# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

## CONGLOMERADO FINANCEIRO BARIGUI

**SUMÁRIO**

## 1. OBJETIVO

O objetivo desta política é promover as práticas de segurança para o transito das informações no âmbito do Conglomerado Financeiro Barigui, na forma de Diretrizes e Normas, para o trato de seus ativos e passivos, disseminando uma cultura de segurança das informações entre seus colaboradores, mantendo a segurança dos sistemas, a integridade e disponibilidade de dados, a confidencialidade das informações, a continuidade dos negócios e a aderência às leis e normas que regulamentam os negócios da indústria de serviços financeiros. A política sob referência visa, ainda, mitigar riscos que possam resultar em perda ou prejuízo, seja de ordem financeira ou de imagem para as empresas do Conglomerado.

Na busca constante pela excelência de nossos serviços, esta Política é uma declaração formal do Conglomerado Financeiro Barigui em relação ao seu comprometimento em proteger todas as suas informações sensíveis, apoiando metas e princípios de Segurança da Informação, a fim de garantir o cumprimento do objetivo acima, alinhado com estratégias de negócio.

Esta política e os demais procedimentos que suportam sua implementação estão em conformidade com as demais políticas do Conglomerado Financeiro Barigui.

## 2. APLICAÇÃO

Esta Política aplica-se a todos os colaboradores, em todos os níveis, parceiros e prestadores de serviços terceirizados, incluindo trabalhos executados externa e internamente que utilizem o ambiente de sistemas e dados do Conglomerado, ou que, de qualquer forma, tenham acesso a estas informações.

## 3. ATRIBUIÇÕES E RESPONSABILIDADES

Todo e qualquer colaborador ou prestador de serviços, utilizando-se ou não de recursos computadorizados do Conglomerado Financeiro Barigui, tem a responsabilidade de proteger a confidencialidade, a disponibilidade e a integridade das informações e dos equipamentos que as armazenam.

As atribuições e responsabilidades específicas estão descritas a seguir:

### 3.1 Conselho de Administração

Responsável pela aprovação da Política de Segurança de Informações (PSI), incluindo seus documentos anexos.

### 3.2 Diretoria

Responsável por criticar, revisar, implementar e garantir o cumprimento da PSI, devendo também aprovar a Política e seus Anexos, previamente a sua submissão ao Conselho de Administração.

Responsável também por indicar as principais diretrizes, referendando e adotando procedimentos, bem como delegando as demais responsabilidades.

### 3.3 Departamento de Tecnologia da Informação

Responsável por:

a) fornecer todos os recursos de tecnologia, incluindo ferramentas, hardware, software, serviços de TI e executar os processos necessários para o cumprimento das diretrizes e normas definidas na PSI;
b) garantir o funcionamento adequado e contínuo de todos os ativos de tecnologia sob sua responsabilidade;
c) desenvolver, implementar e executar os devidos procedimentos operacionais para a operação dos processos de segurança determinados nesta política;
d) realizar processos de avaliação de riscos para a segurança das informações, identificando ameaças e vulnerabilidades, gerando relatórios com os resultados conclusivos sobre tais avaliações de risco;
e) administrar e controlar os contratos com os fornecedores de serviços de TI e dos fornecedores de sistemas aplicativos, acompanhando e dando suporte às solicitações de alterações na infraestrutura e nos sistemas, quer sejam por demanda interna (solicitação de alteração ou desenvolvimento de nova funcionalidade) quanto por solicitação do próprio fornecedor (nova versão do pacote, por exemplo);
f) criar, manter e distribuir planos de resposta a incidentes de segurança e os devidos procedimentos de escalonamento, quando necessário, incluindo:

    - As estratégias de comunicação e definição de responsabilidades; e
    - Informações detalhadas sobre os incidentes e problemas relacionados.

Os planos devem ser também enviados para parceiros, como Adquirentes e Associações de Cartões, quando tais parceiros estiverem relacionados com o incidente ou com a solução.

### 3.4 Área de Segurança da Informação

Responsável por sugerir, definir, monitorar e garantir o cumprimento das Diretrizes, Normas e Procedimentos de segurança estabelecidos nesta Política e também nos respectivos procedimentos operacionais de TI, relacionados com as normas de segurança aqui estabelecidas.

Responsável por garantir que os procedimentos de contingenciamento e continuidade dos negócios do Conglomerado Financeiro Barigui estejam atualizados e testados conforme definido no PCN – Plano de Continuidade dos Negócios.

### 3.5 Departamento de Recursos Humanos

Responsável por criar e disseminar treinamentos de Conscientização da Segurança da Informação para todos os colaboradores do Conglomerado Financeiro Barigui, trabalhando em conjunto com o DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO e com a ÁREA DE SEGURANÇA DA INFORMAÇÃO, de forma a implementar um programa formal de conscientização da segurança das informações das Instituições do Conglomerado Financeiro Barigui e dos dados dos portadores de cartões.

Responsável por garantir que todos os colaboradores do Conglomerado Financeiro Barigui tenham ciência das diretrizes de segurança da informação presentes na Política.

Responsável por manter os termos assinados por todos os colaboradores e prestadores de serviço, referente à ciência e responsabilidade sobre a Política de Segurança da Informação. Tais termos devem estar anexos à documentação "Código de Conduta", o qual garante a ciência das informações contidas neste documento.

Responsável por comunicar o desligamento de funcionários ao DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO, para que o departamento desabilite/remova todos os acessos da pessoa desligada.

### 3.6 Áreas de Negócios

Responsáveis por manter termos e acordos, por escrito, que incluam o reconhecimento dos eventuais prestadores de serviços terceirizados, incluindo serviços de armazenamento, transmissão e processamento de dados, pela segurança dos dados dos usuários e clientes do Conglomerado Financeiro Barigui, incluindo mas não se limitando, aos dados dos portadores de cartões, de acordo com regras do PCI-DSS.

### 3.7 Todos os Colaboradores

Responsáveis por atender e disseminar todas as diretrizes e normas determinadas nesta *Política de Segurança da Informação*.

# 4. DIRETRIZES DE SEGURANÇA DAS INFORMAÇÕES

## 4.1 Diretrizes Gerais

A informação é um ativo de alto valor para o Conglomerado Financeiro Barigui e, assim, deve ser preservada e protegida, independentemente da forma de apresentação e armazenamento.

Na elaboração das normas de segurança específicas a cada ambiente e processo, o Conglomerado Financeiro Barigui seguiu diretrizes determinadas por seu Conselho de Administração, seguindo boas práticas de segurança das informações, garantindo a confidencialidade, integridade e disponibilidade das informações e dados processados nas suas operações e negócios.

