

1. PROPÓSITO

Essa política estabelece os papéis e responsabilidades dos colaboradores e prestadores de serviços do Banco CNH (Banco), bem como as diretrizes e normas para a condução das atividades envolvendo o tratamento e a garantia da privacidade e da proteção de dados pessoais, ou seja, dados de pessoas naturais (titulares), com as quais o Banco se relaciona, para executar suas atividades de negócio.

2. APLICAÇÃO

Todas as atividades relacionadas aos negócios do Banco que tratam dados pessoais devem ser orientadas por esta política, em conjunto com as políticas relacionadas no item 14, que tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

3. PRINCÍPIOS GERAIS

1- Compliance com Leis e Regulamentações

Esta política foi elaborada de forma a atender aos requisitos da lei 13.709/2018, “Lei Geral de Proteção de Dados” (LGPD), especialmente no tocante às boas práticas e à governança da segurança dos dados pessoais.

2- Definições de dados pessoais e da proteção de dados pessoais.

Dados pessoais são informações relativas a uma pessoa viva, identificada ou identificável. Também constituem dados pessoais o conjunto de informações distintas que possam levar à identificação de uma determinada pessoa.

Os dados pessoais são necessários em diferentes atividades de negócios no Banco, podendo ter várias formas de representação, armazenamento e divulgação, sendo que o seu significado e valor dependem do contexto em que se encontram, podendo ser, por exemplo:

- a) Em papel: listas de presença, formulários de cadastro em papel, relatórios, memorandos, etc.
- b) Em mídia digital: arquivos digitais gravados em discos, SSDs, flash drives, etc.
- c) Em som: gravação de reuniões e outras atividades, secretária eletrônica, etc.
- d) Em imagem: fotos de pessoas e de seus documentos, vídeos contendo pessoas, etc.

A proteção dos dados pessoais deve garantir fundamentos e direitos básicos das pessoas, como o respeito à privacidade, à dignidade e à autodeterminação; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; a livre iniciativa e a livre concorrência; a defesa do consumidor e outros direitos humanos relacionados com a personalidade e o exercício da cidadania.

Para que os objetivos de proteção de dados pessoais sejam alcançados, os colaboradores e prestadores de serviços do Banco devem seguir as práticas determinadas nesta Política de Privacidade e Proteção de Dados Pessoais, os procedimentos operacionais relacionados a este documento, à Política de Segurança da Informação (PSI), aos Procedimentos de Confidencialidade e Gestão de Documentos e Informação e à Política de Segurança Cibernética, documentos que estabelecem diretrizes e normas gerais de segurança para todos os ativos de informação da instituição, incluindo dados pessoais e também outros tipos de dados sensíveis e de valor para os negócios.

4. PAPÉIS E RESPONSABILIDADES

De forma geral, todas as pessoas (colaborador, consultor, concessionários/correspondentes no país, terceirizados e demais indivíduos) a serviço do Banco são responsáveis pela adoção de boas práticas de segurança da informação no tratamento dos dados pessoais.

A seguir, estão relacionados os papéis e responsabilidades específicos de cada função dentro da estrutura do Banco:

4.1 Diretoria

O papel da Diretoria é garantir que as políticas e procedimentos de proteção de dados pessoais sejam seguidos e executados, de forma que a instituição esteja em conformidade com a Lei.

São responsabilidades da Diretoria:

- Garantir que os princípios de proteção de dados pessoais, ou seja, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e a prestação de contas sejam aplicados no Banco.
- Indicar o Encarregado dos Dados Pessoais e promover a sua capacitação.

4.2 Proprietário dos Dados Pessoais

Os Proprietários dos Dados Pessoais são os gestores responsáveis pelos processos ou atividades de negócio relacionados com a coleta, uso e/ou tratamento de cada uma das bases de dados pessoais presentes no Banco.

