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 **Conglomerado**, 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 por 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 **Conglomerado** 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 **CONGLOMERADO**.

2. OBJETIVOS DE SEGURANÇA CIBERNÉTICA

A estrutura de segurança cibernética do **CONGLOMERADO**, 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 **CONGLOMERADO**, em conformidade com as melhores práticas de mercado e normas nacionais e internacionais.

3. PROCEDIMENTOS E CONTROLES DE VULNERABILIDADES

Tomando por base os objetivos de segurança cibernética do **CONGLOMERADO**, 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 **CONGLOMERADO**.

3.1. AUTENTICAÇÃO

Deve ser estabelecido 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.

3.2. CRIPTOGRAFIA

Deve ser estabelecido 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.

3.3. PREVENÇÃO E A DETECÇÃO DE INTRUSÃO

Serviços do **CONGLOMERADO** que são disponibilizados para a Internet requerem um controle para detecção e prevenção a intrusão. É mandatória a utilização de sistemas de detecção e prevenção de intrusão um serviço ou sistema é disponibilizado via internet.

3.4. PREVENÇÃO DE VAZAMENTO DE INFORMAÇÕES

A manipulação de informações classificadas como confidenciais deve ser monitorada por um sistema de Prevenção de Perda de Informações efetivo e adequado ao porte dos serviços e sistemas do **CONGLOMERADO**.

3.5. TESTES E VARREDURAS PARA DETECÇÃO DE VULNERABILIDADES

O **CONGLOMERADO** 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 **CONGLOMERADO** 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 **CONGLOMERADO**.

As vulnerabilidades identificadas devem ser remediadas de forma tempestiva.

3.6. PROTEÇÃO CONTRA SOFTWARES MALICIOSOS

O **CONGLOMERADO** 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 ser atualizado 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.

3.7. MECANISMOS DE RASTREABILIDADE

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

Os sistemas aplicativos do **CONGLOMERADO** 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.

3.8. CONTROLES DE ACESSO E DE SEGMENTAÇÃO DA REDE

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

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.

3.9. CÓPIAS DE SEGURANÇA

O **CONGLOMERADO** 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 **CONGLOMERADO** é a Análise de Impacto de Negócios, internamente denominado como BIA.

4. CLASSIFICAÇÃO DA INFORMAÇÃO

A informação é um importante ativo do **CONGLOMERADO** e deve ser preservado e salvaguardado, 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.

5. 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 o Plano de Resposta à Incidentes do **CONGLOMERADO**.

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 **CONGLOMERADO** também devem possuir procedimentos e controles voltados à prevenção e ao tratamento dos incidentes.

Na eventual ocorrência de incidentes relevantes e de interrupções de serviços relevantes que configurem situação de crise, o **CONGLOMERADO** 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.

O **CONGLOMERADO** 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.

6. 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 **CONGLOMERADO** deve elaborar cenários de teste de continuidade de negócios considerando de incidentes cibernéticos.

7. DISSEMINAÇÃO E TREINAMENTO

A política é disponibilizada para todos os funcionários e colaboradores do **CONGLOMERADO**. Como forma adicional de disseminação da política e conscientização sobre Segurança Cibernética, o **CONGLOMERADO** organiza eventos e comunicações internas reforçando a cultura de mitigação dos riscos associados à Segurança Cibernética.

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

8. RELATÓRIO

O **CONGLOMERADO** deve elaborar relatório anual referente à gestão das atividades relacionadas à segurança cibernética, este relatório deve ser submetido ao comitê de risco e apresentado à diretoria do **CONGLOMERADO**.

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

Serviços relevantes de processamento e armazenamento de dados e de computação em nuvem são aqueles que impactam diretamente as atividades "core" do **CONGLOMERADO**, 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 **CONGLOMERADO** deve adotar procedimentos que assegurem a devida gestão e monitoramento dos serviços prestados além de garantir a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço.

10. AUDITORIA INTERNA

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

11. APROVAÇÃO E REVISÃO

A diretoria do **CONGLOMERADO** 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.