As principais diretrizes adotadas na elaboração desta política foram as seguintes:

- Garantir que esta Política de Segurança da Informação e os procedimentos operacionais relativos ao cumprimento das normas aqui definidas estejam compatíveis com os requisitos legais e regulamentares aplicáveis ao Conglomerado Financeiro Barigui;
- Classificar as informações pelo grau de confidencialidade, adotando medidas de proteção para as informações classificadas como de acesso restrito e confidenciais;
- Manter processos de avaliação de risco, identificando ameaças e vulnerabilidades, gerando relatórios com os resultados conclusivos sobre as avaliações de risco.
- Gerenciar e controlar os acessos às contas de usuários, incluindo adições, exclusões e modificações. Os acessos a informações do Conglomerado Financeiro Barigui devem ser formalmente autorizadas;
- Manter, instalar e testar recursos e planos de contingência e continuidade dos negócios, mantendo também backups dos dados e sistemas críticos;
- Mídias que armazenam dados classificados como confidenciais devem ser armazenadas e protegidas de acordo com a sua classificação;

- Treinar e conscientizar os responsáveis e também os usuários, quanto às suas responsabilidades pela segurança das informações e pelas respostas a uma quebra de segurança;
- Prevenir intrusão e alertar caso seja detectada alguma anomalia na integridade dos dados;
- Revisar periodicamente os logs dos componentes críticos para a segurança dos dados das Instituições, incluindo as operações com cartões, tais como Firewalls, Autenticação, Autorização e Monitoramento de Acesso.
- Conservar as trilhas e os registros de auditoria referentes aos processos e recursos de segurança por um período mínimo de um ano.
- Garantir que todos os colaboradores e prestadores de serviço conheçam a cumpram com as exigências desta Política.

### 4.2 Diretrizes para o Comportamento Seguro

É importante que todos os colaboradores e prestadores de serviços adotem comportamento seguro com o objetivo de proteger as informações pertencentes ao Conglomerado Financeiro Barigui, com destaque para os seguintes itens:

- Diretores, gerentes, coordenadores, funcionários, parceiros e prestadores de serviços devem assumir atitude proativa no que diz respeito à proteção das informações do Conglomerado Financeiro Barigui.
- Os colaboradores e prestadores de serviços devem compreender as ameaças internas e externas que podem afetar a segurança das informações da empresa, tais como vírus de computador, interceptação de mensagens eletrônicas, uso de dispositivos não autorizados e homologados ao ambiente, uso de webmail, acesso a conteúdo suspeito e malicioso, bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação.
- Informações confidenciais ou de acesso restrito do Conglomerado Financeiro Barigui não devem ser transportadas em qualquer tipo de mídia sem as devidas proteções e autorizações.
- As senhas de usuários devem ser pessoais e intransferíveis, não podendo ser reveladas, compartilhadas, registradas em locais vulneráveis, como papel, etiquetas e dispositivos eletrônicos.
- Assuntos confidenciais só podem ser falados/comentados em áreas restritas do Conglomerado Financeiro Barigui, não podendo ser reveladas em ambientes públicos, como elevadores, taxis, restaurantes, etc.
- Dúvidas sobre a Política e Normas de Segurança da Informação devem ser imediatamente esclarecidas com os Gestores ou o responsável da área de SEGURANÇA DA INFORMAÇÃO.

## 4.3 Diretrizes para Propriedade Intelectual

Todos os documentos produzidos por intermédio de recurso originado de processamentos informatizados do Conglomerado Financeiro Barigui são de propriedade do Conglomerado Financeiro Barigui, assim como todo e qualquer registro de dados, voz e/ou imagem armazenados em meio magnético, óptico, eletrônico, impresso ou qualquer outro veículo de exibição.

Toda informação de propriedade do Conglomerado Financeiro Barigui deve ser tratada de acordo com a sua classificação.

## 4.4 Diretrizes para Privacidade e Proteção de Dados Pessoais

Informações armazenadas, tratadas ou enviadas por meio de recursos do Conglomerado Financeiro Barigui são consideradas informações profissionais.

Os dados pessoais de funcionários, colaboradores, parceiros e clientes deverão ser tratados conforme a finalidade de uso autorizada pelo titular, e pelo tempo informado e necessário para este uso, conforme definido na Lei Geral de Proteção de Dados.

Todos os dados pessoais de colaboradores, parceiros e clientes serão considerados dados confidenciais. O Conglomerado Financeiro Barigui se compromete em não acumular ou manter intencionalmente dados pessoais de colaboradores, parceiros e clientes além daqueles relevantes na condução do seu negócio. Adicionalmente, os dados pessoais de colaboradores, parceiros e clientes sob a responsabilidade do Conglomerado Financeiro Barigui não serão usados para fins diferentes daqueles para os quais foram coletados e não serão compartilhados com terceiros, exceto quando exigido pelo negócio, e desde que o proprietário dos dados autorizem formalmente a compartilhar tais informações.

Todos os dados trafegados nos ambientes físicos e sistêmicos do Conglomerado Financeiro Barigui estão sujeitos a monitoramento. Assim, ao utilizar qualquer recurso do Conglomerado Financeiro Barigui, os usuários automaticamente consentem este monitoramento.

## 4.5 Diretrizes para Gerenciamento de Incidentes e Problemas

Procedimentos operacionais para o atendimento, registro, resposta, correção, monitoramento e prevenção de incidentes e problemas relacionados com segurança da informação devem ser definidos e documentados pelo Departamento de TI e pela área de Segurança da Informação, a fim de garantir a segurança dos dados e a continuidade dos serviços disponibilizados para os usuários internos e externos.

Os procedimentos de resposta a incidentes de segurança devem também prever escalonamento, quando necessário, assegurando a administração oportuna e eficiente de todas as situações. Para este fim, devem ser definidos níveis de responsabilidade para respostas aos alertas e incidentes de segurança.

### 4.6 Diretrizes de Atendimento ao PCI-DSS

Toda documentação de segurança da informação desenvolvida pelo Conglomerado Financeiro Barigui, além de garantir a confidencialidade, integridade e disponibilidade da informação, deve também atender a todos os requisitos do PCI-DSS, garantindo assim a segurança dos dados do portador do cartão dos clientes do Conglomerado Financeiro Barigui.

Todos os funcionários que forem ter acesso ao ambiente escopo de avaliação do PCI-DSS, ou seja, que forem trabalhar no ambiente que possua dados do portador do cartão devem ter verificações referentes ao histórico do emprego anterior e verificação das referências curriculares. Esta verificação deve ser feita de acordo com o que a legislação permite e requer.

Deve haver documentação formalizando a confirmação de que os prestadores de serviço são também responsáveis pela segurança dos dados dos portadores de cartões.

## 5. CLASSIFICAÇÃO DAS INFORMAÇÕES

Todos os ativos de informação devem ser identificados, inventariados, ter classificações definidas e seus gestores responsáveis designados.

Deve ser definido e estabelecido um processo para a classificação das informações do Conglomerado Financeiro Barigui, de forma que estas possam ser mantidas protegidas de acordo com sua relevância e grau de confidencialidade para os processos de negócios do Conglomerado Financeiro Barigui.

É de responsabilidade do Gerente/Supervisor/Coordenador de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (cadastros, dados de transações, logs, relatórios e/ou mídias) gerada por sua área, de acordo com os níveis abaixo:

**1 – Informação Pública**

Toda informação que pode ser acessada por todos os usuários da organização, clientes, fornecedores, prestadores de serviços, podendo e/ou devendo ser divulgada para o público em geral. Geralmente este tipo de informação refere-se a Marketing, Dados Legais Públicos, Relações com Investidores, Ouvidoria, etc.

