POLÍTICA DE SEGURANÇA CIBERNÉTICA

ÍNDICE

1. FINALIDADE

A finalidade desse documento é formalizar a política para gestão da segurança cibernética. Estas diretrizes estão compatíveis com a natureza, o porte, a complexidade, a estrutura, o perfil de risco, modelo de negócios da instituição e a sensibilidade dos dados e das informações sob responsabilidade do Conglomerado.

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 a partir deste momento.

2. OBJETIVOS DE SEGURANÇA CIBERNÉTICA

A estrutura de segurança cibernética do BMB é composta por pessoas, sistemas e processos. Seu objetivo é a prevenção, detecção e redução de vulnerabilidades e impactos gerados pelos incidentes relacionados ao ambiente cibernético e que afetem a confidencialidade, a integridade e disponibilidade dos dados e dos sistemas de informação utilizados pelo BMB.

3. ABRANGÊNCIA

Esta política se aplica a todos os colaboradores, diretores executivos, gestores, empregados, aprendizes, estagiários, consultores, terceiros ou parceiros de negócios que que acessam e / ou processam às informações do BMB.

4. PROGRAMA DE SEGURANÇA CIBERNÉTICA

O grupo Daimler mantém um Programa de Segurança Cibernética projetado para garantir a confidencialidade, integridade e disponibilidade de sistemas de informação e informação. O Diretor Global de Segurança da Informação (CISO) é responsável pelo Programa de Segurança Cibernética. O Programa é gerenciado e apoiado pela equipe de segurança cibernética Global do grupo Daimler AG.

O Programa foi projetado para identificar, avaliar e proteger contra riscos internos e externos de segurança cibernética que possam ameaçar a segurança ou integridade dos sistemas de informação ou informação. O Programa baseia-se em avaliações de risco realizadas para identificar e avaliar os riscos internos e externos de segurança cibernética que podem ameaçar a segurança ou integridade das informações gerenciadas ou armazenadas pela Empresa. As avaliações de risco são realizadas com base nos processos de gestão de riscos da Daimler e nos padrões da indústria.

O Programa utiliza infraestrutura defensiva e implementação de políticas e procedimentos para proteger os sistemas de informação contra acesso não autorizado, uso ou atos mal-intencionados. O Programa foi projetado para detectar e responder a eventos de segurança cibernética identificados ou detectados para mitigar efeitos negativos.

O Programa inclui as principais funções de segurança cibernética conforme abaixo:

- Política e normas de segurança da informação e segurança cibernética
- Classificação e governança de informações
- Gerenciamento de riscos
- Gerenciamento de vulnerabilidades
- Gerenciamento de incidentes
- Educação e programa de conscientização
- Gestão de ativos e dispositivos
- Gestão de identidade e acesso
- Continuidade de negócios e recuperação de desastres
- Operações e segurança de sistemas
- Segurança de rede
- Sistemas e monitoramento de rede
- Desenvolvimento seguro de aplicativos
- Segurança física
- Gestão de fornecedores e provedores de serviços terceirizados

O Programa é baseado em padrões da indústria e melhores práticas. O Programa é revisado anualmente pela equipe DMO Global Cybersecurity e equipe Cybersecurity Local, o mesmo está disponível na Social Intranet.

5. PROCEDIMENTOS E CONTROLES DE SEGURANÇA CIBERNÉTICA

Para alcançar os objetivos de segurança cibernética, o BMB adota, no mínimo, os controles e diretrizes listados a seguir com base no Programa global de segurança cibernética listado acima, Daimler Corporate 'Information Security Policy' (A21) e Daimler Information Security Framework (DIS-F) disponíveis na Social Intranet. Estes controles devem ser aplicados nos ativos, na infraestrutura de TI, no desenvolvimento e ou contratação de sistemas de informação e na adoção de novas tecnologias pelo BMB.

A proteção dos ativos de informação é atingida pela implementação de um conjunto adequado de controles que precisam ser estabelecidos, monitorados, revisados e melhorados para assegurar que os objetivos específicos de segurança e do negócio da organização sejam atendidos.

5.1. RISK MANAGEMENT

O BMB definirá um processo de gerenciamento de risco de segurança da informação e adotará as diretrizes Globais do Daimler Information Security Framework (DIS-F/RISE) disponíveis na Social Intranet, para garantir que as opções apropriadas de tratamento de risco de segurança da informação sejam aplicadas. O Processo de Gestão de Riscos de Segurança da Informação deve ser integrado ao Sistema de Gestão de Riscos Corporativos. Os proprietários de risco são obrigados a tomar uma decisão sobre como os riscos identificados devem ser tratados. As seguintes opções são efetivamente aplicáveis: mitigação de riscos, transferência de riscos, prevenção de riscos ou aceitação de riscos.

