Ebury Bank

Política de Segurança Cibernética e da Informação
V.9.2026

Responsável pela Política: *Segurança da Informação*

Controle de Documento

Versão	Data da Criação	Autor	Aprovado por	Data da Aprovação	Data da próxima revisão
1.0	25/03/2019	Tiago Tavares	Diretoria	25/03/2019	25/03/2020
2.0	21/04/2020	Carlos Grilli	Diretoria	21/04/2020	21/04/2021
3.0	07/04/2021	Carlos Grilli	Diretoria	07/04/2021	07/04/2022
4.0	05/04/2022	Carlos Grilli	Diretoria	05/04/2022	05/04/2023
5.0	19/06/2023	Thiago Oliveira	Diretoria	19/06/2023	19/06/2024
6.0	04/08/2023	Thiago Oliveira	Diretoria	04/08/2023	04/08/2024
7.0	31/07/2023	Carlos Grilli	Diretoria	31/07/2023	31/07/2024
8.0	31/07/2025	Luis Gonelli	Gerente Sênior	31/07/2025	31/07/2026
9.0	11/02/2026	Luis Gonelli	Gerente Sênior	11/02/2026	11/02/2027

Alterações:

Revisão de política de acordo com às Resoluções CMN nº 4.893/2021 e CMN nº 5.274/2025 do Banco Central do Brasil.

Sumário

1 Introdução

A informação é um dos patrimônios mais importantes a ser preservado pela Instituição. Assim, o Ebury Bank estabelece a presente Política, a fim de orientar e garantir a aplicação das diretrizes estratégicas e princípios para proteção dos ativos tangíveis e intangíveis da Instituição, dos clientes e interesses do público em geral.

Ainda, é objetivo deste normativo atender às leis e normas regulamentadoras do mercado, principalmente no tocante às Resoluções CMN nº 4.893/2021 e CMN nº 5.274/2025 do Banco Central do Brasil, fazendo com que se torne parte da cultura de segurança cibernética, por meio de programas de capacitação, prestação de informações à clientes e usuários sobre precaução na utilização de produtos e serviços e o comprometimento da Alta Administração com a melhoria contínua dos procedimentos.

2 Abrangência

Esta Política visa atender o público geral, especialmente clientes e parceiros, administradores, gestores, colaboradores, estagiários e prestadores ou fornecedores de serviços que se relacionam com o Ebury Bank, direta ou indiretamente.

3 Base Legal

Resolução BCB nº 85 de 8 de abril de 2021 e suas alterações - Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil;

Resolução CMN n° 4.893, de 26 de fevereiro de 2021 e suas alterações - 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 financeiras autorizadas a funcionar pelo Banco Central do Brasil;

Comunicado nº 41.782 de 24 de junho de 2024 - Divulga procedimentos a serem observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil na comunicação a essa Autarquia das informações relativas à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem de que tratam a Resolução CMN nº 4.893, de 26 de fevereiro de 2021 e a Resolução BCB nº 85, de 8 de abril de 2021 e suas alterações posteriores.

Resolução CMN n° 5.274 de 18 de dezembro de 2025 - Atualiza e endurece as regras de segurança cibernética para as instituições financeiras no Brasil. Ela altera a norma anterior (Resolução CMN nº 4.893/2021) para refletir os novos riscos atribuídos ao Sistema de Pagamento Brasileiro - SPB.

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

4 Detalhamento

4.1 Procedimentos e Controles

As violações das Políticas e procedimentos de segurança do Ebury Bank, após apuração e constatação de responsabilidades, poderão desencadear ações disciplinares, rescisão de contrato de trabalho e medidas administrativas/judiciais cabíveis.

4.2 Compromisso de Sigilo e Confidencialidade

Terceiros e parceiros deverão assumir o dever de sigilo, por si, seus empregados, prepostos ou terceiros sob suas ordens e efetuar uso, com prévia autorização, das informações críticas sobre todos os processos de negócio do Ebury Bank, ainda que em caso de rescisão contratual.