**2 – Informação de Acesso Restrito**

Toda informação que pode ser acessada por determinado grupo de usuários/colaboradores da organização, e, em alguns casos, somente mediante aprovação submetida a alçadas de poderes. Geralmente, a divulgação não autorizada dessa informação pode causar impactos financeiros, de imagem ou operacionais ao negócio da organização ou ao negocio do parceiro;

**3 – Informação Confidencial**

Toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia negocial da organização. Estes tipos de acessos devem ter reconhecimento da Diretoria, Controladoria e Compliance deste Conglomerado Financeiro.

Informações de terceiros sob responsabilidade ou custódia do Conglomerado Financeiro Barigui devem ser, se não classificadas formalmente, submetidas a medidas e critérios estabelecidos entre as partes, alinhadas com o processo de classificação interno, as cláusulas contratuais e aos termos de sigilo estabelecidos.

## 6. NORMAS DE SEGURANÇA DAS INFORMAÇÕES

### 6.1 Plano de Continuidade de Negócios

Cabe ao Departamento de Tecnologia da Informação e à área de Segurança da Informação definirem, em conjunto com as demais áreas das empresas do Conglomerado, o desenvolvimento, manutenção e testes de um Plano de Continuidade dos Negócios (PCN), que determine, no mínimo:

1. Os principais serviços críticos que não podem ser interrompidos por um longo período de tempo;
2. Os riscos e eventos possíveis de ocorrer, que podem impactar na perda de continuidade destes serviços. Por exemplo: falhas técnicas (internas ou externas) ou eventos de força maior (catástrofes ou intervenção externa como ação sindical, por exemplo);
3. O tempo máximo de recuperação (RTO – Recovery Time Objective) de cada um dos serviços críticos definidos;
4. Os responsáveis pelo diagnóstico da situação e acionamento do Plano; e
5. Os procedimentos a serem executados para a recuperação de cada um dos serviços críticos impactados e os respectivos responsáveis por sua execução.

O PCN deverá prover a rápida retomada das atividades e garantir a segurança de todos os funcionários e prestadores externos que porventura estejam nas dependências do Banco.

O PCN deverá ser revisado e aprovado pela Diretoria e pelo Conselho de Administração. Para os casos de necessidade de alteração no PCN, o Departamento de Tecnologia e a área de Segurança da Informação devem atualizar o documento e informar a nova versão a todos os colaboradores, bem como submeter para nova aprovação pela Diretoria e Conselho.

Treinamento específico e testes do PCN devem ser programados de acordo com um calendário a ser definido pelo Departamento de Tecnologia da informação, com aprovação da Diretoria.

Os resultados dos testes de execução do PCN devem demonstrar o atendimento aos tempos de recuperação definidos (RTO). Tais testes devem ser sempre documentados, gerando evidências que possam ser consultadas sempre que requerido e necessário.

## 6.2 Gestão da Disponibilidade de Sistemas e Informações

Cabe à área de Segurança da Informação a responsabilidade de definir os procedimentos operacionais para o planejamento, controle, resposta e monitoramento de riscos que possam impactar na disponibilidade dos sistemas e dados, bem como dos serviços de TI do Conglomerado Financeiro Barigui.

Para isso, a área deverá atuar em conjunto com o Departamento de Governança, inserindo e atualizando os riscos relacionados na Matriz de Riscos do Conglomerado Financeiro Barigui, com o apoio das demais áreas, com o objetivo de:

- Monitorar se as respostas definidas para cada um dos riscos identificados estão sendo efetivas para uma adequada mitigação.
- Avaliar se não há riscos que não mais se aplicam aos negócios e ao ambiente do Conglomerado. Neste caso, estes riscos podem ser eliminados da matriz de riscos.
- Avaliar se não há outros ou novos riscos que possam impactar na disponibilidade dos sistemas e serviços de TI da instituição. Neste caso, estes novos riscos devem ser adicionados à matriz, bem como as demais informações relacionadas, incluindo as respostas para mitigação e seus responsáveis.

Por questões de confidencialidade das informações, a Matriz de Riscos deverá ser armazenada em local seguro com acesso somente ao pessoal do Departamento de Governança e da Diretoria.

Caberá também à área de Segurança da Informação a responsabilidade de informar ao Departamento de Governança os fatos apurados no tocante aos riscos listados na matriz de riscos do Conglomerado Financeiro Barigui. Em havendo a materialização de impactos

relativos à disponibilidade dos sistemas, informações e serviços de TI, deve a área de Segurança da Informação esclarecer as ocorrências e os planos de ação para mitigação daqueles riscos.

Merece realce o fato de que novos riscos podem ser identificados, ocorrência que deverá gerar pronta comunicação ao Departamento de Governança para inserção na Matriz de Riscos, informando as áreas e/ou serviços impactados.

### 6.3 Gestão de Problemas e Incidentes de Segurança

O Departamento de TI deverá desenvolver e manter um procedimento operacional, detalhando as atividades do processo de Gerenciamento de Incidentes e Problemas relacionados com segurança das informações e demais aspectos de TI.

O escopo deste processo de Gerenciamento de Incidentes e Problemas deve incluir qualquer evento que interrompa ou que possa interromper um serviço de TI, ou que impacte em perda da confidencialidade, integridade e disponibilidade de qualquer informação importante para os negócios.

O processo de Gerenciamento de Incidentes e Problemas deve abranger eventos que podem ser:

- Identificados pelas áreas de TI, incluindo Segurança da Informação;
- Identificados pelo Departamento de Governança; e
- Comunicados diretamente pelos usuários, usando os seguintes canais: telefone, e-mail, ou por sistema de gestão de help desk (ferramenta específica para o registro e controle de chamados definidos pelo Conglomerado Financeiro Barigui).

O escopo do processo de Gerenciamento de Incidentes e Problemas, bem como as ferramentas de registro de chamados de help desk devem abranger todas as informações e registros de incidentes e problemas, tanto para Tecnologia da Informação como para desenvolvimento e manutenção de sistemas aplicativos.

Com base nas definições a seguir, uma lista de prioridades de atendimento deve ser elaborada sob a responsabilidade do Departamento de Tecnologia da Informação, bem como as evidências que deverão ser documentadas sobre cada atendimento:

- Incidente: refere-se a qualquer falha pontual ou um evento que não seja parte da operação normal de um serviço, que venha causar uma redução na qualidade ou indisponibilidade temporária daquele serviço;
- Problema: refere-se a qualquer falha ininterrupta e ainda não corrigida, ou um evento que não seja parte da operação normal de um serviço e que esteja causando uma suspensão na disponibilidade daquele serviço.

- Categorização do chamado: os chamados serão categorizados de acordo com o atendimento a ser realizado, sendo categorizados como incidentes problemas ou requisições de serviço e solicitações de melhoria.
- Priorização do chamado: a priorização do chamado deve ser realizada em conjunto com o usuário envolvido, e, sopesada sua relevância, com a Diretoria, com base no incidente identificado, para estabelecer sua prioridade e urgência de resolução.