São responsabilidades do Proprietário dos Dados Pessoais:

- Garantir o cumprimento das regulamentações, políticas e procedimentos de proteção de dados pessoais.
- Definir quem pode ter acesso aos dados pessoais sob a sua responsabilidade.
- Definir os controles que devem ser aplicados para garantir a qualidade, gerenciar os riscos e proteger os dados pessoais sob sua responsabilidade.
- Assegurar que qualquer nova atividade de tratamento de dados pessoais seja devidamente comunicada ao Encarregado dos Dados Pessoais, inclusive envolvendo-o de forma que os riscos de proteção dos dados pessoais sejam plenamente avaliados e tratados.
- Assegurar que todos os novos dados coletados, bem como todos os eventos de alterações nas estruturas das bases de dados pessoais sob a sua gestão, além dos eventos de alteração, correção ou eliminação de registros de dados pessoais, sejam sempre devidamente comunicados ao Encarregado dos Dados Pessoais, para que o mesmo possa manter o inventário de dados pessoais atualizado.

4.3 Operador

“Operadores” são os prestadores de serviços externos, terceirizados, que de alguma forma realizam a coleta, o uso ou qualquer tratamento de dados pessoais dos quais o Banco é o controlador.

Cada operador tem a responsabilidade de garantir, manter o registro e evidenciar, sempre que requerido, que adota todos os processos e aplica todos os recursos necessários de proteção de dados pessoais, de acordo com a Lei e conforme definido nesta Política, nos mesmos moldes exigidos das áreas de negócios do Banco.

4.4 Encarregado dos Dados Pessoais

No Banco o Encarregado dos Dados Pessoais (“DPO – Data Protection Officer”) é uma função exercida por colaborador(a) do departamento de Controles Internos e Compliance, de acordo com definição da Diretoria.

O principal papel do Encarregado dos Dados Pessoais é garantir que o Banco realize o tratamento de dados pessoais em conformidade com a Legislação e Regulações, bem como atuar como canal de comunicação entre o Banco, os Operadores, os Titulares dos Dados Pessoais e a Autoridade Nacional de Proteção de Dados (ANPD).

São responsabilidades do Encarregado dos Dados Pessoais:

- Implementar medidas organizacionais adequadas para garantir e demonstrar que o tratamento de dados pessoais é realizado de acordo com a Lei.
- Implementar políticas e procedimentos adequados à proteção de dados pessoais.
- Informar e instruir as pessoas (colaborador, consultor, temporário, concessionários/correspondente no país, terceiro e demais indivíduos) a serviço do Banco sobre os requisitos da Lei e a importância de conformidade com a mesma.
- Abordar potenciais riscos à proteção dos dados pessoais de forma proativa e contínua.
- Manter o registro de todas as atividades e processos que compreendam o uso e tratamento de dados pessoais realizados pela Instituição, incluindo as finalidades destas atividades e processos, quais dados pessoais estão envolvidos, quem é o proprietário dos dados pessoais dentro do Banco e o tempo durante o qual a instituição manterá estes dados.
- Monitorar o desempenho das ações realizadas para a proteção de dados pessoais e fornecer recomendações sobre o impacto das mesmas.
- Coordenar as comunicações internas relacionadas aos processos de gestão da proteção dos dados pessoais, identificando os responsáveis para cada atividade e monitorando a sua execução.
- Atuar como ponto de contato entre o Banco e os titulares dos dados para informá-los sobre como seus dados pessoais estão sendo usados, o direito de apagá-los e sobre as medidas que a instituição adota para protegê-los, facilitando o exercício dos seus direitos.
- Disponibilizar os dados pessoais ao titular dos dados mediante solicitação expressa.
- Atuar como o ponto de contato entre o Banco e a ANPD.
- Elaborar o relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente às suas operações de uso e tratamento de dados pessoais e que contenha, no mínimo:
 - A descrição dos tipos de dados pessoais.
 - A metodologia utilizada para a coleta e para a garantia da segurança dos dados pessoais.
 - A análise do Banco com relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados.
- Convocar o Comitê de LGPD para discutir assuntos relevantes.