4.3 Contratação de Fornecedores e Prestadores de Serviços

A contratação de fornecedores deverá observar diretrizes internas, a fim de assegurar a contratação de fornecedores parceiros idôneos, de boa conduta social, ambiental e ética, que incentivem a adoção de boas práticas, bem como contratar bens e serviços por preços coerentes praticados pelo mercado.

Caso o serviço a ser contratado utilize armazenamento de dados relevantes em nuvem, após procedimento interno de averiguação, deverá haver a comunicação ao Banco Central do Brasil, em até dez dias após a contratação dos serviços.

Ainda, nos casos de inexistência de convênio para troca de informações entre o Banco Central do Brasil e às autoridades supervisoras dos países onde os serviços poderão ser prestados, o Compliance deverá solicitar autorização do Banco Central do Brasil, no prazo mínimo de (60) sessenta dias antes do início da contratação.

4.4 Prevenção de vazamento de informações

São utilizados mecanismos de prevenção de vazamento de dados (DLP) para monitorar, detectar e bloquear a transmissão não autorizada de dados sensíveis em repouso, em uso ou em trânsito. O tráfego de rede será inspecionado para identificar padrões de exfiltração de informações, garantindo que o fluxo de dados ocorra apenas por canais homologados. Mecanismos de rotulagem e classificação automática de documentos serão aplicados para reforçar a proteção conforme a criticidade do conteúdo.

4.5 Proteção contra Vírus e Softwares Maliciosos

Servidores, estações de trabalho ou notebook, deverão ser protegidos por software de antimalware, homologado pela Instituição. As estações de trabalho serão gerenciadas pelos administradores, impossibilitando que o colaborador desabilite os softwares de proteção.

4.6 Cópia de segurança (backup)

A área de Tecnologia da Informação realizará controle de backup, estabelecendo dados a serem copiados e a periodicidade de retenção, a fim de garantir a recuperação em caso de falha ou desastre e ainda atender requisitos legais e fiscais. O armazenamento deverá ser efetuado com a identificação de cada mídia, data do backup e tempo de retenção.

4.7 Criptografia

As informações confidenciais internamente tratadas são armazenadas e trafegadas de forma criptografada, conforme nível de criticidade e confidencialidade definidos nos documentos de classificação da informação.

4.8 Uso da rede corporativa

Os usuários autorizados possuem acesso à rede corporativa para disponibilidade e armazenamento de arquivos pertinentes ao negócio, devendo o acesso ser tratado conforme classificação de informação e não como informação particular. O acesso deverá ser realizado de forma a atender normas internas.

4.9 Monitoramento

O Ebury Bank assegurará a rastreabilidade total de todos os sistemas e recursos computacionais que suportam transações e operações financeiras, visando a prevenção e identificação de fraudes ou atividades não autorizadas. É mandatória a geração de trilhas de auditoria que permitam o rastreamento fim a fim do processamento de dados, incluindo o registro e o monitoramento sistemático de logs para identificação de falhas e comportamentos atípicos. Adicionalmente, devem ser definidos tempos de retenção específicos para essas informações, de acordo com a natureza do processamento, garantindo que os dados armazenados subsidiem análises técnicas e assegurem a plena auditabilidade e integridade do ambiente.

4.10 Controle de acessos e senhas

O Ebury Bank possui procedimentos formais para concessão, alteração, revogação e revisão de contas de usuários, contas de terceiros e contas de serviços, que são passíveis de controle e auditoria, incluindo a autorização formal dos gestores responsáveis para o gerenciamento de usuários, no que diz respeito a usuários inclusão de usuários, alteração de acesso, exclusão de usuário, gerenciamento de perfis seguros, gerenciamento de senhas e uso do múltiplo fator de autenticação (MFA).

A identificação de usuários do Ebury Bank é única bem como sua senha é pessoal e intransferível, além disso sua senha deve conter as características definidas como senhas fortes. É terminantemente proibido compartilhar senha ou anotar senha em cadernos e post-its. O acesso a informações, serviços de rede e aplicações são controlados visando evitar o acesso indevido.

Existem regras para controle e revisão de acesso, considerando as permissões de acordo com a sensibilidade da informação. As regras de acesso devem ser aplicadas a Rede (Sistema Operacional) e Sistemas Aplicativos (opções de controle por menu e funções, particulares em cada aplicação), restringindo ao máximo a atribuição de direitos de acesso, permitindo apenas o necessário para atendimento e desenvolvimento do trabalho habitual.