Caso o incidente seja relacionado com indícios ou fatos de perda de confidencialidade ou violação de documentos sigilosos, o Gestor da Informação deve informar, formal e imediatamente, seu superior hierárquico, a Diretoria, o departamento de TI e a área de Segurança da Informação, que devem adotar medidas imediatas para remediação e para mitigar a vulnerabilidade causadora do ocorrido.

## 6.4 Gerenciamento de Mudanças

O Departamento de TI desenvolveu e mantém um procedimento operacional, detalhando as atividades do processo de Gerenciamento de Mudanças na Infraestrutura e nos Sistemas, de forma a garantir a disponibilidade, integridade e confidencialidade das informações, sistemas e infraestrutura.

O processo de Gerenciamento de Mudanças tem como objetivo atender demandas relacionadas com mudanças na Infraestrutura de TI e sistemas informatizados do Conglomerado Financeiro Barigui. Tais mudanças podem ser necessárias para garantir a segurança das informações.

O processo prevê duas categorias básicas de mudanças – normal e emergencial, garantindo que todas as atividades de mudança sejam documentadas, testadas, evidenciadas e aprovadas conforme as alçadas definidas.

## 6.5 Segurança Física

Todos os ativos de informação devem ser protegidos de acordo com a criticidade e importância para o Conglomerado Financeiro Barigui.

Os ativos classificados como confidenciais e de acesso restrito devem contar com recursos que restrinjam e controlem o acesso físico.

O Departamento de TI e a área de Segurança da Informação são responsáveis pelo controle e monitoramento dos acessos físicos aos ativos de tecnologia e também pela definição de procedimentos e indicadores necessários para a efetiva gestão destes acessos.

Todas as áreas que armazenam dados e informações classificadas como confidenciais e de acesso restrito devem contar com câmeras de monitoramento, bem como também áreas comuns, que dão acesso a estas áreas de proteção.

Adicionalmente, deve haver controles de acesso através de liberação biométrica na entrada para colaboradores do Conglomerado Financeiro Barigui, para acessos aos Departamentos de Tecnologia da informação e Tesouraria. Somente colaboradores destes departamentos poderão acessar tais áreas. Pessoal de outros departamentos e terceiros somente poderão ter acesso a estas áreas por meio de requisição previamente aprovada pelo responsável do departamento.

O acesso de visitantes às dependências do Conglomerado Financeiro Barigui deverá sempre ocorrer após a autorização de um funcionário e sempre acompanhado do mesmo.

## 6.6 Segurança Lógica e Gestão de Acessos Lógicos

A rede local utilizada para o acesso dos colaboradores aos sistemas de gestão das operações de negócios do Banco deve ser segregada logicamente de qualquer outra rede que permita acesso público.

Fornecedores e prestadores de serviços devem usar conexão independente e segregada para acesso à Internet, não podendo utilizar a rede dos sistemas de produção do Conglomerado Financeiro Barigui.

Para garantir a segurança dos acessos lógicos às redes, sistemas, dados e demais serviços que fornecem informações, deve haver um processo de gerenciamento de acessos, que vise assegurar que as concessões e alterações em direitos de acesso sejam realizadas de forma controlada (avaliadas, registradas e aprovadas), reduzindo o risco e impacto de perda de confidencialidade, disponibilidade e integridade das informações.

O processo de Gerenciamento de Acessos Lógicos tem como objetivo atender demandas relacionadas com os diferentes níveis de acessos lógicos à Rede, aos Sistemas e aos Bancos de Dados do Conglomerado Financeiro Barigui e deve garantir a opção de restrição de acesso aos dados, sistemas e demais recursos que armazenam e processam informações.

O Departamento de TI e a área de Segurança da Informação são responsáveis por definir e disponibilizar o processo e ferramentas que permitam:

- Concessão de acessos à rede e sistemas (acesso somente ao que o usuário necessita);
- Alteração de acessos na rede e sistemas;
- Revogação de acessos;
- Revisão periódica de perfis de acessos sistêmicos (acesso e autoridade para execução das atividades);
- Administração da rede, sistemas e Bancos de Dados (incluindo acessos de terceiros);

- Gestão de usuários não nominais (genéricos).

Procedimentos de revisões periódicas devem ser implementados com prazo máximo de 06 meses e devem ser devidamente formalizados e evidenciados. Alterações sistêmicas que demandem revisões de acessos e autoridades mais complexas devem ser planejadas antes de implementação em ambiente de produção.

Acessos privilegiados, por exemplo, contas e logins de administração de equipamentos, sistemas operacionais, bancos de dados e sistemas aplicativos, deverão ser tratadas com extrema cautela e controles que previnam o seu uso indevido.

Acessos privilegiados são considerados aqueles concedidos para atualização, manutenção e administração dos sistemas, serviços e fluxos de trabalho que possam comprometer os controles de segurança existentes.

A concessão de acesso privilegiado deve ser solicitada formalmente, e por escrito, pelo gestor do colaborador ao gestor da informação, assim como, ao gestor do Departamento de Tecnologia e da área de Segurança da Informação. A autorização referente a esta solicitação, quando concedida, deverá ser apresentada formalmente e por escrito.

Todo e qualquer acesso privilegiado concedido deverá possuir, no mínimo:

- Registro de controle e acompanhamento de todos os acessos concedidos, sob a responsabilidade da área de Segurança da Informação.
- Geração de logs para os logins que possuírem tais acessos.

Para o gerenciamento de senhas do usuário, as senhas devem ser criadas e compostas de acordo com os privilégios atribuídos às suas contas, devendo, portanto, ser tratadas como senhas administrativas e senhas não administrativas. As primeiras são aquelas associadas às tarefas de manutenção e administração de sistemas e ambientes computacionais, enquanto as últimas são aquelas senhas cujas contas são utilizadas para as atividades rotineiras e sem os privilégios de acesso concedidos às tarefas de manutenção e administração de sistemas.

Os técnicos do Departamento de TI deverão configurar os sistemas do Conglomerado Financeiro Barigui (sistemas operacionais, banco de dados, etc.) para que as senhas expirem a cada 90 dias, tanto para as senhas administrativas tanto para as senhas não administrativas.

As senhas devem ser criadas evitando o uso de combinações de fácil dedução, e considerando os aspectos a seguir para a sua composição:

- As senhas devem ter um tamanho mínimo de oito caracteres;
- Devem ser formadas a partir da combinação de caracteres alfabéticos, maiúsculos e minúsculos, numéricos e especiais (%, #, $, @, &, entre outros);
- Não é recomendado usar:

- Palavras encontradas em dicionários de qualquer idioma;
- Dados pessoais, tais como: datas, placas de carro, nomes próprios e de pessoas conhecidas;
- Palavras, números ou letras repetidos, em sequência ou formando séries óbvias, como, por exemplo, "senhasenha", "aaaabbbb", "12345678", "Ana0000";
- Não deve ser permitida a reutilização das últimas 6 (seis) senhas.

Quando for solicitada alteração de senha, deverão ser criados procedimentos de identificação que possam assegurar que o solicitante é o proprietário da senha a ser alterada.

Quando da necessidade de impressão das senhas, devem ser criados procedimentos para que as mesmas não sejam reveladas a pessoas não autorizadas.

As bases que contêm as senhas dos usuários devem ser protegidas contra acesso não autorizado, bem como separadas das outras informações do Conglomerado Financeiro Barigui.

