Política Pública de Resiliência Operacional

Introdução

O BBVA Brasil atua no setor financeiro, oferecendo produtos e serviços aos seus clientes. No curso de suas atividades, o BBVA Brasil se compromete a garantir o bom funcionamento dos serviços e produtos que presta.

A gestão eficaz dos riscos operacionais, que podem surgir de interrupções na prestação desses serviços, exige que o BBVA Brasil alcance níveis adequados de Resiliência Operacional. Este conceito abrange a Gestão de Continuidade de Negócios, Tecnologia de Informação e Comunicação (TIC) e a Resiliência Operacional Digital. A segurança de redes e sistemas de informação, em particular, é fundamental para resistir a qualquer evento que possa comprometer a disponibilidade, a autenticidade, a integridade e a confidencialidade dos dados.

Para assegurar essa resiliência, o BBVA Brasil adota políticas, procedimentos, diretrizes, arquitetura de segurança e controles técnicos robustos. Nossas políticas e controles são continuamente avaliados para garantir sua relevância e alinhamento com os padrões de mercado e os requisitos regulatórios aplicáveis, incluindo os estabelecidos na Resolução CMN nº 4.893 do Banco Central do Brasil, especialmente no que diz respeito à segurança cibernética e contratação de serviços de TIC.

Objetivo

O objetivo desta política é estabelecer os princípios e diretrizes básicas de gestão e controle que o BBVA Brasil segue. Com ela, garantimos a capacidade de identificar, proteger-nos de ameaças e potenciais eventos disruptivos e, caso se materializem, responder e nos recuperar deles para minimizar seu impacto, assegurando assim níveis adequados de Resiliência Operacional.

Princípios Essenciais da Resiliência Operacional do BBVA Brasil

A Resiliência Operacional no BBVA Brasil é guiada por princípios específicos para garantir a proteção e a continuidade dos serviços:

- **Princípio da Disponibilidade:** Processos comerciais críticos, sistemas de informação e dados associados devem estar disponíveis de forma confiável para clientes, funcionários ou terceiros autorizados.
- **Princípio da Confidencialidade:** Dados sensíveis e confidenciais são protegidos para garantir acesso apenas por usuários devidamente autorizados.

- **Princípio da Integridade:** Dados críticos são protegidos contra modificações inadequadas ou destruição, seja voluntária ou acidental.
- **Princípio da Autenticidade:** Dados críticos, especialmente os relacionados a clientes e transações, são autenticados para garantir sua origem legítima e confiável, prevenindo fraudes.
- **Princípio da Segurança Física:** Instalações, ativos, processos operacionais e pessoas são protegidos para evitar acesso não autorizado ou adulteração.

Além destes princípios, o BBVA Brasil adota as seguintes diretrizes e capacidades:

1. Gestão de Continuidade de Negócios e Recuperação

O BBVA Brasil possui uma abordagem abrangente com políticas, padrões e procedimentos para garantir que operações críticas possam ser mantidas e recuperadas em tempo hábil em caso de interrupção.

- **Análise de Impacto no Negócio:** Processos críticos de negócio são identificados por meio de análise de impacto, considerando eventos de baixa probabilidade e alto impacto financeiro, legal, reputacional e/ou regulatório.
- **Planos de Resposta e Recuperação:** Planos, procedimentos e mecanismos são implementados para garantir a continuidade das atividades e responder a incidentes, incluindo a contenção de danos, estimativa de repercussões e comunicação.
- **Cópias de Segurança (Backup):** Padrões e procedimentos de backup são definidos para a restauração de sistemas de TIC e a recuperação de dados críticos, incluindo cópias inalteráveis para proteção contra ataques destrutivos.

2. Resiliência Operacional Digital e Segurança de TIC

O BBVA Brasil mantém uma estrutura robusta de gestão de riscos de TIC, que inclui estratégias, normas, procedimentos e ferramentas para proteger todos os Ativos de Informação e Ativos de TIC (software, hardware, servidores, infraestrutura física, como data centers).

- **Identificação de Riscos:** Funções, deveres, responsabilidades e ativos de TIC que suportam processos de negócio críticos são identificados e classificados. Ameaças cibernéticas e vulnerabilidades de TIC relevantes são continuamente avaliadas.
- **Proteção de Sistemas:** A segurança e operação dos sistemas e ferramentas de TIC são continuamente monitoradas e controladas. São implementados padrões, procedimentos e ferramentas de segurança para garantir resiliência, continuidade, disponibilidade, integridade, confidencialidade e autenticidade dos dados.

- **Detecção de Anomalias:** Mecanismos são estabelecidos para detectar urgentemente atividades anômalas, mau funcionamento e incidentes de TIC, com diferentes níveis de controle e alertas automáticos para o pessoal responsável.
- **Gestão de Controles de Acesso:** São estabelecidos controles de acesso para garantir que apenas usuários autorizados tenham acesso a dados e sistemas sensíveis.
- **Segurança do Ciclo de Vida do Software:** O desenvolvimento de software incorpora requisitos funcionais e não funcionais, rastreabilidade de testes e segurança no código-fonte para garantir a resiliência operacional.
- **Segurança de Redes:** A proteção de redes e sistemas de informação é fundamental para resistir a eventos que possam comprometer a disponibilidade, autenticidade, integridade e confidencialidade dos dados. A segmentação de rede é aplicada para fortalecer a segurança.

3. Segurança Física

Medidas de segurança física são implementadas para proteger as instalações, ativos, processos operacionais do Banco, funcionários e clientes contra eventos de origem intencional.

4. Gestão de Riscos com Terceiros

A resiliência operacional do BBVA Brasil também depende da capacidade de terceiros envolvidos em seus processos operacionais e cadeias de valor. Um processo de avaliação da relevância dos prestadores de serviços, com base em critérios e requisitos de segurança cibernética para serviços de processamento, armazenamento de dados e computação em nuvem, é estabelecido, em conformidade com a Resolução CMN nº 4.893 do Banco Central do Brasil.

5. Formação e Conscientização

Programas de treinamento são estabelecidos para todos os funcionários e a alta gerência, com nível de complexidade adequado às suas responsabilidades. Esses programas são estendidos a provedores terceirizados de serviços de TIC, quando apropriado.

6. Gestão e Notificação de Incidentes

O BBVA Brasil desenvolve processos para a detecção, gestão, comunicação a clientes (quando requerido), e notificação às autoridades competentes e reguladores dos incidentes mais significativos, baseando-se em uma classificação de criticidade.

7. Testes e Melhoria Contínua

- **Testes de Resiliência:** Um programa de testes é estabelecido, mantido e revisado regularmente para avaliar o estado de preparação, identificar fraquezas e implementar medidas corretivas.
- **Melhoria Contínua:** Os resultados dos testes, a experiência de incidentes reais e os problemas encontrados na ativação de planos são continuamente incorporados ao processo de avaliação de risco.

8. Governança e Supervisão

A política de Resiliência Operacional do BBVA Brasil está alinhada ao modelo de controle que inclui indicadores para monitorar o progresso.

- Três Linhas de Defesa: A gestão de riscos é estruturada em três linhas de defesa:
    - A Primeira Linha de Defesa é responsável pela gestão diária dos riscos e verificação da conformidade com a política e regulamentações.
    - A Segunda Linha de Defesa é independente da primeira e define Controles e Monitoramentos de Riscos de TIC, garantindo que as medidas implementadas mitiguem os riscos e verificando o cumprimento das normas internas.
    - A Auditoria Interna atua como a terceira linha de defesa, realizando uma revisão independente dos controles e cumprimento da política.