movimentações, admissões e desligamentos dos profissionais da FLAGSHIP;

b) Garantir que todos os profissionais tenham recebido, lido e assinado Termo de Recebimento e Responsabilidade, bem como armazenar adequadamente.

10.8. AUDITORIA / CONSULTORIAS ESPECIALIZADAS

a) Auditar os processos executados pela estrutura de Compliance e demais departamentos da FLAGSHIP, testar a aderência a esta política e as regulamentações externas, bem como atestar a eficiência dos controles mantidos internamente para suportar o processo de gestão de segurança e cibernética.

10.9. USUÁRIOS

a) Guardar sigilo sobre toda e qualquer informação, principalmente privilegiada, e zelar pela segurança dos ativos da informação utilizados em qualquer âmbito de relacionamento, sejam eles profissionais ou pessoais, obedecendo aos requisitos contratuais, legais, bem como aqueles estabelecidos em diretrizes, políticas e procedimentos da FLAGSHIP;

b) Conhecer, disseminar e cumprir todas as diretrizes da FLAGSHIP, em especial as definidas nesta política;

c) Denunciar práticas que estejam em desacordo com obrigações contratuais, legais, bem como aqueles estabelecidos em diretrizes, políticas e procedimentos da FLAGSHIP ao seu gestor ou ao Compliance, através do e-mail compliance@ipflagship.com.br .

10.10. TERCEIROS ESTRATÉGICOS DE NEGÓCIO

a) Emitir os certificados digitais necessários para acesso aos ambientes (homologação e produção), seguindo as recomendações técnicas fornecidas pela FLAGSHIP;

b) Gerir o vencimento, a renovação, e sempre que necessário, disponibilizar o novo certificado root com até 60 dias de antecedência do vencimento do vigente para FLAGSHIP através do canal disponível no website https://ipflagship.freshdesk.com/ ;

c) Gerir o vencimento e a renovação do novo certificado cliente atualizar a aplicação em seus sistemas internas para a correta interface com a FLAGSHIP;

d) Em casos de vazamento ou comprometimento do certificado, deverá revogar, gerar e disponibilizar o(s) novo(s) certificado(s) através do canal disponível no website https://ipflagship.freshdesk.com/ ;

e) Comunicar os incidentes de segurança para a correta classificação, análise de causa raiz e tratamento através do canal disponível no website https://ipflagship.freshdesk.com/ ;

f) Guardar sigilo sobre toda e qualquer informação, principalmente privilegiada, e zelar pela segurança dos ativos da informação utilizados em qualquer âmbito de relacionamento, sejam eles profissionais ou pessoais, obedecendo aos requisitos contratuais, legais, bem como aqueles estabelecidos em diretrizes, políticas e procedimentos da FLAGSHIP

11. CONTROLE DO DOCUMENTO

11.1. CONTROLE DO DOCUMENTO

Versão	Rev	Data da Publicação	Descrição	Responsável	Vencimento
1	0	18/08/2021	Criação do documento	Compliance	18/08/2022
1	1	22/09/2021	1. Ajustes pontuais de nomenclatura no Item 4. Abrangência e no 5.5. Responsabilidades 2. Alteração no Item 5.21 Propriedade Intelectual.	Compliance	18/08/2022
2	0	09/09/2022	Revisão Anual	Compliance	12/09/2023
3	0	29/09/2023	1. Inclusão de normas aplicáveis, responsabilidades de terceiros de negócio e ajustes no layout do documento.	Tecnologia e Compliance	29/09/2024
3	1	19/12/2023	1. Ajusta do item 6.3 para inclusão de mecanismos para disseminação da cultura de segurança cibernética. 2. Ajustes pontuais no documento.	Tecnologia e Compliance	19/12/2024

11.2. CICLO DE REVISÃO

Este documento será revisto e atualizado, sem prejuízo no disposto no item acima, sempre que necessário, para:

- Atendimento de solicitação de correção ou inclusão de informações;

- Atendimento de requisitos legais, boas práticas ou recomendações de órgãos reguladores e auditoria;

- Adequação em razão de mudança organizacional com impacto relevante em atividade abordada neste documento.

11.3. GUARDA E RETENÇÃO

As versões deste documento deverão ser armazenadas por cinco anos, após o vencimento de seu prazo de validade.

flagship

FLAGSHIP INSTITUIÇÃO DE PAGAMENTO LTDA.

São Paulo, 19 de dezembro de 2023

Versão: 3.1