DIÁRIO OFICIAL DA UNIÃO

Publicado em: 13/11/2020 | Edição: 217 | Seção: 1 | Página: 57

Órgão: Ministério da Economia/Banco Central do Brasil/Àrea de Regulação/Departamento de Regulação do Sistema Financeiro

INSTRUÇÃO NORMATIVA BCB Nº 37, DE 29 DE OUTUBRO DE 2020

Divulga a versão 1.0 do Manual de Segurança do Open Banking.

Os Chefes do Departamento de Regulação do Sistema Financeiro (Denor) e de Tecnologia da Informação (Deinf), no uso das atribuições que lhe conferem os arts. 23, inciso I, alínea "a", 62, inciso IV, do Regimento Interno do Banco Central do Brasil, anexo à Portaria nº 84.287, de 27 de fevereiro de 2015, com base no art. 3º, inciso IV, da Resolução BCB nº 32, de 29 de outubro de 2020, resolvem:

Art. 1º Esta Instrução Normativa divulga a versão 1.0 do Manual de Segurança do Open Banking, de observância obrigatória por parte das instituições participantes,conforme Anexo.

Parágrafo único. O manual de que trata o caput, em sua versão mais recente, estará acessível na página do Open Banking no sítio eletrônico do Banco Central do Brasil na internet.

Art. 2º Esta Instrução Normativa entra em vigor na data de sua publicação.

HAROLDO JAYME MARTINS FROES CRUZ
Chefe do Departamento de Tecnologia da Informação

JOÃO ANDRÉ CALVINO MARQUES PEREIRA
Chefe do Departamento de Regulação do Sistema Financeiro

ANEXO

Manual de Segurança do Open Banking Versão 1.0

Histórico de revisão

Data	Versão	Descrição das alterações
29/10/2020	1.0	Versão inicial.

Apresentação

Este manual estabelece os requisitos mínimos de segurança das APIs e demais sistemas relacionados ao Open Banking, em complemento às determinações constantes da regulamentação vigente.

Ao longo deste documento será constante o uso de siglas para designar algumas expressões cotidianas dos profissionais da área de segurança da informação. Alguns exemplos das mais frequentemente utilizadas, com as correspondentes definições, são as seguintes:

I - ACL: Access Control List;

II - API: Application Programming Interface;

III - HTTP: HyperText Transfer Protocol;

IV - IP: Internet Protocol;

V - NTP: Network Time Protocol;

VI - PFS: Perfect Forward Secrecy;

VII - PGP: Pretty Good Privacy;

VIII - TCP: Transmission Control Protocol;

IX - TLS: Transport Layer Security;

X - URI: Uniform Resource Identifier; e

XI - UTC: Universal Time Coordinated.

Termos de Uso

Este manual detalha os requisitos técnicos para a implementação dos elementos necessários à operacionalização do Open Banking, complementando a regulamentação vigente sobre o tema.

O manual será revisto e atualizado periodicamente a fim de preservar a compatibilidade com a regulamentação, bem como para incorporar os aprimoramentos decorrentes da evolução do Open Banking e da tecnologia.

Informações mais detalhadas e exemplos da aplicação deste manual poderão ser encontrados nos guias e tutorias disponíveis no Portal do Open Banking no Brasil, na Área do Desenvolvedor.

Sugestões, críticas ou pedidos de esclarecimento de dúvidas relativas ao conteúdo deste documento podem ser enviados ao Banco Central do Brasil por meio dos canais institucionais dessa autarquia.

Referências

Estas especificações baseiam-se, referenciam, e complementam, quando aplicável, os seguintes documentos:

Referência	Origem
Resolução Conjunta nº 1, de 2020	https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20Conjunta&numero=1
Resolução BCB nº 32, de 2020	https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=32
Resolução CMN nº 4.658, de 2018	https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=4658
Circular nº 3.909, de 2018	https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3909
Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018)	http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
BCP 195/RFC 7525	https://tools.ietf.org/html/rfc7525
Owasp API Top 10	https://owasp.org/www-project-api-security/
Sans Top 25 Software Errors	https://www.sans.org/top25-software-errors
CWE Top 25 Software Weaknesses	https://cwe.mitre.org/top25/archive/2020/2020_cwe_top25.html

1. Introdução

Para garantir a segurança do Open Banking no País, a regulamentação vigente estabelelce a obrigatoriedade de se cumprir uma série de medidas, dentre as quais as descritas neste manual.

Este manual detalha em termos operacionais as diretrizes de segurança estabelecidas pela Resolução Conjunta nº 1 e pela Resolução BCB nº 32, ambas de 2020. Ele abrange tanto os requisitos mínimos de segurança obrigatórios para as instituições participantes como para os demais elementos que compõem a estrutura do Open Banking, a exemplo do diretório.

A abordagem da segurança neste manual foi pautada nos pilares da governança, da proteção, da detecção e da reação. Com relação ao compartilhamento de informações sobre canais de atendimento, produtos e serviços disponíveis à contratação nas instituições participantes, os requisitos de segurança assumem um caráter próprio para esse tipo de dado, que é público e não requer consentimento prévio de clientes para o seu compartilhamento. Entretanto, na medida em que o Open Banking abranger o compartilhamento de outros dados e serviços, requisitos de segurança mais estritos serão acrescentados ao manual, em complemento à regulamentação aplicável.

