# RESUMO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

## 1. OBJETIVO

Em atenção à Resolução CMN nº 4.893, de 26 de fevereiro 2021 e à Lei n. 13.709/2018, este documento estabelece os princípios, conceitos, valores e práticas a serem adotados visando assegurar a confidencialidade, a integridade e a disponibilidade dos dados da instituição ou por ela controlados e dos sistemas de informação por ela utilizados, permitindo à instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

## 2. PÚBLICO-ALVO

Este documento é dirigido aos acionistas, administradores, colaboradores, empregados ou não, menores aprendizes, estagiários, correspondentes, prestadores de serviços terceirizados e todas e quaisquer pessoas que tenham acesso aos dados da instituição ou por ela controlados e aos sistemas por ela utilizados.

## 3. REFERÊNCIAS NORMATIVAS

A presente Política de Segurança Cibernética deve ser lida e interpretada em conjunto com os seguintes documentos:

### 3.1. Normas Externas:

**Resolução CMN nº 4.557, de 23 de fevereiro de 2017:** Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações.

**LEI Nº 12.414, DE 9 DE JUNHO DE 2011:** Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

**LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011:** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

**DECRETO Nº 8.771, DE 11 DE MAIO DE 2016**: Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados

na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

**LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990**: Dispõe sobre a proteção do consumidor e dá outras providências.

**LEI Nº 12.965, DE 23 DE ABRIL DE 2014:** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

**LEI N o 10.406, DE 10 DE JANEIRO DE 2002**: Institui o Código Civil.

**LEI COMPLEMENTAR Nº 105, DE 10 DE JANEIRO DE 2001**: Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências

**Resolução CMN n° 4.893 de 26/2/2021:** Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

### 3.2. Normas Internas

I. Código de Conduta;

II. Política de Segurança da Informação do Grupo Dufrio;

III. Plano de Contingência e Continuidade de Negócios;

IV. Política de Gerenciamento de Risco e Gerenciamento de Capital;

V. Declaração de Apetite Por Risco (RAS);

## 4. DOS PRINCÍPIOS

As ações da Instituição regem-se pelos seguintes princípios:

**I. Confidencialidade:** princípio de segurança da informação que garante que a informação seja acessada somente por pessoas ou processos que tenham autorização para acessá-las. Pressupõe a limitação do acesso à informação, sendo permitido o acesso somente às pessoas autorizadas e em circunstâncias que se apresentem efetivamente necessário o acesso, protegendo informações que devem ser acessíveis apenas por um determinado grupo de usuários contra acessos não autorizados.

**II. Disponibilidade:** princípio de segurança da informação que garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido. Pressupõe a garantia de acesso das pessoas devidamente autorizadas à informação sempre que o acesso for necessário, prevenindo interrupções das operações da Instituição por meio de um controle físico e técnico das funções dos sistemas de dados,

assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança.

**III. Integridade:** princípio de segurança da informação que garante a não-violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital. Pressupõe a garantia da veracidade, fidelidade e integridade da informação e dos métodos de seu processamento e eventual tratamento da informação, pois esta não deve ser alterada enquanto está sendo transferida ou armazenada, impedindo que a informação fique exposta ao manuseio por uma pessoa não autorizada e impedindo, também, alterações não aprovadas e sem o controle do controlador (corporativo ou privado) da informação.

## 5. DAS DIRETRIZES DE SEGURANÇA CIBERNÉTICA

A Segurança Cibernética na Instituição segue as seguintes diretrizes:

a) As informações da Instituição, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.

b) As informações e os dados devem ser utilizados de forma transparente e apenas para as finalidades para as quais foram coletadas.

c) Os procedimentos e os controles deverão abranger a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

d) A identificação daqueles que têm acesso às informações da Instituição deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

e) Somente deve ter concedido acesso às informações e recursos de informação imprescindíveis para o pleno desempenho das suas atividades do indivíduo autorizado

f) A senha é utilizada como assinatura eletrônica, sendo pessoal e intransferível, e deve ser mantida secreta, sendo proibido seu compartilhamento.

g) Devem ser reportados à área de Tecnologia da Informação da Instituição, que será responsável pelo registro e controle dos efeitos de incidentes relevantes, os riscos às informações, bem como eventuais fatos ou ocorrências que possam colocar em risco tais informações.

h) As responsabilidades quanto à Segurança Cibernética devem ser amplamente divulgadas a todos aqueles considerados público-alvo desta política, que devem entender e assegurar o cumprimento do aqui disposto.