4.5 Comitê de LGPD

O Comitê de LGPD é responsável por:

- Deliberar sobre as solicitações trazidas por titulares, incidentes de segurança ou qualquer tema que traga risco ao Banco
- Discutir riscos e controles mitigatórios bem como tendências, benchmarks e atualizações de regulação
- Discutir casos de Privacy by design no eventual lançamento de produtos ou processos novos
- Acompanhar ações de prevenção aos riscos

4.6 Segurança da Informação (SI) - IT SEC - COMPLIANCE

A função de Segurança da Informação (SI) é definir diretrizes e normas, apoiar na implementação, controlar e monitorar as demais áreas de negócios e de suporte, em todas as questões relacionadas com a confidencialidade, integridade e disponibilidade das informações do Banco, incluindo os dados pessoais.

O Banco compartilha das políticas de segurança da informação do Grupo CNH e da estrutura de segurança da informação definidas em suas políticas.

São responsabilidades da Segurança da Informação em relação à Privacidade e Proteção aos Dados Pessoais:

- Definir, elaborar, divulgar e apoiar na implementação de uma adequada Política de Segurança da Informação (PSI), alinhada também com Política de Segurança Cibernética e esta Política. A PSI é o documento que contém as diretrizes e normas para garantir que a coleta, o tratamento e o armazenamento de dados pessoais são realizados com segurança, de acordo com os requisitos da Lei.
- Apoiar a área de Tecnologia da Informação, bem como o Encarregado e os Proprietários dos Dados Pessoais, provendo informações e diretrizes sobre segurança, para que possam exercer suas funções, por exemplo: detalhes sobre as normas e os controles de proteção dos dados pessoais, que são um subconjunto das informações tratadas no âmbito da instituição.

4.7 Tecnologia da Informação (IT) – Information Technology

No que tange à privacidade e proteção de dados pessoais, o papel da área de Tecnologia da Informação (IT) do banco, em conjunto com a área de Segurança da Informação da indústria, é o de garantir que o Banco realize o tratamento dos dados pessoais com os controles e recursos tecnológicos de proteção adequados, garantindo a confidencialidade, integridade e disponibilidade de tais dados.

São responsabilidades de IT:

- Implementar os controles, recursos e processos tecnológicos para atendimento da Política de Segurança da Informação, de forma a garantir e demonstrar que a coleta, o tratamento e o armazenamento de dados pessoais são realizados com segurança, de acordo com os requisitos da Lei.
- Garantir a proteção e a segurança dos dados pessoais nos ambientes de armazenamento e processamento de dados, bem como nos canais digitais de comunicação (e-mail, intranet, redes sociais internas e externas, sistemas de mensagens instantâneas, sistemas de trocas de arquivos, serviços web, etc.); adotando, provendo e implementando medidas, processos e recursos técnicos suficientes para

proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

- Implementar processo e rotina de apagamento ou de anonimização de dados pessoais obsoletos, cujo prazo de armazenamento já foi atingido.

4.8 Auditoria Interna

A Auditoria Interna é responsável por testar os processos e controles relacionados com a proteção de dados pessoais e com a adequada atuação do Encarregado dos Dados Pessoais, para garantir a conformidade com a Lei.

Assim, a Auditoria Interna deve incluir tais testes no seu plano de trabalho periódico ou seguindo o cronograma alinhado com o Conselho de Administração.

Ao avaliar os processos e controles relacionados à proteção de dados pessoais, a Auditoria Interna deve também reportar seus apontamentos ao Encarregado dos Dados Pessoais, para apoiar na adequação dos controles às políticas e procedimentos.

5. DIREITOS DOS TITULARES

Os titulares dos dados coletados e processados pelo Banco possuem os seguintes direitos em relação aos seus dados pessoais tratados pela instituição.