Quando houver suspeita de vazamento das senhas dos usuários, as mesmas deverão ser alteradas imediatamente pelo Departamento de Tecnologia da Informação e os usuários e seus gestores diretos deverão ser notificados, conforme o caso e extensão do incidente.

Devem ser disponibilizados mecanismos que permitam ao usuário a troca da senha quando o mesmo considerar necessário.

### 6.7 Uso de Dispositivos Móveis

O uso de dispositivos móveis de propriedade dos funcionários e prestadores de serviços dentro do ambiente do Conglomerado Financeiro Barigui é permitido, porém tais dispositivos somente podem ser conectados a redes públicas, segregadas das redes dos sistemas de produção do Conglomerado Financeiro Barigui

Equipamentos pessoais de funcionários e prestadores de serviço devem estar abrangidos nos termos e cláusulas de confidencialidade nos contratos de trabalho e de prestação de serviços.

Em casos excepcionais, em que seja necessário o uso na rede dos sistemas de negócios, em decorrência de atividade ou situação específica, o colaborador deverá enviar solicitação formal ao gestor da área de Segurança da Informação, contendo aprovação prévia da Diretoria. O gestor da área de Segurança da Informação avaliará o cenário e concederá acesso temporário, desde que o grau de risco esteja dentro de parâmetros aceitáveis.

Os dispositivos móveis fornecidos pelo Conglomerado Financeiro Barigui para uso de seus colaboradores poderão ser conectados às redes dos sistemas de produção, inclusive redes WI-FI.

## 6.8 Uso de Softwares e Aplicativos

Apenas os aplicativos e softwares disponibilizados, homologados e aprovados pelo Conglomerado Financeiro Barigui são permitidos para uso nos equipamentos do Banco.

É proibida a instalação de qualquer software ou aplicativo pelo próprio usuário. Todo e qualquer software somente poderá ser instalado pelo Departamento de TI.

A instalação ou uso de software não autorizado pelo Departamento de Tecnologia da Informação pode ocasionar riscos graves para a segurança das informações do Conglomerado Financeiro Barigui, ficando o seu responsável sujeito às sansões cabíveis.

## 6.9 Transporte de Informações

As informações classificadas como confidenciais e de acesso restrito devem ser transportadas, ou seja, transferidas de seu local habitual de armazenamento, somente com autorização prévia e formal do Gestor da informação, em conjunto com a área de Segurança da Informação.

As informações confidenciais devem ser transportadas somente de forma controlada e registrada. Independentemente da forma adotada no transporte, o processo deve conter uma mensagem ao portador ou transportador, identificando o grau de sigilo daquela informação, bem como uma advertência para que o responsável pelo transporte redobre a atenção durante o processo, evitando descuidos que possam diminuir o grau de segurança do processo.

Todo arquivo de origem desconhecida ou conhecidamente de procedência externa, transportados por meios não seguros, como Pen-drive, USB Drive, Flash Memory, discos rígidos ou SSDs externos, CD/DVD/Blue Ray, celulares, máquinas fotográficas, Internet, ou qualquer outro meio de armazenamento e transporte de dados deve ter o seu conteúdo verificado pela Área de Segurança da Informação antes de ser copiado para qualquer equipamento do Banco.

## 6.10 Uso de E-mail e Outras Formas de Mensagens Eletrônicas

O e-mail (...@bancobari.com.br) e as demais formas de comunicação e trocas de mensagens eletrônicas disponibilizadas aos colaboradores pelo Conglomerado Financeiro Barigui devem ser exclusivamente utilizadas para mensagens profissionais, relacionadas com os negócios do Banco.

Vale relembrar que, ao redigir qualquer tipo de mensagem escrita, incluindo e-mails, os colaboradores devem redobrar sua atenção para evitar que as mensagens possam ser interpretadas como contendo comentários de cunho não profissional, abusivos, obscenos ou difamatórios, ou ainda qualquer outro material que possa trazer má publicidade, risco à imagem ou constrangimento público para o Conglomerado Financeiro Barigui, seus clientes, prestadores de serviços, parceiros ou acionistas.

É importante destacar a todos os colaboradores e prestadores de serviços que o e-mail é uma forma de comunicação extremamente vulnerável e passível de leitura e interceptação por terceiros. Assim, deve-se evitar a utilização do e-mail para troca de mensagens com informações confidenciais e/ou estratégicas para os negócios do Conglomerado Financeiro Barigui. Quando necessário, recomenda-se adotar criptografia nos arquivos anexados ou o uso de canais mais seguros, tais como: transferência eletrônica com protocolos seguros (por exemplo, SFTP) ou cópias gravadas em pastas seguras nos servidores de rede.

Adicionalmente, é terminantemente proibido o envio de documentos e informações classificadas como confidenciais ou de acesso restrito para e-mails pessoais ou em provedores públicos, tais como Gmail, Hotmail, Outlook, Yahoo e outros.

O Conglomerado Financeiro Barigui reserva-se ao direito de monitorar o conteúdo e armazenar todas as mensagens - de e-mail e de outras formas de comunicação eletrônica - que trafeguem pelos meios por ele disponibilizados, com o objetivo de se resguardar e assegurar as boas práticas de segurança, conforme determinado nesta Política.

Destaca-se também que o emitente das mensagens é considerado o único responsável pela segurança das informações contidas nestas mensagens.

### 6.11 Impressão de Documentos

Os equipamentos de impressão deverão ser configurados para somente imprimir documentos quando os usuários digitarem uma senha (PIN) presencialmente no equipamento.

Os colaboradores deverão recolher o material impresso imediatamente.

Todo o funcionário que constatar a presença de documentos impressos nos equipamentos sem a devida atenção do responsável, deverá comunicar o fato ao gestor daquelas informações, ao responsável pela área de Segurança da Informação e à área de Compliance, que têm autonomia para destruir o que foi encontrado e não retirado da impressora, além de informar ao superior hierárquico do infrator.

Todo e qualquer documento somente deverá ser impresso se for estritamente necessário, observando princípios de preservação ambiental.

## 6.12 Mesa Limpa

O colaborador deverá sempre bloquear seu computador ao deixar a estação de trabalho, ainda que momentaneamente e não deverá deixar informações sensíveis ou confidenciais disponíveis ao alcance de outras pessoas.

Ao final do expediente, todo colaborador deverá guardar todos os documentos em local fechado com chave e desligar sua estação de trabalho, a fim de deixar a sua mesa limpa e sem nenhum tipo de informação disponível.

Deve-se, ainda, manter os armários e gaveteiros devidamente trancados, evitando assim o acesso indevido a informações do Conglomerado Financeiro Barigui.

## 6.13 Segurança Cibernética

O Departamento de Tecnologia da Informação deve descrever as atividades de planejamento, controle, resposta e monitoramento dos mecanismos de Segurança Cibernética, ou seja, de proteção e segurança para prevenir, detectar e reduzir vulnerabilidades a ataques digitais à infraestrutura de TI que suporta os principais sistemas e dados de operação dos negócios do Conglomerado Financeiro Barigui, incluindo os dados sensíveis aos negócios, classificados como "Confidenciais" e de "Acesso restrito" na Classificação das Informações do Conglomerado Financeiro Barigui.