Todos os usuários nominais são identificados por uma identificação única (user ID) e autenticação das contas são realizadas por meio de logins, usuários e a atribuição de um segundo fator de autenticação (ex: mensagem de texto, código temporário ou tokens).

4.11 Aquisição, desenvolvimento e Manutenção dos sistemas de informação

Todo o desenvolvimento dos sistemas de informação deverá seguir a metodologia adotada pelo Ebury Bank. Aquisições, desenvolvimentos ou manutenções de sistemas de informação, deverão ser

considerados os requisitos especiais de segurança. O processo deverá possuir documentação técnica e operacional, para criar base de conhecimento e melhor controle dos sistemas utilizados.

4.12 Controle de implementações e mudanças operacionais

Toda alteração em ambiente de produção deverá ser planejada e homologada.

4.13 Gestão de Vulnerabilidade

A detecção e prevenção de vulnerabilidades utiliza vários métodos, como Testes de Penetração (Intrusão) e Monitoramento Contínuo de Vulnerabilidades (CVM), tanto para descobrir novas fragilidades quanto para confirmar se as correções/alterações de configuração foram aplicadas corretamente.

A gestão de vulnerabilidades se aplica a todos os sistemas e dispositivos de informação do Ebury Bank, incluindo, entre outros: serviços em nuvem, servidores, laptops, dispositivos móveis, equipamentos de rede e todos os ambientes (ou seja, Produção, Teste e Desenvolvimento).

4.14 Resposta a Incidentes de Segurança

A resposta aos incidentes deverá ser tratada de forma a limitar os danos e minimizar o tempo e os custos de recuperação, que envolve um método organizado para lidar com as consequências de um ataque contra a segurança de um sistema computacional. A implementação deste processo será de responsabilidade da equipe de resposta a incidentes, ou CSIRT (Computer Security Incident Response Team), formada por analistas de segurança e representantes legais. O processo de resposta aos incidentes de segurança compreende: detecção, triagem e análise, mitigação, investigação, resposta e educação. As tratativas dos incidentes deverão ocorrer, ressalvadas as características principais e considerando os quesitos de origem, vulnerabilidade, criticidade, impacto e ativo alvo. Não obstante, deverão ser observados os tipos de severidade - média e baixa, alta ou severidade crítica.

4.15 Compartilhamento de Informações sobre os incidentes relevantes

Exceto em casos que exigem sigilo de informações estratégicas para o negócio, será adotado o padrão de soluções de ferramentas disponibilizadas ou sugeridas pelas associações das quais o Ebury Bank faz parte, para que o compartilhamento de incidentes seja eficiente e garanta a assimilação do processo.

4.16 Inventário

Os principais ativos de informação e ativos de tecnologia são identificados, inventariados e classificados de acordo com a importância, para proteção efetiva e de acordo com o grau de criticidade e confidencialidade necessários. Todo ativo de informação do Ebury Bank possui controles de identificação dos seus recursos computacionais (ex: notebooks, servidores, celulares e dispositivos de mídia física removíveis como HD externo) por meio de tags de patrimônio, serial number e respectivo responsável que são gerenciados por softwares de gestão de inventário.

4.17 Gestão de Patching

O Ebury Bank deve implementar um processo sistemático para identificar, testar e aplicar correções de segurança em todos os ativos tecnológicos. É mandatório que o ciclo de vida dos patches seja documentado, garantindo a conformidade e a integridade do ambiente. O monitoramento contínuo deve validar a eficácia das atualizações e identificar ativos que possuam falhas de segurança pendentes. A falha na aplicação de patches essenciais será tratada como uma não conformidade grave aos controles de proteção de dados.

