# Política de Segurança Cibernética – Resolução Nº 4.658 do Banco Central do Brasil ("Política de Segurança Cibernética - Brasil")

Este é um resumo contendo as linhas gerais da Política de Segurança Cibernética – Brasil, em cumprimento à Resolução n° 4.658 ("Resolução 4.658") do Banco Central do Brasil ("Bacen").

Versão 1/201905

Publicado no Portal Banco JPMorgan em Junho 2019

## 1. Sumário

A Resolução N° 4.658 dispõe sobre a política de segurança cibernética e os requisitos para os serviços de processamento e armazenamento de dados e computação em nuvem contratados por instituições financeiras e demais instituições autorizadas a operar pelo Bacen.
A Resolução 4.658 exige que tais instituições desenvolvam, implementem e mantenham uma política de Segurança Cibernética abrangente baseada em princípios e diretrizes que buscam garantir a confidencialidade, integridade e disponibilidade dos dados e dos sistemas de informação utilizados. A política de segurança cibernética deve abranger:

- Objetivos de segurança cibernética, que devem contemplar a capacidade da instituição de prevenir e detectar incidentes cibernéticos, reduzindo a vulnerabilidade;
- Procedimentos e controles para mitigar vulnerabilidades a incidentes e atender a outros objetivos da segurança cibernética, incluindo autenticação, criptografia, prevenção e detecção de intrusão, prevenção de vazamento de dados, realização periódica de testes e varreduras para detecção de vulnerabilidades, proteção contra softwares maliciosos, controle de acesso, redes de computadores segmentadas e manutenção de cópias de segurança dos dados e das informações;
- Controles para garantir a rastreabilidade dos dados, a fim de proteger informações sensíveis;
- Gerenciamento de Incidente, incluindo procedimentos aplicáveis a fornecedores e comunicação tempestiva de incidentes relevantes ao Bacen, incluindo incidentes relatados por fornecedores;
- Cenários de incidentes cibernéticos a serem considerados nos Testes e Planos de Continuidade de Negócios;
- Mecanismos de divulgação da cultura e das disposições da política de segurança cibernética dentro da instituição, incluindo:

  a) programas recorrentes de treinamento de pessoal;

  b) informações aos clientes e usuários sobre os cuidados com o uso de produtos e serviços financeiros;

  c) compromisso da alta administração com a melhoria contínua dos procedimentos relacionados à segurança cibernética.
- Compartilhamento de informações com outras instituições financeiras; e
- Diretrizes para a classificação de dados/informações.

A política de segurança cibernética deve ser compatível com:

I - o tamanho, o perfil de risco e o modelo de negócio da instituição financeira;
II - a natureza de suas operações e a complexidade de seus produtos, serviços, atividades e processos; e
III - o sigilo dos dados e das informações sob a responsabilidade da instituição financeira.

Além disso, a Resolução 4.658 estabelece que tais instituições financeiras devem cumprir requisitos específicos para serviços de processamento, armazenamento e computação em nuvem.

## 2. Escopo

| | |
|---|---|
| Linhas de Negócios | Todas as Linhas de Negócios |
| Função(ões) | Todas as funções |
| Locais | • Brasil |
| Entidades Legais | • Banco J.P. Morgan S.A.<br>• J.P. Morgan Corretora de Câmbio e Valores Mobiliários S.A.<br>• J.P. Morgan S.A. - Distribuidora de Títulos e Valores Mobiliários<br>• J.P. Morgan Chase Bank, National Association (Filial Brasileira) |

A Política de Segurança Cibernética - Brasil aplica-se às Entidades Legais mencionadas acima, definidas coletivamente como “JPMC Brasil”, incluindo todos os seus empregados, terceirizados e estagiários com acesso aos sistemas/dados do JPMC Brasil e de prestadores de serviço relevantes que processam/armazenam dados do JPMC Brasil. Qualquer referência a “JPMC” ou “Empresa” nesta Política de Segurança Cibernética - Brasil inclui o JPMC Brasil e qualquer outra Entidade Legal do JPMorgan Chase & CO.

## 3. Política de Segurança Cibernética - Brasil

O JPMC faz parte do Programa Global de Segurança da Informação do JPMC, que engloba a governança, políticas, processos, avaliações, controles, testes e treinamento, além de controles de Segurança Cibernética aplicados para prevenir, detectar e reagir aos ataques cibernéticos conforme requeridos na Resolução 4.658.