Os objetivos dos procedimentos de gerenciamento de segurança e proteção contra-ataques digitais são:

- Identificar e conhecer as principais vulnerabilidades que podem permitir que um atacante, ou seja, uma pessoa não autorizada, seja ela interna ou externa, acesse informações, dados ou sistemas de negócios do Conglomerado Financeiro Barigui ou de seus clientes;
- Monitorar a eficácia dos processos e recursos de proteção contra os ataques digitais (Cyber Security), além de planejar e executar ações preventivas, sempre que necessário;
- Definir e executar ações corretivas de novas vulnerabilidades identificadas;
- Definir e executar ações de resposta a incidentes e problemas relacionados com ataques digitais.

Haverá uma política específica para tratar todos os aspectos e processos relacionados com Segurança Cibernética.

## 6.14 Integrações e Interfaces Sistêmicas

Os sistemas do Conglomerado Financeiro Barigui possuem rotinas automatizadas e interfaces com outros sistemas e instituições externas (regulatórias ou não), de forma que devem estar disponíveis para atender às demandas requeridas.

Os principais sistemas financeiros do Conglomerado Financeiro Barigui são o Lydians, Sicred, Prognum e ERSystems. Considerando a criticidade das interfaces e integrações entre estes sistemas, assim como das integrações de dados entre estes sistemas e outros sistemas externos, o Departamento de TI deverá garantir a existência de controles de integridade dos dados trafegados e pelo monitoramento das rotinas de troca de dados nestas interfaces sistêmicas, considerando as seguintes atividades:

- Desenvolvimento de rotinas de integração utilizando controles de prevenção contra perda de integridade dos dados. Por exemplo: adoção de controles automáticos utilizando recontagem da quantidade de registros, conciliação de valores totalizadores de campos, etc.
- Configuração das rotinas e interfaces para o envio automático de mensagens de alerta ao Departamento de Tecnologia da informação, no caso de falhas na execução;
- Tratativa de todos os erros (por exemplo: reexecução da rotina);
- Coleta e armazenamento de evidência da execução destas tratativas;
- Registro formal, em chamado, da tratativa do erro de execução.

Somente as áreas de TI (e os respectivos fornecedores dos sistemas, mediante aprovação do Gestor da Informação) poderão alterar as rotinas e os códigos executados nas interfaces entre os sistemas do Conglomerado Financeiro Barigui.

### 6.15 Telecomunicações e conectividade

Os servidores contendo sistemas e dados críticos do Conglomerado Financeiro Barigui estão protegidos por soluções de "Firewall" nas conexões internas e externas, soluções estas administradas pelo Departamento de TI do Grupo Comercial Barigui.

O controle de uso, a concessão de permissões e a aplicação de restrições em relação ao uso dos links de comunicação de dados e dos ramais telefônicos do Conglomerado Financeiro Barigui, assim como o uso de eventuais outras formas de comunicação utilizando tais recursos, como os ramais virtuais instalados nos computadores, é de responsabilidade do Departamento de Tecnologia da Informação e da área de e Segurança da Informação deste Conglomerado Financeiro Barigui, de acordo com as definições da Diretoria.

Todos as formas de comunicação, incluindo ramais telefônicos, são monitorados e podem ter suas atividades gravadas e armazenadas em mídias internas do Conglomerado Financeiro Barigui. Estas gravações são armazenadas por um período de 5 (cinco) anos, conforme regulamentos do CMN e do Banco Central do Brasil.

Para recuperação de um registro de ligações realizadas nas dependências deste Conglomerado Financeiro Barigui, deverá ser aberto um chamado para o Departamento de TI, com aprovação prévia do Diretor responsável por aquele ramal.

### 6.16 Bancos de Dados

As regras de segurança para as informações armazenadas e processadas por sistemas gerenciadores de bancos de dados são definidas pelo Departamento de Tecnologia da Informação e pela área de Segurança da Informação do Conglomerado Financeiro Barigui.

Já a disponibilização, manutenção, atualização e proteção dos bancos de dados dos sistemas aplicativos contendo informações classificadas como confidenciais e de acesso restrito, bem como dos servidores que contém estes bancos de dados, são de responsabilidade do Departamento de TI do Grupo Barigui, sendo estes serviços contratualmente acordados entre as partes.

Cabe ao Departamento de Tecnologia da Informação do Conglomerado Financeiro Barigui monitorar o funcionamento das operacionalidades transacionais ocorridas nos bancos de dados do Conglomerado Financeiro Barigui. Este Departamento deverá ainda reportar formalmente ao Departamento de TI do Grupo Comercial Barigui qualquer alerta, evidências e/ou suspeita de mau funcionamento, inoperância ou vulnerabilidades de segurança nestes serviços.

Em caso de catástrofes ou falhas nos servidores de banco de dados, é também de responsabilidade do Departamento de TI do Grupo Barigui a recuperação do hardware e dos respectivos softwares afetados, ficando somente ao Departamento de Tecnologia da Informação do Conglomerado Financeiro Barigui a responsabilidade pela reconfiguração lógica destes serviços.

### 6.17 Contratação de Terceiros

No tocante aos critérios de decisão quanto à terceirização de serviços, deve haver uma atenção especial a serviços relevantes de desenvolvimento e manutenção de sistemas, além de processamento e armazenamento de dados e de computação em nuvem, estes últimos ao amparo da Resolução CMN nº 4.658.

Assim, previamente à contratação de tais serviços, o Conglomerado Financeiro Barigui deve adotar procedimentos que contemplem a adoção de práticas de governança e gestão proporcionais à relevância do serviço a ser contratado e aos riscos relacionados, além da verificação da capacidade do potencial prestador de serviço de assegurar: o cumprimento da legislação e da regulamentação em vigor;

- o acesso do Conglomerado Financeiro Barigui aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

- a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
- a sua aderência a certificações exigidas pelos órgãos reguladores para a prestação do serviço a ser contratado;
- o acesso do Conglomerado Financeiro Barigui 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, caso exista;
- o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- a identificação e a segregação dos dados dos clientes do Banco, por meio de controles físicos ou lógicos; e
- a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes do Banco.

Na avaliação da relevância do serviço a ser contratado, mencionada acima, a o Conglomerado Financeiro Barigui deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado e/ou pelos sistemas desenvolvidos e/ou mantidos pelo contratado.

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

Para o cumprimento destes termos, o fornecedor a ser contratado deverá, antes da contratação, apresentar uma declaração relacionando todos os processos e controles de segurança de informações que adota em seu ambiente interno e também os que adotará na execução dos serviços ao Conglomerado Financeiro Barigui, para atendimento dos aspectos relacionados acima.

O Conglomerado Financeiro Barigui deverá avaliar a suficiência de tais controles para a execução dos serviços objeto do contrato e poderá auditar estes controles antes de aprovar a contratação do fornecedor.

Os procedimentos desta avaliação devem ser documentados.

