# Autoavaliação dos requisitos de SI

**Versão 1.0 10/02/2021**

Esse documento foi elaborada para auxiliar os participantes do Open Banking a alcançar um nível adequado de Segurança da Informação por meio de um checklist que contém os seguintes domínios:

* Governança: Tem o objetivo de estruturar um sistema que alinhe os objetivos específicos da segurança da informação com a estratégia institucional para Open Banking, para dessa forma reduzir os riscos e maximizar a entrega de valor, dirigindo e controlando as atividades da segurança da informação;
* Proteção: Definir controles mínimos de segurança da informação, necessários para proteção dos ativos de informações das Instituições participantes do Open Banking;
* Detecção: Demonstrar métodos detectivos de segurança da informação destinados aos participantes do Open Banking;
* Reação: Definir controles, capacitação e processos integrados de modo que os participantes do Open Banking possam responder a eventos e violações de segurança e se comunicarem entre si quando necessário;
* Diretório: Define controles que os participantes devem exercer no Diretório relacionados à Segurança da Informação.

Deve ser feito o preenchimento da coluna “Implementação”, quando aplicável, com “Sim”, “Não” ou “N/A” (N/A quando o item descrito não se aplica à instituição) a fim de mensurar o nível de maturidade de Segurança (SI) da instituição participante do Open Banking.