4.18 Proteção de Redes Corporativa

O Ebury Bank deve implementar a segmentação rigorosa de suas redes, assegurando o isolamento do ambiente de produção e dos recursos que suportam processos críticos de negócio. Esta estrutura deve ser protegida por controles rigorosos de firewall e monitoramento contínuo de conexões, visando mitigar tentativas de acesso originadas por ativos externos à rede corporativa. É mandatória a definição de critérios para o estabelecimento e a vigilância de conexões com ambientes externos, com especial atenção à prevenção de acessos indevidos e à detecção de eventos atípicos em horários noturnos e dias não úteis. Processos e ferramentas de análise e tratamento de anomalias no ambiente produtivo devem ser mantidos, garantindo que o acesso às redes seja restrito exclusivamente a dispositivos e ativos de tecnologia devidamente homologados e autorizados.

O Ebury Bank deve possuir mecanismos para limitar o acesso à rede corporativa a usuários credenciados e a dispositivos autorizados.

4.19 Gestão de Certificados Digitais

O Ebury Bank deve monitorar continuamente o uso de certificados e assinaturas digitais, assegurando a implementação de mecanismos de rastreabilidade plena para todas as operações. É mandatória a definição de procedimentos rigorosos para a custódia de informações, abrangendo controles de acesso físico e lógico às chaves privadas sob responsabilidade da instituição, de modo a impedir seu compartilhamento indevido ou exposição não autorizada. Adicionalmente, devem ser estabelecidos processos e ferramentas para a validação tempestiva de certificados revogados perante as autoridades certificadoras.

4.20 Inteligência de Ameaças

O Ebury Bank deve implementar ações de inteligência cibernética voltadas à identificação antecipada de ameaças. Isso inclui o monitoramento sistemático de informações de interesse da instituição na internet, Deep Web e Dark Web, além da vigilância em grupos privados de comunicação. O objetivo é detectar precocemente indícios de fraudes, vazamentos de dados ou planejamentos de ataques, permitindo a adoção de medidas preventivas e a proteção da reputação e dos ativos da instituição.

4.21 Desenvolvimento Seguro

O Ebury Bank e seus prestadores de serviços de desenvolvimento de sistemas devem estabelecer e manter requisitos técnicos de segurança para a integração de seus sistemas de informação via interfaces eletrônicas (APIs e Web Services). Tais integrações devem obrigatoriamente utilizar protocolos de autenticação e autorização robustos, criptografia de dados em trânsito e mecanismos de controle que garantam a integridade e a confidencialidade do tráfego. Além disso, devem ser definidos padrões de conformidade para a comunicação com ambientes de terceiros, assegurando que toda interface eletrônica seja submetida a análises de vulnerabilidade e monitoramento contínuo, em conformidade com as diretrizes regulatórias vigentes.

4.22 Continuidade de Negócios

Os procedimentos e a metodologia adotados pela Instituição serão base para as simulações de teste de continuidade de negócio, a fim de garantir a confidencialidade, integridade e disponibilidade dos serviços contratados em nuvem. Neste sentido, as áreas de Tecnologia e Segurança da Informação deverão garantir a continuidade e recuperação nos serviços de nuvem contratados, além do gerenciamento das interrupções que possam ocorrer.

Ainda, deverão ser consideradas opções de portabilidade, para assegurar que os negócios não dependam de provedor único, com objetivo de evitar aprisionamento tecnológico ou dependência de fornecedores e eventuais custos que sobreponham à troca de fornecedor ou tecnologia empregada.

4.23 Conformidade

Visando assegurar a inexistência de irregularidades nas atividades executadas pelo Ebury Bank, deverão ser tomados os devidos cuidados para atendimento à conformidade com os requisitos de negócio, leis civis, contratuais e regras de segurança.

4.24 Campanhas de Conscientização de Segurança

O Ebury Bank, periodicamente, proverá treinamento de conscientização de segurança aos colaboradores, com apoio e envolvimento da Alta Administração. Assim como a divulgação periódica de informes, com o objetivo de disseminar e aculturar todos os colaboradores da instituição, quanto às diretrizes de Segurança da Informação.

4.25 Comunicação

Quaisquer indícios de irregularidades no cumprimento das determinações desta Política serão alvo de investigação interna e devem ser comunicadas imediatamente ao Departamento de Segurança da Informação, através do e-mail: infosec@ebury.com

5 Manutenção deste documento

Esta Política é mantida atualizada em consonância com as diretrizes do Ebury Bank e dos órgãos reguladores a que se submete.