### 6.18 Guarda e Uso de Chaves de Criptografia Privadas

O Departamento de TI e a Área de Segurança da Informação devem garantir que cada chave privada de criptografia, incluindo os arquivos e dispositivos contendo os certificados digitais do Conglomerado Financeiro Barigui, possuam pelo menos uma cópia de segurança, guardada em local seguro, preferencialmente em cofre trancado.

A área de Segurança da Informação será a responsável por definir o custodiante de cada chave privada, bem como será o responsável pela guarda segura da cópia daquela chave.

Os custodiantes devem ser escolhidos levando em consideração critérios éticos, além de seu histórico e reputação. Devem também ter, ao menos, conhecimentos mínimos de computação e de como manipular arquivos digitais de forma segura.

A área de Segurança da Informação deve orientar os custodiantes acerca de sua responsabilidade, das práticas corretas de manuseio com segurança das chaves privadas e do prazo de custódia. Deve também exigir que os custodiantes assinem um Termo de Compromisso e Responsabilidade.

O Termo de Compromisso e Responsabilidade deve possuir, pelo menos, os seguintes termos:

- Que o custodiante se compromete a manter em sigilo que está custodiando chaves privadas;
- Que o custodiante se compromete a manter em sigilo o local de guarda da chave privada;
- Que o custodiante não irá entregar a chave privada para ninguém, salvo quando solicitado formalmente pela área de Segurança da Informação e após aprovado pela direção do Conglomerado Financeiro Barigui;
- Que o custodiante deve manter a chave privada em local seguro, não identificado e protegido por senha; e
- O prazo de custódia será de, no máximo, 5 (cinco) anos.

A área de Segurança da Informação deve garantir que os custodiantes das chaves privadas não tenham acesso ao ambiente de produção das bases de dados criptografados, incluindo dados de cartões.

A área de Segurança da Informação deve solicitar a chave privada ao custodiante quando:

- O método de criptografia se tornar obsoleto. Neste caso, a chave será usada para refazer o banco de dados usando os métodos mais recentes e seguros;
- Houver comprometimento ou suspeita de comprometimento da chave privada ou do banco de dados; ou
- O tempo máximo de armazenamento estiver expirado.

A solicitação da chave privada deve ser feita por escrito e aprovada pela direção do Conglomerado Financeiro Barigui.

O custodiante, mediante a entrega da CHAVE PRIVADA, deve assinar o termo específico para este fim, onde se encerra sua responsabilidade.

A área de Segurança da Informação deve garantir que os Termo de Responsabilidade e Compromisso, os nomes e os dados dos custodiantes estejam armazenados dentro de um ambiente seguro no Conglomerado Financeiro Barigui, sob a classificação CONFIDENCIAL.

A área de Segurança da Informação deve manter uma lista dos "hash" das chaves que já foram utilizadas e descartadas, para que elas não sejam reaproveitadas no futuro.

### 6.19 Normas Relacionadas com PCI-DSS

Esta Política, Normas e Procedimentos de Segurança da Informação desenvolvidos no Conglomerado Financeiro Barigui devem atender a todos os requisitos do PCI/DSS. Os principais pontos são:

- Documentação para Classificação da Informação, assim como toda mídia deve ser classificada e rotulada;
- Todos os componentes de sistema devem ser configurados de forma adequada e segura. De acordo com as suas características e utilização, os equipamentos devem ter aplicados procedimentos de hardening (mapeamento de ameaças), proteção contra malwares e agentes intrusivos, atualização de patches, geração, captura e análise das trilhas de auditorias e correlação de eventos em sistema centralizado;
- Deve haver documentação e procedimentos para gestão de mudança (GMUD). Os procedimentos de GMUD devem ser aplicados para todos os componentes do sistema;
- Todos os acessos físicos aos diversos ambientes que contenham dados do portador do cartão devem ser registrados e armazenados por três meses. Também, deve haver monitoração por câmeras em todos os principais ambientes que possuam dados do portador do cartão;
- Deve haver utilização de crachás para funcionários, fornecedores e prestadores de serviços e visitantes, onde os crachás de funcionários devem ser diferentes dos demais crachás;
- Deve haver Plano e Procedimentos para resposta a incidente de segurança da informação; e
- Devem ser realizados testes de invasão, varredura de vulnerabilidades, e aplicação de análise de riscos de acordo com os períodos especificados pelo PCI/DSS.

## 7. DIVULGAÇÃO

A Política de Segurança da Informação, bem como os procedimentos operacionais relacionados, serão divulgados por meio de:

- Campanhas de conscientização
- Treinamentos
- Comunicados internos
- Intranet, mensagens instantâneas e outros meios de divulgação interna

## 8. PENALIDADES

O não cumprimento de qualquer um dos itens presentes nesta Política de Segurança da informação e Normas associadas poderá implicar sanções disciplinares, sanções administrativas, legais e/ou penais, dependendo do grau e natureza da infração.

Ao observar uma violação da Política de Segurança da Informação, o usuário observante deve comunicar a infração aos responsáveis pela Segurança da Informação do Conglomerado Financeiro Barigui. Caso seja detectado que o colaborador não comunicou a infração, mesmo sabendo da sua existência, o mesmo pode ser considerado conivente com a mesma e, assim, também estar sujeito a sansões.

Em nenhuma hipótese será admitida a alegação de desconhecimento para o não cumprimento desta Política de Segurança da Informação.

## 9. LEGISLAÇÃO E REGULAMENTAÇÃO

- Resolução CMN 4.658/2018 - Política de Segurança Cibernética e Requisitos para a Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem.
- Resolução CMN 4.557/2017 – Gerenciamento Integrado de Riscos e Capital
- Resolução CMN 3.467/2009 – Qualidade e adequação do Sistema de Controles Internos
- Resolução CMN 2.554/1998 – Implantação e Implementação de Sistema de Controles Internos.
- Instrução CVM nº 558/2015
- Instrução CVM nº 542/2013
- Instrução CVM nº 505/2011
- Instrução CVM nº 301/1999

- COBIT - Control Objectives For Information and Related Technology – "Framework" de boas práticas para Governança e Gestão de TI.
- ABNT NBR ISO/IEC 27001:2013 – Sistema de Gestão de Segurança da Informação.
- ABNT NBR ISO/IEC 27002:2013 – Código de Prática para Gestão da Segurança da Informação
- Payment Card Industry/Data Security Standards (PCI/DSS) v.3.2

## 10. GLOSSÁRIO

- Ativos - Tudo aquilo que manipule direta ou indiretamente uma informação. Em termos de segurança da informação, um ativo pode ser um computador, uma impressora, um fichário na recepção, o próprio usuário etc. Não deve ser confundido com o ativo patrimonial.
- Autenticidade - Declaração de que o dado ou informação são verdadeiros e confiáveis tanto na origem quanto no destino.
- Certificado Digital - Documento eletrônico que contém informações necessárias para correta identificação do portador, o mesmo deve prover mecanismos para garantir autenticidade, confidencialidade e integridades de informações.
- Chave privada – (ou chave criptográfica privada) é um arquivo usado em vários métodos de criptografia para cifrar ou decifrar mensagens ou qualquer conteúdo digital. Em métodos de criptografia que usam chaves assimétricas, há duas chaves diferentes, uma para cifrar e outra para decifrar. Quando uma chave é usada para

cifrar, a outra é usada para decifrar, não sendo possível usar a mesma chave para cifrar e decifrar ou vice-versa. A chave privada, neste contexto é a chave capaz de decifrar um conteúdo previamente cifrado com a chave pública.

