POLÍTICA DE SEGURANÇA CIBERNÉTICA

Conglomerado Banco Mercedes-Benz do Brasil S/A

ÍNDICE

1. OBJETIVO

O objetivo desse documento é formalizar as diretrizes necessárias para assegurar a confidencialidade, integridade e a disponibilidade das informações e dos sistemas de informação utilizados pelo **BMB**, constituindo a base de um sistema de gestão da segurança cibernética bem como de direcionadores para um programa de prevenção, detecção e redução de impactos gerados pelos incidentes, levando em consideração, o porte, a complexidade, a estrutura, o perfil de risco, os requisitos do negócio, a legislação e regulamentações vigentes.

Esta política de segurança cibernética constitui um conjunto de princípios e diretrizes, sendo parte integrante do sistema de Controles Internos do Conglomerado Banco Mercedes-Benz (Conglomerado). O **BMB** entende que uma gestão apropriada do risco de segurança cibernética contribui para o atingimento de seus objetivos estratégicos e de negócios.

Para assegurar a gestão integrada de riscos, os assuntos relacionados à segurança cibernética fazem parte das atribuições e agenda do Comitê de Risco do **BMB**.

Para fins desta política, o conglomerado Banco Mercedes-Benz é composto pelas seguintes empresas:

- Banco Mercedes-Benz do Brasil
- Mercedes-Benz Leasing Arrendamento Mercantil
- Mercedes-Benz Corretora de Seguros
- Mercedes-Benz Assessoria Comercial

Denominamos este conjunto de companhias como **BMB** ou simplesmente **Banco Mercedes Benz do Brasil** nesta política.

2. OBJETIVOS DE SEGURANÇA CIBERNÉTICA

A estrutura de segurança cibernética do **BMB**, composta por pessoas, sistemas, controles, processos e procedimentos tem por objetivo a prevenção, detecção e redução de vulnerabilidades e impactos gerados pelos incidentes relacionados ao ambiente cibernético.

Esta estrutura também deve assegurar a confidencialidade, a integridade e disponibilidade dos dados e dos sistemas de informação utilizados pelo **BMB**, em conformidade com as melhores práticas de mercado e normas nacionais e internacionais.

3. ABRANGÊNCIA

Esta Política se aplica a todos os colaboradores, sejam eles diretores executivos, gestores, empregados, aprendizes, estagiários, terceiros e parceiros que possuam acesso às informações do **BMB**.

4. PROCEDIMENTOS E CONTROLES DE VULNERABILIDADES

Tomando por base os objetivos de segurança cibernética do **BMB**, abaixo estão as diretrizes e controles mínimos para que estes objetivos sejam alcançados.

Os procedimentos e os controles aqui previstos devem ser aplicados, quando possível, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades do **BMB**.

4.1. AUTENTICAÇÃO

O dono da informação deve estabelecer juntamente com o responsável de Segurança da Informação um nível de autenticação seguro baseado na classificação da informação, seguindo os controles de senhas fortes, utilização de dois fatores ou duas etapas, rastreabilidade e integração com uma base centralizada e segura de usuários.

4.2. CRIPTOGRAFIA

O dono da informação deve estabelecer juntamente com o responsável de Segurança da Informação um nível seguro de mecanismos para garantir a confidencialidade das informações. A utilização de chave de criptografia segura é mandatória para informações classificadas como confidencial em todos os ambientes do **BMB**. A utilização de criptografia para informações classificadas como interna é mandatória somente em ambiente externo do **BMB**.

4.3. PREVENÇÃO E A DETECÇÃO DE INTRUSÃO

Serviços do **BMB** que são disponibilizados para a Internet requerem um controle para detecção e prevenção a intrusão. É mandatória a utilização de sistemas de IDS/IPS (*Intrusion Detection/Prevention System*) em perímetro de borda da Internet quando necessário a publicação de um serviço ou sistema via internet.