- a) Confirmação da existência de tratamento de seus dados pessoais.
- b) Acesso aos dados pessoais.
- c) Correção de seus dados pessoais, quando estiverem incompletos, inexatos ou desatualizados.
- d) Eliminação de seus dados pessoais, quando estes forem desnecessários, excessivos ou tratados em desconformidade com a Lei, inclusive quando houver consentimento por parte do titular, desde que os dados pessoais não sejam utilizados para cumprir com obrigações legais e regulatórias.
- e) Portabilidade de seus dados pessoais para outro fornecedor de serviço ou produto, mediante requisição expressa do titular, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- f) Informação das entidades públicas e privadas com as quais a instituição compartilhou seus dados pessoais.
- g) Informação sobre a possibilidade de não fornecer consentimento para o tratamento de seus dados pessoais.
- h) Revogação do consentimento para o tratamento de seus dados pessoais.

6. COLETA, USO E TRATAMENTO DE DADOS PESSOAIS

A coleta pode ocorrer quando necessário para estabelecer a relação comercial entre o Banco, seus colaboradores, parceiros de negócios e clientes, para a execução de um contrato ou para o cumprimento de uma obrigação legal à qual o Banco está sujeito.

O Banco também faz o tratamento dos dados pessoais para atender aos interesses legítimos da instituição, comprometendo-se a cumprir com toda a legislação aplicável em relação à proteção dos dados pessoais, assegurando que sejam coletados, utilizados e tratados de acordo com as disposições da LGPD e outras leis e regulações aplicáveis, se houver.

Em todos os casos em que os dados pessoais coletados não forem anonimizados e a coleta não for para fins de (i) cumprimento de obrigação legal ou regulatória, (ii) execução de contrato ou procedimentos

preliminares relacionados a contrato do qual seja parte o titular, (iii) exercício regular de direitos em processo judicial, administrativo ou arbitral, (iv) proteção do crédito e (v) legítimo interesse, o Banco deverá requerer o consentimento expresso do titular dos dados, devendo ficar este consentimento registrado e arquivado em mídia digital ou impressa.

Sempre que houver mudanças na finalidade, o Banco deverá informar previamente o titular sobre as mudanças e pedir novo consentimento, podendo o titular revogar o consentimento, caso discorde das alterações.

Quando o tratamento de dados pessoais for condição para o Banco fornecer um produto ou serviço, ou para o exercício de seu direito, o titular será informado sobre esse fato e sobre os meios pelos quais poderá exercer os direitos elencados na Lei.

7. NOVOS PROJETOS E PROCESSOS DE MUDANÇAS EM DADOS PESSOAIS

Qualquer nova atividade de tratamento de dados pessoais deve ser devidamente comunicada pelos Proprietários ao Encarregado dos Dados Pessoais, inclusive envolvendo este último no planejamento de novos projetos que possam envolver a coleta e tratamento de dados pessoais, de forma que os riscos à proteção de dados pessoais sejam plenamente avaliados e tratados.

Nos processos normais de operação dos negócios, toda e qualquer mudança em dados pessoais deverá ser comunicada ao Encarregado dos Dados Pessoais, de forma manual ou automática (integração sistêmica), para que o mesmo possa atualizar os registros na(s) sua(s) ferramenta(s) de controle. Incluem-se neste processo de comunicação/integração tanto as mudanças na estrutura de dados como nos registros, por exemplo:

- Novos dados pessoais coletados em sistemas/processos atuais.
- Alteração, correção ou eliminação de registros de dados pessoais nos sistemas/processos atuais.
- Mudanças na estrutura das bases de dados pessoais de sistemas/processos já existentes.

8. TRATAMENTO DE DADOS PESSOAIS COLETADOS FORA DO BRASIL

O tratamento e a proteção desses dados devem seguir os mesmos procedimentos e controles adotados para os dados coletados no Brasil.