|  |
| --- |
| **Checklist para auto avaliação aos cumprimentos dos requisitos de segurança da informação** |
| **Seção** | **Item** | **Título** | **Implementação** |
| **1** |   | **Governança** |   |
| 1 | 1.1 | Compõem, de forma não exaustiva, o rol de atos normativos cuja observância é essencial pelas instituições participantes do Open Banking: |  |
|  1 | 1.1.1 | Resolução Conjunta CMN/BCB nº 1, de 2020; |   |
|  1 | 1.1.2 | Resolução CMN nº 4.658, de 2018; |   |
|  1 | 1.1.3 | Circular BCB nº 3.909, de 2018; e |   |
|  1 | 1.1.4 | Lei Geral de Proteção de Dados Pessoais (LGPD - Lei nº 13.709, de 2018). |   |
| 1 | 1.2 | O plano de ação e resposta a incidentes do participante deve contemplar as APIs de Open Banking, de acordo com a regulamentação vigente. |   |
| 1 | 1.3 | Monitorar e garantir que os terceiros contratados pelas instituições participantes do ecossistema implementem regras e boas práticas fazendo parte do plano de resposta a incidentes da instituição, de acordo com a regulamentação vigente. |   |
| 1 | 1.4 | As instituições participantes do ecossistema Open Banking devem garantir que os terceiros, especialmente os prestadores de serviços, cumpram toda a legislação e regulamentação aplicável sobre Segurança da Informação, privacidade e proteção de dados. |   |
| 1 | 1.5 | Os dados devem ser armazenados de acordo com o propósito e consentimento obtido e descartados de maneira segura após o término de sua finalidade e consentimento. Recomendações: NIST 800-88, DOD 5220.22-M. |   |
| **2** |   | **Proteção** |   |
| 2 | 2.1 | O acesso aos dados no âmbito do Open Banking deve ser realizado exclusivamente por meio de APIs. |   |
| 2 | 2.2 | 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. |   |
| 2 | 2.3 | 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). |   |
| 2 | 2.4 | 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). |   |
| 2 | 2.5 | As funcionalidades "TLS Session Resumption" e "TLS Renegotiation" devem ser desabilitadas. |   |
| 2 | 2.6 | 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. |   |
| 2 | 2.7 | As instituições não devem expor os repositórios de dados utilizados no Open Banking diretamente à internet. |   |
| 2 | 2.8 | Os participantes devem verificar e garantir que os formatos do conteúdo das requisições (schemas) estejam de acordo com aqueles estabelecidos pelas definições de Open Banking. |   |
| 2 | 2.9 | No âmbito do Open Banking Brasil, para a comunicação segura entre as APIs e assinatura de mensagens, devem ser utilizados certificados digitais válidos e emitidos por autoridade certificadora participante da ICP-Brasil de acordo com os padrões para certificação digital definidos na área do desenvolvedor do Portal do Open Banking Brasil, seja para proteção dos canais de comunicação seja para assinatura ou criptografia de mensagens trocadas em API´s. |   |
| 2 | 2.9.1 | Em caráter de exceção, durante a fase de implementação, será tolerado o uso de certificados digitais emitidos pelo serviço de Diretório. |   |
| 2 | 2.9.2 | O disposto no caput é aplicável, no que couber, aos certificados requeridos para contratações de parceria para fins de compartilhamento de dados previstas na regulamentação em vigor. |   |
| 2 | 2.10 | Para o estabelecimento de conexões TLS das chamadas de endpoints confidenciais devem ser utilizados os algoritmos TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 e TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384. |   |
| 2 | 2.11 | Os certificados utilizados para comunicação de sistemas Front-End, acessados diretamente por usuários, em especial para realizar autenticação de usuários devem ser do tipo EV e podem ser emitidos por Autoridade Certificadora válida de mercado. |   |
| 2 | 2.12 | Qualquer segredo ou chave devera possuir meios seguros de armazenamento, transferência, utilização e destruição para que se possa garantir toda a integridade e confidencialidade da informação que está sendo utilizada. Como exemplo, mas não se limitando a: refresh token, chaves privadas e outros, observada a regulamentação em vigor. |   |
| 2 | 2.13 | Caso seja feito uso de algoritmos criptográficos para proteção e armazenamento de segredos, recomendando-se: AES-256bits ou superior, SHA-256bits ou superior, RSA-2048bits ou superior. |   |
| 2 | 2.14 | É recomendável que segredos e chaves utilizados para autenticar, proteger e garantir integridade de dados sejam gerados de maneira a respeitar processos de duplo controle e split-of-knowledge, contendo registro que incluem data de geração, participantes e responsáveis pela custódia, quando aplicável. |   |
| 2 | 2.15 | Os participantes responsáveis por APIs utilizadas no Open Banking devem implementar mecanismos de segurança capazes de verificar a presença vulnerabilidades nas APIs durante todo o seu ciclo de vida, observada a regulamentação em vigor. |   |
| 2 | 2.16 | Os participantes devem implementar processos de revisão periódica para garantir que somente portas e serviços autorizados estejam habilitados, observada regulamentação vigente. |   |
| 2 | 2.17 | As instituições participantes devem definir e orientar os requisitos necessários para implementação de mecanismos de autenticação e autorização em sistema, incluindo as aplicações, respeitando: |   |
| 2 | 2.17.1 | As instituições participantes devem garantir que portais e aplicações possuam meios de autenticação confiáveis e controle de autorização. |   |
| 2 | 2.17.2 | O processo de autenticação deve ser sempre realizado através de um canal de comunicação seguro, como por exemplo TLS 1.2 ou superior. |   |
| 2 | 2.18 | Os acessos remotos a sistemas ou infraestrutura relacionada ao Open Banking devem ser realizados com autenticação de usuários, mediante uso de MFA, observada regulamentação vigente. |   |
| **3** |   | **Detecção** |   |
| 3 | 3.1 | 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. |   |
| 3 | 3.2 | 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. |   |
| 3 | 3.3 | As vulnerabilidades encontradas nas APIs ou demais sistemas relacionados ao Open Banking devem ser categorizadas e priorizadas de acordo com classificação de risco. |   |
| 3 | 3.4 | As APIs e demais sistemas relacionados ao Open Banking devem ser implementados usando padrões de configuração segura (hardening), observada a regulamentação vigente. |   |
| 3 | 3.5 | Os participantes e demais integrantes do ecossistema devem monitorar os logs de suas APIs, em especial os registros que indicarem erros internos (ex: status HTTP 500), requisições inválidas (ex: status HTTP 400), observada a regulamentação em vigor. |   |
| 3 | 3.6 | As instituições devem implementar um processo formal de aplicação de patch baseando-se nas políticas internas da organização e que contemple todos os sistemas relacionados a implementação do Open Banking, observada regulamentação vigente. |   |
| **4** |   | **Reação** |   |
| 4 | 4.1 | 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 | 4.2 | Em caso de comprometimento de credencial, o participante do Open Banking deve revogá-la imediatamente junto ao diretório e comunicar aos demais participantes, observando a regulamentação vigente. |   |
| 4 | 4.3 | Efetuar comunicação para todas as instituições participantes no momento da confirmação de um incidente cibernético ligado aos serviços do Open Banking, independente da instituição ser transmissora ou receptora de dados. |   |
| 4 | 4.4 | No âmbito do Open Banking e observada a regulamentação em vigor, o plano de ação e resposta a incidentes deve contemplar, no mínimo, procedimentos para detectar e reagir a incidentes que possam implicar em: |   |
| 4 | 4.4.1 | Acesso não autorizado; |   |
| 4 | 4.4.2 | Vazamento de dados; |   |
| 4 | 4.4.3 | Negação de serviço. |   |
| 4 | 4.5 | As instituições participantes devem dar conhecimento à equipe definida no item 5.5 em casos de bloqueios ou suspeitas de ataques que contenham como origem um dos participantes do Open Banking. |   |
| **5** |   | **Diretório** |   |
| 5  | 5.1 | 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. |   |
|  5 | 5.2 | Cada instituição deve disponibilizar os contatos de e-mail das equipes de segurança conforme a RFC 2142 (abuse e security). |   |
|  5 | 5.3 | O acesso às áreas restritas do diretório de participantes deve ser condicionado à autenticação por, no mínimo, dois fatores. |   |
|  5 | 5.4 | 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. |   |

**Nível de aderência:**