Os sistemas de IDS/IPS devem ser monitorados pela área de TI e avaliados pelo responsável de Segurança da Informação, seguindo as boas práticas de mercado, ex. ISO 27001.

4.4. PREVENÇÃO DE VAZAMENTO DE INFORMAÇÕES

A manipulação de informações classificadas como confidenciais deve ser monitorada por um sistema de DLP (*Data Loss Prevention*) efetivo e adequado ao porte dos serviços e sistemas do **BMB**.
O sistema de DLP deve ser monitorado pela área de TI e avaliado pelo responsável de Segurança da Informação, seguindo as boas práticas de mercado, ex. ISO 27001.

4.5. TESTES E VARREDURAS PARA DETECÇÃO DE VULNERABILIDADES

O **BMB** considera o gerenciamento de vulnerabilidades um dos principais controles de segurança. A identificação de vulnerabilidades é o primeiro passo a redução/mitigação de riscos cibernéticos.

Para atender este controle o **BMB** deve possuir sistemas e processos que identifiquem os pontos mais fracos que podem ser explorados por ameaças cibernéticas. Estes sistemas e processos devem atender aos diferentes perímetros e camadas de tecnologias do **BMB**.

Abaixo os requisitos mínimos de sistemas e processos para avaliação de testes, varreduras e remediações periódicas de vulnerabilidades:

- Desenvolvimento de código dos sistemas aplicativos;
- Sistemas operacionais;
- Serviços web, transferência de arquivos, gerenciamento, etc;
- Bancos de Dados.

O **BMB** também deve executar anualmente, por relevância, testes de intrusão em:

- Sistemas que contenham informações classificadas como confidenciais;
- Servidores que suportam serviços considerados críticos.

A remediação das vulnerabilidades identificadas nos testes acima deve seguir a recomendação de prazos estipulados pelo responsável de Segurança da Informação.

4.6. PROTEÇÃO CONTRA SOFTWARES MALICIOSOS

O **BMB** considera mandatória a utilização de programas de antivírus e atualização de correções de segurança em todos as estações de trabalhos e servidores.

O programa de antivírus deverá atualizar periodicamente conforme os padrões corporativos. É proibida a inclusão de máquinas na rede com sistemas obsoletos, sem suporte a um programa de antivírus ativo e atualização das correções de segurança.

4.7. MECANISMOS DE RASTREABILIDADE

O **BMB** considera o gerenciamento de logs um mecanismo essencial para governança, monitoramento, detecção e resposta para ações maliciosas.

Os sistemas aplicativos do **BMB** devem garantir um padrão mínimo de logs que permita a rastreabilidade de acesso aos dados, considerando a informação acessada, quem, quando, onde e quais operações realizadas.

4.8. CONTROLES DE ACESSO E DE SEGMENTAÇÃO DA REDE

O **BMB** deve conhecer o nível de acesso a informação mapeado por criticidade e exposição.

Abaixo a segmentação mínima adequada ao porte do **BMB**:

- Serviços de Produção;
- Serviços de Teste e Aceite de usuários;
- Serviços de Desenvolvimento;
- Camada de apresentação de serviços de internet;
- Camada de apresentação de serviços de intranet;
- Camada de aplicação e inteligência do negócio;
- Camada de bancos de dados.

Todos os segmentos e perímetros devem possuir um controle de acesso adequado ao mínimo necessário para funcionamento dos serviços e/ou necessário para desempenho das funções corporativas. Este controle de acesso deve ser realizado considerando múltiplas camadas de acesso e suas devidas tecnologias, como firewalls e demais sistemas de autenticação e controle de acesso.

4.9. CÓPIAS DE SEGURANÇA

O **BMB** é responsável pelo processo de salvaguarda dos dados necessários para completa recuperação dos seus sistemas relevantes, a fim de atender os requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes, além de auxiliar em sua ágil recuperação.