Os Dados podem ser transferidos a terceiros para seguir as obrigações legais, operar e manter a segurança do Banco e seguir as ordens das autoridades públicas ou exercer nossos direitos perante autoridades judiciais. O Banco pode compartilhar os dados também com demais empresas do grupo econômico (CNH e Iveco Group), parceiros comerciais e rede de concessionários, corretoras de seguros parceiras e prestadores de serviços desde que constante no termo SCR/LGPD assinado por ocasião da colocação da proposta e que o titular não haja solicitado a revogação da autorização.

Os dados também podem ser transferidos a parceiros de negócios quando ocorrer venda da carteira de crédito ou contratação de seguro para ela.

Em observância às normas do Banco Nacional de Desenvolvimento Econômico e Social (BNDES), serão compartilhados com os órgãos gestores dos programas de crédito, com a Controladoria-Geral da União e Tribunal de Contas da União, todas as informações referentes à concessão do crédito, quando a operação envolver recursos equalizáveis (recursos públicos).

Em observância ao normativo do Conselho Monetário Nacional e Banco Central do Brasil, quando for identificado indício de ocorrência ou de tentativa de fraude, os dados dos envolvidos serão compartilhados com as demais instituições financeiras.

O Banco está obrigado por lei a comunicar às entidades reguladoras que supervisionam a sua atividade, e a outras entidades públicas/oficiais, bem como aos auditores externos, dados pessoais dos seus

clientes, relacionados com a sua identidade e com as suas responsabilidades de crédito, incluindo as seguintes entidades:

- (a) Banco Central do Brasil - Sistema de Informações de crédito;
- (b) Autoridade Tributária no caso de clientes investidores;
- (c) Conselho de Controle de Atividades Financeiras – COAF e demais autoridades judiciais e policiais nos termos previstos na Lei de Combate à Lavagem de Dinheiro e Financiamento ao Terrorismo.
- (d) Comissão de Valores Mobiliários e B3, nos termos previstos no regime legal e regulatório dos mercados de instrumentos financeiros.
- (e) Secretaria do Tesouro Nacional, Controladoria-Geral da União e Tribunal de Contas da União, todas as informações referentes à concessão do crédito, quando a operação envolver recursos equalizados pelo Tesouro Nacional.
- (f) Empresas de auditoria externa.

9. DESCARTE DE DADOS PESSOAIS

Encerrado o período de utilização ou quando terminar a finalidade para a qual os dados pessoais foram coletados e tratados e em não havendo outra finalidade que justifique a manutenção dos dados, os Proprietários dos Dados Pessoais deverão excluí-los nos termos da legislação em vigor.

Nos casos em que o Banco não puder excluir os dados pessoais para cumprir exigências legais ou por alguma outra necessidade legítima, esses dados devem ser arquivados com segurança até que a exclusão seja possível.

10. PROCESSOS DE COMUNICAÇÃO COM TITULARES E COM A ANPD

O Banco deve estabelecer um canal de comunicação para que a ANPD e os titulares possam entrar em contato com a instituição sempre que desejarem exercer seus direitos. O responsável pela operação deste canal de comunicação é o Encarregado dos Dados Pessoais.

Este canal de comunicação deverá ser publicado na internet e/ou em outros meios que facilitem a divulgação aos titulares e à ANPD.

Adicionalmente, sempre que requerido, o Encarregado dos Dados Pessoais deverá também atender aos pedidos de informações, emissão de relatório de impacto para a ANPD e a ocorrência de incidentes, entre outras demandas legais que poderão ser regulamentadas pela ANPD.

11. MEDIDAS DE PROTEÇÃO

11.1 Proteção de dados pessoais em papel:

Para a correta proteção dos locais que contém dados pessoais em papel, os seguintes controles devem estar implementados:

- a) Estrutura física adequada contra impactos, alagamentos ou incêndios.
- b) Acesso físico controlado e monitorado de acordo com as regras da indústria, incluindo o acompanhamento por colaborador do Banco na entrada e na saída, em caso de visitante. Para terceirizados, é realizada a integração e concedido crachá, quando assume responsabilidade pelas regras recebidas durante a integração.