- Ciclo de Vida - Criação ou aquisição, utilização, transporte, guarda e descarte de uma informação.
- Ciclo de Vida da Informação - Desde o momento em que informação ela é gerada, rotulada, manipulada, armazenada, transmitida até a sua destruição.
- Classificação - Atribuição, pela autoridade competente, de grau de sigilo a dado, informação, documento, material, área ou instalação.
- Código Fonte - É qualquer sequência ou declaração escrita em alguma linguagem de programação. Estas linguagens são a ponte de comunicação entre o programador e o computador. Quando o programa está finalizado, é feita uma compilação do código fonte, que o transforma em linguagem de máquina para que o computador consiga interpretar.
- Confidenciais - Informações que pertencem à empresa e informações de clientes, que foram geradas ou adquiridas e que se reveladas, podem trazer impactos negativos aos negócios ou repercussões para a imagem da mesma, embaraços administrativos com colaboradores ou vantagens a concorrentes e terceiros.
- Custodiante - Colaborador responsável pela guarda adequada da informação.
- Desclassificação - Cancelamento, pelo gestor competente, da classificação, tornando públicos dados ou informação.
- Gestor da Informação - Colaborador responsável pelas informações e recursos sob sua gestão, o qual os classifica conforme seu grau de sigilo.
- Grau de Sigilo - Gradação atribuída a dados, informações, área ou instalação considerados sigilosos em decorrência de sua natureza ou conteúdo.
- Guarda Permanente - Consideram-se de guarda permanente os dados ou informações de valor histórico, probatório e informativo que devam ser definitivamente preservados.
- Hash – Código gerado por um método criptográfico, de forma a identificar unicamente um conteúdo digital;
- Internas - Todas as informações geradas, possuídas ou custodiadas pela empresa, que podem ser acessadas por todos os colaboradores, mediante autorização do respectivo proprietário.
- Legitimidade - Asseveração de que o emissor e o receptor de dados ou informações são legítimos e confiáveis tanto na origem quanto no destino.
- Malwares - Código malicioso de computador ou programa malicioso – uma parte de um código executável – com capacidade de autorreplicação podendo destruir

arquivos, formatar a unidade de disco rígido, roubar informações sensíveis ou causar outros danos.

- PCI/DSS (Payment Card Industry/Data Security Standards) **-** Acrônimo de "padrão de segurança de dados da indústria de cartões de pagamento"
- PCI/SSC (Payment Card Industry/Security Standards Council) - É uma organização que dita os padrões de Segurança da Informação para ambientes que armazenem, transmitam ou processem dados do portador do cartão.
- Prestador de Serviço - Todo profissional terceirizado executando atividades pontuais.
- Público - Informações de caráter informativo, profissional ou que, em função da legislação vigente, podem ser divulgadas ao público externo à empresa, mediante a avaliação e aprovação da área responsável pela comunicação da empresa.
- Reclassificação - Alteração, pelo gestor competente, da classificação de dados, informação, área ou instalação sigilosas.
- Segurança da Informação – Conceito que abrange a garantia da confidencialidade, da integridade e da disponibilidade das informações.
- Terceiro - Todo profissional terceirizado executando atividades profissionais com jornada de trabalho fixa e regular.
- Vulnerabilidade - Fragilidade ou fraqueza que podem ser exploradas por ameaças e tornar-se um incidente.

## 11. APROVAÇÃO

Declaramos que a presente Política foi aprovada conforme Ata da 43ª Reunião do Conselho de Administração do BANCO BARIGUI DE INVESTIMENTOS E FINANCIAMENTOS S/A, realizada em 02.05.2019.

## 12. CONTROLE DE ATUALIZAÇÕES

**Responsáveis pelo Documento:**

| RESPONSÁVEL | SETOR |
|---|---|
| Elaboração | Departamento de Tecnologia da Informação |
| Revisão | Departamento de Governança Corporativa, CRO e Diretoria. |
| Aprovação | Conselho de Administração |

**Registro de Atualizações:**

| VERSÃO | ITEM (NS) REVISADO (S) OU INSERIDO (S) | MOTIVO | RESPONSÁVEL | DATA |
|---|---|---|---|---|
| 01 | Elaboração | Regulatório | Rafael Tornilo | Julho de 2018 |
| 02 | Adequação / Ajuste em todo o documento | Primeira versão | Luiz Cabral/ Tiago Kunzler/ Rafael Tornilo | Fevereiro de 2019 |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

## 13. ANEXOS

Anexo nº I – TERMO DE CIÊNCIA E ACEITE QUANTO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Anexo nº II – TERMO DE COMPROMISSO E RESPONSABILIDADE DO CUSTODIANTE DE CHAVES PRIVADAS

**ANEXO I**

## TERMO DE CIÊNCIA E ACEITE QUANTO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Por este instrumento, eu, _____, colaborador

do BANCO BARIGUI, portador do RG nº _____, declaro que:

a) Tive acesso ao documento PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO;
b) Li o documento e tenho plena compreensão de seu conteúdo, estando ciente das condições descritas e da minha responsabilidade em cumprir com as suas determinações;
c) Estou ciente de que todas as minhas atividades, utilizando recursos do Conglomerado e demais empresas do Conglomerado Financeiro, podem ser monitoradas e auditadas, sem aviso prévio;
d) Estou ciente de que a não conformidade para com o disposto na Política de Segurança da Informação pode acarretar em medidas disciplinares e outras medidas aplicáveis; e
e) Comprometo-me a seguir integralmente todas as diretrizes do documento recebido, zelando plenamente pela segurança de todas as informações sensíveis com as quais poderei ter contato.

Tipo de contrato do colaborador:

[ ] Funcionário [ ] Estagiário [ ] Terceiro [ ] Outro

_____

Área de atuação do colaborador: _____.

Líder imediato: _____.
Local e Data : _____, _____/_____/_____

_____

Assinatura do COLABORADOR

**ANEXO II**

**TERMO DE COMPROMISSO E RESPONSABILIDADE DO CUSTODIANTE DE CHAVES PRIVADAS**

**COMO CUSTODIANTE DA CHAVE PRIVADA(Descrição)_____DO** Conglomerado Financeiro Barigui

**EU, _____, RG_____,**

**ESTOU CIENTE DAS NORMAS DEFINIDAS NA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, EM RELAÇÃO À SEGURANÇA DAS CHAVES PRIVADAS DE CRIPTOGRAFIA, COMPROMENTENDO-ME A:**

- Manter a chave privada em local seguro, não identificado e protegido contra acessos indevidos, durante o prazo de vigência da chave;
- Manter em sigilo que estou custodiando chave privada;
- Não entregar a chave privada para ninguém, salvo quando solicitado formalmente pela DIREÇÃO do Conglomerado Financeiro Barigui;
- Se houver indícios de comprometimento da chave privada, avisar formal e imediatamente à Diretoria do Conglomerado Financeiro Barigui.

_____ _____ / _____ /_____

Custodiante da Chave Privada Data