Os Controles de Segurança Cibernética do JPMC (“Controles de Segurança Cibernética”) adotam/seguem as “Políticas e Controles de Tecnologia Globais” que fornecem a base do Programa de Segurança da Informação e estabelecem as regras para proteger o ambiente de TI:

- Garantir a segurança e a confidencialidade das informações de clientes e empregados;

- Proteger contra ameaças ou riscos à segurança dessas informações;
- Proibir o acesso não autorizado ou o uso de informações que possam prejudicar os clientes ou empregados;
- Armazenar, transportar e descartar adequadamente informações de clientes e empregados;
- Informar os empregados sobre suas responsabilidades de proteger as informações de clientes e a segurança dos sistemas do JPMC;
- Garantir que os prestadores de serviços terceirizados e relevantes cumpram com nossas políticas e normas de segurança, bem como as obrigações regulamentares aplicáveis;
- Cumprir todos os requisitos de notificação do cliente para proteção das informações.

Em parceria com as linhas de negócios do JPMC Brasil, a equipe global de Segurança Cibernética e Controles de Tecnologia ("CTC" – Cybersecurity and Technology Controls) identifica os riscos à segurança da informação e promove programas de proteção tecnológica aos recursos de informação do JPMC Brasil, incluindo aplicativos, infraestrutura e informações confidenciais e privadas relacionadas a clientes e empregados.

O CTC é responsável pela governança e supervisão do Programa de Segurança da Informação, que é revisado e aprovado anualmente. Auditores internos e externos revisam continuamente os programas e processos de TI.

A Política de Segurança Cibernética no Brasil foi desenvolvida para atender aos requisitos da Resolução 4.658 e abrange as Políticas, Normas e Procedimentos do JPMC, conforme abaixo indicado.

## 4. Reduzindo as Vulnerabilidades e Protegendo a Confidencialidade, Integridade e Disponibilidade dos Dados

A fim de reduzir a vulnerabilidade do JPMC aos incidentes e cumprir outros objetivos da segurança cibernética, o CTC é responsável pela criação, administração e supervisão de políticas e normas concebidas para garantir que os riscos sejam identificados e gerenciados dentro de tolerâncias corporativas definidas, incluindo a prevenção, detecção, contenção e correção de violações de segurança da informação.

O CTC, por meio de seus programas individuais, contribui coletivamente para o Programa de Segurança da Informação. Os programas são documentados e atualizados anualmente para garantir a conformidade contínua com os requisitos regulamentares.

### 4.1. Autenticação

A Norma de Gerenciamento de Identidade e Autenticação tem como principal objetivo o gerenciamento de identidades digitais para usuários, sistemas e processos, bem como na verificação de identidades que acessam recursos do JPMC.

### 4.2. Criptografia

Os controles relacionados à criptografia são abrangidos pela norma de “Proteção de Dados” cujo objetivo é estabelecer requisitos de controle para proteger os dados em todos os ativos de informação do JPMC. Esta norma se aplica à proteção de dados em armazenamento e na transmissão, para todos os ativos do JPMC, incluindo ativos de terceiros onde os dados do JPMC estão sendo armazenados ou processados.

### 4.3. Prevenção e detecção de intrusão

Controles de mitigação são implementados nos perímetros da rede para limitar e conter o impacto de potenciais eventos de segurança cibernética.

O escopo inclui os perímetros da infraestrutura de rede em que são estabelecidas as conexões.

### 4.4. Prevenção de vazamento de informações

Prevenção à Perda de Dados (DLP – Data Loss Prevention) refere-se à estratégia, às ferramentas e às regras para permitir o controle de informações sensíveis ou críticas enviadas para fora da rede da Empresa. O programa de DLP permite ao JPMC proteger os dados dos clientes, informações da Empresa, propriedade intelectual e informações sensíveis ou confidenciais, impedindo, investigando e monitorando o envio de dados não autorizados. O programa detecta possíveis violações, padrões ou práticas que possam infringir regulamentos da Empresa, incluindo a má conduta de mercado dos empregados.

### 4.5. Realização periódica de testes e varreduras para detecção de vulnerabilidades

A identificação e a eliminação tempestiva de vulnerabilidades de tecnologia são fundamentais para garantir a integridade do ambiente dos processos de negócios. A descoberta de vulnerabilidades aplicáveis ao JPMC exige processos que combinem o monitoramento contínuo (inteligência externa, varredura e métricas) para identificar os recursos afetados e a avaliação de riscos para determinar a priorização para a correção.