Documentos em papel que contenham dados pessoais e que estão sob a responsabilidade do Banco não podem ser retirados da instituição sem autorização expressa prévia do Proprietário dos Dados Pessoais

daquele processo específico e do Encarregado dos Dados Pessoais, excetuados os casos para atendimento legal ou andamento do processo (ex. cartório).

11.2 Proteção em dispositivos e sistemas pessoais

O uso de dispositivos e sistemas pessoais (*notebooks, tablets, smartphones*, mídias portáteis de armazenamento de dados, sistemas de mensagens e de trabalho em grupo na nuvem, etc.) podem acarretar em riscos para a segurança dos dados pessoais.

Os colaboradores que necessitarem utilizar qualquer recurso não fornecido pela instituição para o tratamento de dados pessoais devem pedir autorização prévia ao responsável pela área solicitante e ao responsável pela área de Segurança da Informação (CNHI) que, por sua vez, caso entendam que o uso é de fato requerido, avaliarão o contexto e deverão implementar as medidas necessárias de proteção, de acordo com a Política Traga Seu Próprio Dispositivo e atendendo seus requisitos.

O processo de análise e autorização deverá considerar:

- a) A necessidade do uso do recurso.
- b) Os riscos à proteção de dados pessoais provenientes do uso deste recurso.
- c) A realização das atividades somente após a garantia da adoção das proteções necessárias.

11.3 Proteção de dados pessoais em meio eletrônico

11.3.1 Controles de Acesso

O acesso aos sistemas e redes do Banco que contém dados pessoais deve ser concedido por processos de identificação, autenticação e certificação de *login* e senha de acesso, devendo ser comprovada a necessidade do acesso para desempenho das atividades.

Cabe ao Proprietário de cada base dos dados pessoais determinar os controles apropriados para direito de acesso, concessão de privilégios e gerenciamento dos acessos concedidos aos dados pessoais sob a sua gestão.

11.3.2 Acesso externo

Em relação ao acesso externo a sistemas e equipamentos deve-se garantir a proteção dos dados pessoais.

O acesso externo deverá considerar:

- a) O usuário (colaborador, consultor, temporário, terceiro e demais indivíduos) a serviço do Banco deve obter autorização específica para o uso remoto de sistemas e equipamentos do banco.
- b) Equipamentos não podem ser deixados desprotegidos em áreas públicas, devendo sempre ser transportados pelos seus usuários.
- c) Convém que dispositivos e computadores portáteis sejam carregados como bagagem de mão e oportunamente descaracterizados para não chamar atenção indesejada, sempre que possível.
- d) Equipamentos não devem ser utilizados em área de circulação de pessoas, tal como aeroportos, saguão de hotéis, restaurantes e bares.
- e) Devem ser reforçados os cuidados sobre a segurança de dados pessoais.
- f) Qualquer problema relativo à proteção de dados pessoais deve ser reportado imediatamente ao Encarregado e ao respectivo Proprietário dos Dados Pessoais.

11.3.3 Proteção nas transferências de dados pessoais

Como os riscos de vazamento de informações são maiores nos processos que envolvem transferências entre diferentes equipamentos e/ou sistemas, visando a segurança e proteção de dados pessoais, as seguintes orientações devem ser seguidas por todos os colaboradores e prestadores de serviços:

- a) O uso de conexões aos sistemas da rede interna e da internet é permitido para todos os efeitos e propósitos de negócios, suporte, serviços e objetivos específicos do Banco. O uso destes recursos para outras finalidades é terminantemente proibido.
- b) Qualquer computador de propriedade do Banco ou de propriedade de prestadores de serviços a serviço do Banco, que estiver conectado à rede interna ou à internet, deverá estar devidamente configurado com sistemas de proteção contra a infestação de vírus ou de *software* malicioso.
- c) Todos os computadores, redes, sistemas e softwares estão sujeitos ao monitoramento e, portanto, o Banco poderá, a seu critério, manter o histórico de acessos e transações realizadas através das conexões da rede corporativa (interna) ou da internet (externa).
- d) Prospecções, varreduras ou outra forma qualquer de tentativa de invasão através de mecanismos de testes não podem ser realizadas sem a devida e expressa autorização, configurando assim, ameaça e tentativa de apropriação indevida de dados pessoais.
- e) Toda as conexões entre as redes internas do Banco e outras redes externas, inclusive a internet, deverão obrigatoriamente, ser franqueadas por um sistema específico, configurado e homologado, de *firewall*.
- f) As estações de trabalho devem estar habilitadas com programas específicos, homologados e configuradas para acesso à rede interna e à internet, podendo este ou aquele acesso ser inibido em atenção à solicitação formal do gestor do departamento interessado, do Proprietário ou do Encarregado dos Dados Pessoais, ou para a manutenção dos níveis de segurança de dados pessoais.
- g) A conexão de usuários às redes (internas e externas) deve ocorrer, única e exclusivamente, através de processos de identificação, autenticação e certificação de chave e senha de acesso.
- h) Dispositivos de controle e segurança (Servidor *Proxy*, *Firewall* e similares) deverão ser implementados para garantir a confidencialidade e a integridade de dados pessoais em tráfego por estas redes.
- i) Não realizar *downloads* de softwares não homologados, pois podem conter código malicioso e gerar ameaças à segurança dos dados pessoais.
- j) Manter as opções de compartilhamento de arquivos, a conexão automática em redes Wi-Fi e *Bluetooth* desabilitadas.
- k) Em quaisquer situações, independentemente do que foi anteriormente apontado, todo e qualquer arquivo proveniente de redes ou usuários externos deverão, obrigatoriamente, ser verificados por sistemas de proteção contra vírus e *software* malicioso.

Toda e qualquer transferência de dados pessoais para sistemas e pessoas externas ao Banco, por meio de quaisquer recursos de comunicação, deve ocorrer de maneira segura considerando os seguintes controles:

- a) Evitar o envio de dados pessoais através de mensagens de e-mail ou por outros serviços de mensagens. Idealmente, os dados pessoais devem ser acessados e transferidos usando somente os

recursos próprios dos sistemas de gestão e aplicativos da instituição.

- b) Não utilizar redes públicas (por exemplo, wi-fi público) para troca ou envio de dados pessoais, exceto se estiver adotando recursos de segurança e criptografia nesta comunicação (por exemplo, SSL e VPN).

11.3.4 Criação de perfis para tomada de decisão

O Banco possui aplicativo que emprega técnicas para a tomada de decisão automatizada a partir de dados pessoais, porém o titular pode solicitar os critérios da recusa, observando os segredos comerciais.

11.3.5 Comunicações em caso de incidentes

Um incidente de segurança pode ser qualquer evento que viole a proteção dos dados pessoais e dos dados pessoais sensíveis.

De acordo com a Lei, o Banco deverá comunicar à ANPD e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

O responsável pela Segurança da Informação deverá executar atividades de monitoramento, alerta, responsabilização, resposta, comunicação entre os envolvidos, documentação e registro dos incidentes, contemplando as seguintes atividades:

- a) O monitoramento e gerenciamento de incidentes de segurança relacionados aos dados pessoais, ou seja, que abranjam os bancos de dados dos sistemas, arquivos e locais da rede contendo dados pessoais.
- b) O tratamento e o registro das respostas aos incidentes e das respectivas correções aplicadas.
- c) A comunicação aos devidos responsáveis pela proteção dos dados pessoais, ao Encarregado e ao respectivo Proprietário dos Dados Pessoais, de toda e qualquer ocorrência relacionada à perda ou apropriação indevida de dados pessoais.