2. Governança

As instituições participantes do Open Banking possuem a obrigação de acompanhar a edição e a revogação de eventuais normas com impacto no tema de forma a estar permanentemente em dia com as determinações legais.

Compõem, de forma não exaustiva, o rol de atos normativos cuja observância é essencial pelas instituições participantes do Open Banking:

I - Resolução Conjunta CMN/BCB nº 1, de 2020;

II - Resolução CMN nº 4.658, de 2018;

III - Circular BCB nº 3.909, de 2018; e

IV - Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709, de 2018).

3. Dados Públicos

A fase inicial do Open Banking contempla o compartilhamento de informações sobre canais de atendimento e sobre produtos e serviços relacionados a contas de depósitos à vista e de poupança, contas de pagamento pré-pagas, contas de pagamento pós-pagas e operações de crédito. Trata-se de informações não sigilosas, em geral já acessíveis pelo público, que com o funcionamento do Open Banking poderão ser consultadas de forma estruturada.

Apesar dessa característica, os dados públicos não prescindem de medidas de segurança, dada a importância da preservação de fatores como integridade, qualidade e tempestividade, exemplos de aspectos sujeitos a ameaças. Ademais, a meta é prevenir qualquer ponto de vulnerabilidade no ecossistema do Open Banking e, para tanto, medidas de segurança robustas devem alcançar inclusive o fornecimento de informações não sensíveis.

3.1 Proteção

I - o acesso aos dados no âmbito do Open Banking deve ser realizado exclusivamente por meio de APIs;

II - os sistemas e APIs relacionados ao Open Banking devem ser mantidos em rede interna segregada logicamente de redes ordinariamente utilizadas por estações de trabalho ou redes sem fio;

III - as instituições transmissoras de dados devem implementar controles de tráfego de entrada e saída, de forma a permitir apenas o tráfego necessário para comunicação com as APIs de Open Banking. Exemplos de controles: firewalls, listas de controle de acesso (ACLs) e grupos de segurança (security groups);

IV - as instituições devem implementar criptografia na comunicação com as APIs de Open Banking expostas publicamente, por meio do protocolo TLS na versão 1.2 ou superior, utilizando cifras (cipher suites) que atendam ao requisito de "perfect forward secrecy" (PFS);

V - as funcionalidades "TLS Session Resumption" e "TLS Renegotiation" devem ser desabilitadas;

VI - as instituições devem aplicar controles de segurança na camada de aplicação que permitam a inspeção de ameaças e o bloqueio de ataques de injeção de código, entre outros, adequados às tecnologias utilizadas na API; e

VII - as instituições não devem expor os repositórios de dados utilizados no Open Banking diretamente à internet.

3.2 Detecção

I - as instituições devem manter trilhas de auditoria contendo, no mínimo, endereço IP de origem da chamada, porta de comunicação origem da chamada (porta TCP do cliente), data, hora, sistema, usuário (quando aplicável), objeto, falha ou sucesso da ação das configurações realizadas nos sistemas e APIs relacionados ao Open Banking, observadas a legislação e regulamentação vigentes;

II - os sistemas e APIs relacionados ao Open Banking devem possuir relógio sincronizado com fonte confiável de tempo, por exemplo, por meio do uso do protocolo NTP;

III - as vulnerabilidades encontradas nas APIs ou demais sistemas relacionados ao Open Banking devem ser categorizadas e priorizadas de acordo com classificação de risco; e

IV - as APIs e demais sistemas relacionados ao Open Banking devem ser implementados usando padrões de configuração segura (hardening), observada a regulamentação vigente;

3.3 Reação

I - é facultado às instituições participantes transmissoras de dados implementar bloqueio de acessos às suas APIs, com vistas a tratar riscos cibernéticos ou para tratar incidentes cibernéticos em andamento, caso, por exemplo, perceba uma ação maliciosa. A implementação desses bloqueios deve ser

compatível com a Política de Segurança Cibernética da instituição.

4. Diretório

I - cada instituição deve cadastrar no diretório de participantes os dados de contato de seus representantes para tratamento de incidentes com, no mínimo, e-mail, chaves criptográficas PGP (se houver) e campo para dados adicionais. Tais dados devem ser disponibilizados pelo diretório para acesso aos demais participantes;

II - cada instituição deve disponibilizar os contatos de e-mail das equipes de segurança conforme a RFC 2142 (abuse e security);

III - o acesso às áreas restritas do diretório de participantes deve ser condicionado à autenticação por, no mínimo, dois fatores; e

IV - os acessos ao diretório devem ser registrados em trilhas de auditoria, que devem conter, no mínimo, data e hora do acesso na timezone UTC, endereço IP de origem da chamada, porta de comunicação origem da chamada (porta TCP do cliente), URI acessada, método HTTP utilizado e status de retorno, observada a legislação e a regulamentação vigentes.

Brasília, 29 de outubro de 2020.

Este conteúdo não substitui o publicado na versão certificada.