### 5.1. Das diretrizes para tratamento da Informação

A informação deve receber proteção adequada em observância aos princípios e diretrizes da Segurança Cibernética da Instituição em todo o seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

### 5.2. Das diretrizes para classificação de dados e das informações

As informações e os dados sob responsabilidade da Instituição serão classificados, conforme descrito no plano de ação, para adequação das estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética.

A referida classificação se dará, considerando a relevância, a confidencialidade e as proteções necessárias, nos seguintes níveis e subníveis:

**I. Dado NÃO Pessoal:** informação não relacionada a pessoa natural identificada ou identificável:

**a**. **Público:** aquele explicitamente aprovado por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio. Possuem caráter informativo geral e são direcionadas ao público em geral.

**b. Interno**: destinado ao uso interno da Instituição disponível para todos os usuários. O acesso às informações dessa natureza, ainda que não autorizado, não afetaria os negócios da Instituição, seus funcionários ou seus clientes, contudo é considerado incidente de segurança de baixa relevância e, portanto, seu responsável está sujeito às sanções cabíveis. Essas informações não exigem proteções especiais salvo aquelas entendidas como mínimas para impedir o acesso não autorizado.

**c. Restrito**: dado com acesso autorizado a apenas um usuário específico ou grupo de usuários. Diferem das do dado interno uma vez que que não está disponível para todos os usuários e eventual divulgação poderia afetar significativamente os negócios da Instituição, funcionários, terceiros, clientes ou outros.

**II. Dado Pessoal:** informação relacionada a pessoa natural identificada ou identificável:

**a. Dado pessoal não sensível:** dado pessoal que não seja classificado como sensível pelo art. 5º, inciso II, da Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais) e que não possa ser utilizado para fins discriminatórios, ilícitos ou abusivos;

**b. 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, dado protegido pelo sigilo das operações ativas e passivas e serviços prestados, na forma da Lei Complementar nº 105/01, ou dado que possa ser utilizado para fins discriminatórios, ilícitos ou abusivos, quando vinculados a uma pessoa natural.

A divulgação desses dados é proibida, salvo se solicitada por órgãos fiscalizadores competentes, tais como o Banco Central do Brasil, a Receita Federal do Brasil e a Comissão de Valores Mobiliários ou por decisão judicial.

Os dados pessoais sensíveis deverão ser protegidos de forma mais rígida, incluindo inciativas de rastreabilidade da informação e controle de acesso diferenciado, devendo ser compatível com as funções desempenhadas e com a sensibilidade das informações. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

Uma vez classificada a informação deve ser protegida e receber tratamento e armazenamento adequados.

## 6. PROCEDIMENTO DE CONTRATAÇÃO DE SERVIÇOS RELEVANTES DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

Quando da contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, além das práticas de governança corporativa e de gestão referidas acima, a instituição adotará as seguintes práticas de governança corporativa e de gestão:

### 6.1. Abrangência

Além dos serviços relevantes de processamento e armazenamento de dados, para fins desta política os serviços de computação em nuvem abrangem a disponibilidade à instituição, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

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

II. implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou

III. execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

### 6.2. Avaliação da relevância do serviço a ser contratado

Previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem deve ser avaliada a relevância do serviço a ser contratado, considerando:

I. os riscos aos quais a instituição estará exposta;

II. a criticidade do serviço;

III. a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado;

IV. a classificação da informação a ser tratada pelo prestador.

### 6.3. Avaliação da capacidade do prestador de serviço

Antes da contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, deve ser considerada e documentada a verificação da capacidade do potencial prestador de serviço de assegurar:

I. o cumprimento da legislação e da regulamentação em vigor;

II. o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

III. a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;

IV. a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;

V. o acesso da instituição contratante aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;

VI. o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

VII. a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos; e

VIII. a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

### 6.4. Critérios e processo decisório para contratação

O responsável pela decisão quanto à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, a ser devidamente documentada e arquivada na instituição, deverá considerar a relevância do serviço a ser contratado, além dos seguintes critérios durante o processo decisório:

I. A natureza da atividade do fornecedor e a sua reputação;

II. A ocorrência de investigação ou de ação de autoridade supervisora relacionada a segurança cibernética que tenha tido o fornecedor como objeto ou envolvido;

III. A ocorrência de incidentes de segurança cibernética com o fornecedor;

IV. A representatividade nacional e internacional da confiabilidade do fornecedor em assegurar a confidencialidade, a integridade e a disponibilidade dos dados da instituição ou por ela controlados e dos sistemas de informação por ela utilizados.