A base para definição de processos críticos do **BMB** é a Análise de Impacto de Negócios, internamente denominado como BIA.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

A informação é um importante ativo do **BMB** e deve ser preservada e salvaguardada, em conformidade com suas políticas, normas, procedimentos e controles internos, bem como, com as leis e regulamentos

dos órgãos reguladores e autorreguladores sobre o tema. As informações devem ser classificadas e tratadas de acordo com os requisitos especificados na regulamentação interna e externas vigentes.

6. RESPOSTA A INCIDENTES

Minimizar o impacto às operações do negócio requer uma resposta eficaz a um incidente que poderia pôr em risco a segurança da informação. A resposta a um incidente deve ser administrada em conformidade com os requisitos especificados no Plano de Resposta à Incidentes do **BMB**.

No plano de resposta a incidentes está previsto o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição, incluindo as informações recebidas de empresas prestadoras de serviços.

As empresas prestadoras de serviço que manuseiem dados ou informações sensíveis ou que sejam relevantes para as atividades do **BMB** também devem possuir procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes. Os procedimentos e controles devem ser compatíveis com os utilizados pelo **BMB** em nível de complexidade, abrangência e precisão. O responsável pelo prestador de serviço em conjunto com a área de Segurança da Informação deve assegurar que o prestador possua tais controles.

O **BMB** define incidentes relevantes como aqueles que, de acordo com sua gravidade, se enquadram como prioridade 1 (alta) do plano de resposta a incidentes:

1. Todos os incidentes de segurança de informações que afetam diretamente os processos críticos de negócios e os principais aplicativos
2. Comprometimento de dados secretos
3. Comprometimento de grande quantidade de dados confidenciais
4. Incidentes que podem causar danos financeiros ou à reputação em massa

Na eventual ocorrência de incidentes relevantes e de interrupções de serviços relevantes que configurem situação de crise, o **BMB** deverá comunicar esta ocorrência para o Banco Central do Brasil de forma tempestiva, bem como as ações realizadas para solução do incidente ou reinicio das atividades.

Adicionalmente à comunicação ao Banco Central do Brasil, o **BMB** poderá compartilhar informações sobre os incidentes relevantes, incluindo aqueles provenientes de empresas prestadoras de serviços, com as demais instituições financeiras tomando por base a regulamentação vigente. Este compartilhamento deverá ser realizado sem prejuízo do dever de sigilo e da livre concorrência.

Incidentes serão regularmente reportados ao Comitê de Risco, sendo responsabilidade deste comitê deliberar sobre as comunicações ao Bacen e sobre as iniciativas de compartilhamento de incidentes relevantes com as demais instituições financeiras.

O Plano de RISC (Resposta a Incidentes de Segurança Cibernética) está melhor detalhado nos anexos A, B e C desta política.

7. CONTINUIDADE DE NEGÓCIOS

A continuidade de negócio assegura a capacidade de manter as operações críticas para o negócio. A recuperação de desastres assegura a capacidade de restabelecer os recursos críticos de TI no caso de interrupção.

O planejamento de continuidade do negócio e de recuperação de desastres deve ser administrado em conformidade com os requisitos especificados nos requerimentos internos e melhores práticas de mercado, além do Plano de Continuidade do Negócio do **BMB**.

O **BMB** deve elaborar cenários de teste de continuidade de negócios considerando de incidentes cibernéticos. Estes cenários podem contemplar, por exemplo:

1. Indisponibilidade total do Data Center primário do **BMB**;
2. Infecção ou ataques em grande escala por *malware* de alto comprometimento, como por exemplo ataques do tipo *ransomware* ou *DDoS (Distributed Denial of Service)*.

Qualquer cenário que seja definido deve estar alinhado com o escopo dos testes do Plano de Continuidade de Negócios.

8. DISSEMINAÇÃO E TREINAMENTO

Esta política é disponibilizada para todos os funcionários e colaboradores do **BMB** por meio da ferramenta interna denominada Compass, ao qual todos possuem fácil acesso. Ainda como forma de disseminação da política e conscientização sobre Segurança Cibernética, o **BMB** organiza eventos e comunicações reforçando a cultura de mitigação dos riscos associados à Segurança Cibernética.