### 4.6. Proteção contra softwares maliciosos

O objetivo desta norma é definir os requisitos de controle de detecção e prevenção para impedir que códigos maliciosos sejam executados e se infiltrem na rede da Empresa. O código malicioso pode ser transportado por diferentes meios, incluindo, por exemplo, acessos à Internet, correio eletrônico, anexos de correio eletrônico e dispositivos de armazenamento portáteis. Os mecanismos de proteção contra códigos maliciosos incluem, por exemplo, o monitoramento de atividades de *endpoints* e controles de proteção de hardware.

### 4.7. Estabelecimento de mecanismos de rastreabilidade

O JPMC captura eventos relevantes para a identificação de possíveis incidentes de segurança cibernética (aqueles resultantes de atividades de intenção maliciosa). Os eventos são capturados e analisados pelo Centro de Operações de Segurança (SOC – Security Operations Center) e utiliza serviços/ferramentas de SEIM (Security Event and Incident Management) para monitorar e analisar os dados/alertas.

### 4.8. Controles de acesso e segmentação da rede de computadores

O programa de Gerenciamento de Identidade e Acesso implementa padrões e controles de acesso em toda a infraestrutura e aplicativos, especialmente aqueles que contêm informações de clientes. Esses controles são projetados para autenticar usuários, permitir acesso autorizado, garantir procedimentos administrativos consistentes, manter a segregação de funções e garantir atualizações tempestivas por meio de processos de inclusão/exclusão/transferência nos sistemas da Empresa.

### 4.9. Manutenção de cópias de segurança dos dados e das informações

O backup operacional abrange proteção de dados em nível de arquivo, retenção de dados e recuperação de arquivos para atender aos requisitos de recuperação operacional e inclui backup de dados, restauração e validação de backup e recertificação.

### 4.10. Desenvolvimento de sistemas e adoção de novas tecnologias

A norma de “Desenvolvimento de Tecnologia” estabelece os requisitos de controle para o desenvolvimento de tecnologia, incluindo mudanças de software e configuração, independentemente da estrutura ou do modelo do ciclo de vida de desenvolvimento de software (SDLC) seguido pela equipe.

Esta norma se aplica ao software desenvolvido pelo JPMC, incluindo alterações de configuração, e aos desenvolvedores associados a esse desenvolvimento.

## 5. Gerenciamento de incidente

Os recursos de gerenciamento de eventos e incidentes de segurança possibilitam o monitoramento, a detecção e a investigação de eventos e incidentes relacionados à segurança. Esses recursos se apoiam nos serviços de inteligência *(threat intelligence)*, nas medidas de risco operacional e no contexto dos negócios para melhorar continuamente a detecção antecipada de ameaças e coordenar respostas integradas aos eventos relacionados à segurança.

O JPMC Brasil comunicará em tempo hábil os incidentes relevantes ao Bacen, conforme exigido pelo Art. 19 e pelo Art. 20, III, da Resolução 4.658.

## 6. Cenários de incidentes para continuidade de negócios

O programa de Resiliência e Recuperação é projetado para recuperar funções críticas de negócios e suportar ativos em caso de uma interrupção de negócios. Os principais elementos incluem:

- Fornecer continuidade de serviços ao cliente, protegendo os funcionários e ativos da Empresa;
- Engajar a alta gerência no programa;
- Gerenciar riscos de resiliência proativamente para incorporar procedimentos e controles apropriados;
- Desenvolver e manter planos de resiliência com base na análise de impacto e criticidade;

• Ajudar os empregados a entender seu papel em cenários de recuperação e a realizar exercícios de validação em funções e locais críticos.

Todas os aplicativos identificados como CAF *(Critical Availability Framework)* devem ter planos para cenários de recuperação para endereçar *malwares* cibernético.

## 7. Divulgação da segurança cibernética

O treinamento em segurança cibernética é obrigatório para todos os empregados globalmente. O treinamento é baseado nas políticas e normas de segurança cibernética e é complementado por um programa de conscientização cibernética e iniciativas de testes, incluindo testes de *phishing*.

Os empregados que não passarem nos testes de *phishing* são notificados imediatamente com um lembrete de políticas e recursos disponíveis para melhorar sua capacidade de reconhecer a engenharia social.

## 8. Compartilhamento de Informações

O JPM Brasil compartilha inteligência relacionada a ameaças cibernéticas relevantes e vulnerabilidades (Threat Intelligence) com outras instituições financeiras por meio de plataformas comumente utilizadas.