V. A capacidade do fornecedor de cumprir com as normas legais, regulamentares e contratuais ou arcar com indenizações por eventuais danos por ele causados ou por eventuais descumprimentos contratuais.

VI. A existência de acreditação e certificação da segurança oferecida pelo fornecedor, mediante avaliação realizada por órgãos governamentais ou por órgãos independentes não governamentais.

### 6.5. Documentação das práticas de governança corporativa e de gestão adotadas

Devem ser documentadas as práticas de governança corporativa e de gestão adotadas em relação a cada prestador de serviço contratado, proporcionais à relevância do serviço a ser contratado e aos riscos aos quais a instituição se expõe.

### 6.6. Cláusulas contratuais obrigatórias

Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

I. a indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

II. a adoção de medidas de segurança para a transmissão e armazenamento dos dados;

III. a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;

IV. a obrigatoriedade, em caso de extinção do contrato, de:

a) transferência dos dados ao novo prestador de serviços ou à instituição contratante;

b) exclusão dos dados pela empresa contratada substituída, após a transferência dos dados prevista na alínea "a" e a confirmação da integridade e da disponibilidade dos dados recebidos;

V. o acesso da instituição contratante a:

a) informações fornecidas pela empresa contratada, visando a verificar o cumprimento dessas obrigações;

b) informações relativas às certificações e aos relatórios de auditoria especializada; e

c) informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

VI. a obrigação de a empresa contratada notificar a instituição contratante sobre a subcontratação de serviços relevantes para a instituição;

VII. a permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;

VIII. a adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil; e

IX. a obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

Os contratos devem prever, ainda, cláusulas específicas para o caso de decretação de regime de resolução da instituição contratante pelo Banco Central do Brasil:

I. a obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso, citados no inciso VII do caput, que estejam em poder da empresa contratada; e

II. a obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

a) a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução; e

b) a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

## 7. MECANISMOS PARA DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA NA INSTITUIÇÃO

Para a disseminação da cultura de segurança cibernética a instituição adotará os seguintes mecanismos:

I. a instituição promoverá a disseminação dos princípios e diretrizes da Segurança Cibernética por meio de programas de conscientização, capacitação e avaliação periódicas de pessoal.

II. a política e as regras de segurança da informação e segurança cibernética serão divulgadas e compartilhadas com todo o público-alvo desta política, e devem ser disponibilizadas de maneira que seu conteúdo possa ser consultado a qualquer momento, protegidas contra alterações.

III. a prestação, na página da instituição na internet, de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros

IV. a divulgação ao público, na página da instituição na internet, de resumo contendo as linhas gerais da política de segurança cibernética.

## 8. PROGRAMA DE SEGURANÇA CIBERNÉTICA

Conforme sua criticidade, o programa de segurança cibernética divide-se em:

**Ações críticas**: Correções emergências e imediatas para mitigar riscos iminentes.

**Ações de Sustentação:** Iniciativas de curto / médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro e permitindo que ações de longo prazo/estruturantes possam ser realizadas.

**Ações Estruturantes:** Iniciativas de médio / longo prazo que tratam a causa raiz dos riscos, voltadas para o futuro da Instituição.

## 9. DIVULGAÇÃO

A Política de Segurança Cibernética e as demais políticas e normas complementares da Instituição aqui referenciadas devem ser divulgadas ao Público-Alvo, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações, devendo estar disponíveis em local acessível aos colaboradores e protegidas contra alterações.

.

## 10. DÚVIDAS

Em caso de dúvidas sobre o tema relacionado neste documento, contactar a área de Segurança da Informação do Grupo Dufrio.

## 11. COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO

A Diretoria da Instituição, ao aprovar esta Política de Segurança Cibernética, institui um compromisso para com a melhoria contínua dos procedimentos relacionados com a

segurança cibernética e da informação, buscando sempre manter a instituição em conformidade com normas legais e regulamentares sobre os referidos temas, guiada pelos princípios, conceitos, valores e práticas aqui adotados, com o objetivo de assegurar a confidencialidade, a integridade e a disponibilidade dos dados da instituição ou por ela controlados e dos sistemas de informação por ela utilizados, permitindo à instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

## 12. VIGÊNCIA

Esta Política entra em vigor a partir da data de aprovação e permanece vigente até sua atualização

## 13. APROVAÇÃO DA POLÍTICA

A presente Política de Segurança da Cibernética foi aprovada pela Diretoria da Dufrio Financeira, Crédito, Financiamento e Investimentos S.A.