Adicionalmente, a política de Segurança Cibernética é divulgada para empresas prestadoras de serviço com linguagem clara e com o nível de detalhe compatível com as funções desempenhadas e com a sensibilidade das informações.

O **BMB** possui um plano periódico de capacitação direcionado ao desenvolvimento e manutenção das habilidades dos funcionários e terceiros sobre segurança cibernética.

O **BMB** deve garantir que seus clientes, parceiros de negócios e prestadores de serviços sejam orientados sobre precauções relacionadas ao ambiente cibernético na utilização de seus produtos e serviços disponibilizados publicamente.

Deverá ser divulgado ao público no sitio da internet do **BMB** resumo contendo as linhas gerais da política de segurança cibernética.

9. RELATÓRIO

O **BMB** deve elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes com data-base de 31 de dezembro. Este relatório deve conter, no mínimo:

I - A efetividade da implementação das ações planejadas pelo **BMB** para adequar as estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética.

II - O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias utilizados na prevenção e na resposta a incidentes.

III - Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período.

IV - Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório deve ser submetido ao comitê de risco e apresentado à diretoria do **BMB** até 31 de março do ano seguinte ao da data-base.

10. SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

O processo de definição de terceirização de atividades está alinhado com a estratégia do **BMB** e decidida pelos níveis hierárquicos apropriados.

A contratação de fornecedores, que prestam serviços relevantes ou não, deve seguir as diretrizes estabelecidas no procedimento de compras vigente no **BMB**.

Serviços relevantes de processamento e armazenamento de dados e de computação em nuvem são aqueles que impactam diretamente as atividades "core" do **BMB**, ou seja, aqueles cuja possível indisponibilidade afete a continuidades dos negócios. Adicionalmente, a sensibilidade dos dados e das

informações a serem processados, armazenados e gerenciados pelo contratado também devem ser consideradas na definição de relevância do serviço prestado.

Previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, o **BMB** deve adotar procedimentos que contemplem:

I - a adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas; e
II - a verificação da capacidade do potencial prestador de serviço de assegurar:
a) o cumprimento da legislação e da regulamentação em vigor;
b) o acesso do **BMB** aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
c) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
d) a sua aderência a certificações que por ventura sejam exigidas pelo **BMB** para a prestação do serviço a ser contratado;
e) o acesso do **BMB** aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
f) o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
g) a identificação e a segregação dos dados dos clientes do **BMB** por meio de controles físicos ou lógicos; e
h) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes do **BMB**.

Estes procedimentos e verificações devem estar devidamente documentados.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser previamente comunicada pelo **BMB** ao Banco Central do Brasil, com no mínimo 60 dias de antecedência da contratação. A comunicação deve conter:

I - a denominação da empresa a ser contratada;
II - os serviços relevantes a serem contratados; e
III - a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, no caso de contratação no exterior.

As alterações contratuais que impliquem modificação das informações já prestadas devem ser comunicadas ao Banco Central do Brasil, no mínimo, sessenta dias antes da alteração contratual.

No caso de contratação de serviços no exterior, os seguintes requisitos devem ser observados:

I - a existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;
II - assegurar que a prestação dos serviços não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;
III - definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e
IV - prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

A observação destes requisitos devem ser devidamente documentados.

11. AUDITORIA INTERNA

Os procedimentos descritos nesta política devem ser submetidos a testes periódicos pela auditoria interna, quando aplicável, compatíveis com os controles internos do **BMB**.

12. APROVAÇÃO E REVISÃO

A diretoria do **BMB** é responsável pela aprovação da política e suas subsequentes revisões, reforçando assim seu o comprometimento com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

Tanto esta política quanto o plano de ação e de resposta a incidentes deverão ser revisados, no mínimo, anualmente.