Cabe ao Encarregado dos Dados Pessoais convocar o Comitê de LGPD para analisar a severidade do incidente seguindo as instruções contidas nos documentos: Regras de avaliação e notificação de violação de dados pessoais, CNH_Autoavaliação e notificação de vazamento de dados pessoais e Notificação de vazamento- avaliação. Caso um incidente seja entendido como acarretando risco ou dano relevante aos titulares, o Encarregado dos Dados Pessoais deverá elaborar e realizar a devida comunicação à ANPD e aos titulares.

12. ATUALIZAÇÃO DA POLÍTICA

De acordo com a Política de documentação este documento deverá ser atualizado no mínimo anualmente.

13. GLOSSÁRIO

- **Anonimização:** utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
- **ANPD:** Autoridade Nacional de Proteção de Dados - órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.
- **Banco de Dados:** conjunto estruturado de dados, podendo ter dados pessoais, em meio eletrônico ou físico.
- **Bloqueio:** suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.
- **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

- **Controlador:** pessoa natural ou jurídica a quem compete determinar a finalidade e o meio de tratamento dos dados pessoais executadas pela própria Instituição ou pelo Operador.
- **Dado Anonimizado:** dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- **Dado Pessoal:** informação relacionada a pessoa natural identificada ou identificável.
- **Dado Pessoal Sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. (como estas definições estão no início do documento, penso que não seja necessário aqui)
- **Eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.
- **Encarregado dos Dados Pessoais:** função do Banco indicada para atuar como canal de comunicação entre a instituição, os titulares dos dados e a ANPD.
- **Operador:** prestador de serviço externo, terceirizado, que realiza a coleta, e/ou uso, e/ou o tratamento de dados pessoais dos quais o Banco é o controlador.
- **Portabilidade de dados pessoais:** transferência do tratamento de Dados Pessoais para outro fornecedor de serviço ou produto, mediante requisição expressa do titular dos dados.
- **Proprietário dos dados pessoais:** pessoa ou grupo de pessoas responsável pela coleta e tratamento dos dados pessoais.
- **PSI:** Política de Segurança da Informação, documento que estabelece diretrizes e normas gerais de segurança para todos os ativos de informação do Banco, incluindo dados pessoais e outros tipos de dados sensíveis e de valor para os negócios.
- **Titular dos dados:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- **Tratamento:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

14. OUTROS DOCUMENTOS RELACIONADOS

- Lei 13709/18- LGPD
- Procedimento de Administração de Acessos a Sistemas
- 200102PD001 Procedimentos Confidencialidade e Gestão de Documentos e Informação
- Políticas e Diretrizes de IT CNH e Globais
- Política de Segurança da Informação – CNH
- Política Traga Seu Próprio Dispositivo- CNH
- SEC-POL-Data Classification and Handling [Políticas de ICT \(sharepoint.com\)](#)
- Notificação de vazamento - avaliação
- CNH_Autoavaliação e notificação de vazamento de dados pessoais
- Regras de avaliação e notificação de violação de dados pessoais

HISTÓRICO DE ALTERAÇÃO

Data Publicação	Versão	Publicado por	Substitui/Log
Agosto/2020	1.0	Nilce Mocellin- Controles Internos	n/a
Agosto/2023	2.0	Nilce Mocellin- Controles Internos	V1- revisão periódica, inclusão dos documentos como instruções recebidas da equipe global de privacidade de dados: Regras de avaliação e notificação de violação de dados pessoais, Notificação de vazamento- avaliação e CNHI_Autoavaliação e notificação de vazamento de dados pessoais
Outubro/2024	3.0	Nilce Mocellin- Controles Internos	V2- revisão periódica, sem alteração significativa

ANEXOS

N/A

APROVAÇÃO

Heberson Goes – Presidência	Via sistema IB
Lorena Camargo - Controles Internos	Via sistema IB