5.2. TESTES E VARREDURAS E DETECÇÃO DE VULNERABILIDADES

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.

O BMB também deve executar anualmente ou a cada dois anos, por relevância, testes de intrusão em:

- Sistemas expostos nas Internet com existência de dados pessoais, executar anualmente.
- Sistemas expostos nas Internet sem existência de dados pessoais, executar a cada dois anos.

A remediação das vulnerabilidades identificadas nos testes acima deve seguir a recomendação de prazos estipulados pela DMO Global Cybersecurity no documento *"Remediation Timeline for Vulnerabilities"*. A gestão local deve assegurar que informações sobre vulnerabilidades técnicas dos sistemas de informação, em suas áreas de responsabilidade, sejam obtidas em tempo hábil. Para isso, devem ser utilizados os serviços de gestão de vulnerabilidades técnicas fornecidos pela DMO Global Cybersecurity. As áreas ligadas à segurança da informação devem assegurar redução adequada dos riscos identificados.

5.3. PREVENÇÃO E A DETECÇÃO DE INTRUSÃO

Serviços do BMB que são disponibilizados para a internet requerem um controle para detecção e prevenção à intrusão. É mandatória a utilização de sistemas de IDS/IPS (*Intrusion Detection/Prevention System*) em perímetro de borda da Internet quando necessária 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. As redes corporativas devem ser gerenciadas e controladas. A gestão global de redes deve gerenciar estas atividades para todas as redes corporativas.

5.4. CLASSIFICAÇÃO DA INFORMAÇÃO

A informação é um importante ativo do BMB e deve ser protegida em conformidade com as Políticas, diretrizes da Daimler e com as leis e regulamentos aplicáveis. Todas as informações devem ser devidamente classificadas e regidas de acordo com os requisitos especificados na regulamentação vigente. As informações serão classificadas considerando confidencialidade, integridade e disponibilidade.

Quanto à confidencialidade, as informações devem ser classificadas em um dos 4 níveis a seguir: publica, interna, confidencial ou secreta. Toda informação não classificada quanto à confidencialidade, será classificada como informação interna.

Quanto à disponibilidade, a informação deve ser definida em um dos seguintes níveis: disponibilidade padrão ou disponibilidade crítica. Toda informação não classificada quanto à disponibilidade, será considerada como sendo de disponibilidade padrão.

Quanto à integridade, a informação deve ser classificada em: integridade padrão e integridade crítica. Toda informação não classificada quanto à integridade, será classificada como sendo de integridade padrão.
Ativos de informação devem ser classificados para indicar a necessidade, prioridade e nível de proteção durante o ciclo de vida da informação. Isto inclui tanto os ativos de informações eletrônicas quanto não eletrônicas. Os ativos de informação devem ser rotulados com base na classificação atribuída à informação.

5.5. PROTEÇÃO CONTRA SOFTWARES MALICIOSOS

O BMB mantém proteção contra *malwares* e atualização das correções de segurança em todas as estações de trabalho e servidores. Deve ser atualizada conforme os padrões corporativos. É proibida a implementação de ativos na rede com sistemas obsoletos, sem suporte e atualizações das correções de segurança. As informações e instalações de processamento de informações devem ser protegidas contra *softwares* e *hardwares* maliciosos (*malwares*). Os controles de detecção, prevenção e recuperação para proteção contra *malware* devem ser implementados. Deve ser assegurada uma conscientização apropriada ao usuário.

5.6. MECANISMOS DE RASTREABILIDADE

O BMB mantém um gerenciamento de *logs* para garantir a governança, monitoramento, detecção e resposta a ações maliciosas. Os sistemas e aplicativos devem garantir um padrão mínimo de eventos e *logs* que permitam a rastreabilidade do acesso aos dados, considerando quem, quando, onde e quais operações foram realizadas.
Eventos relevantes devem ser gravados e evidências devem ser geradas de acordo com a legislação aplicável. Os registros de eventos devem ser gerados, mantidos e revisados. A instalações e informações dos registros devem ser protegidas. As atividades do administrador e do operador dos sistemas devem ser registradas. Estes registros devem ser protegidos, monitorados e regularmente revisados.

5.7. CONTROLES DE ACESSO E DE SEGMENTAÇÃO DA REDE

O BMB deve conhecer o nível de acesso à 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 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. A segregação das redes corporativas deve ser realizada baseada em análise de riscos e considerações de segurança.

5.8. CONTROLES DE ACESSO

O controle de acesso deve seguir as diretrizes listadas no documento "Política Corporativa de Controle de Acessos aos Sistemas" e Daimler Information Security Framework (DIS-F/RISE), disponíveis na Social Intranet e Compass, que estabelece os procedimentos a serem adotados na concessão, alteração, exclusão de acessos, além da revisão de perfis de acessos dos usuários nos sistemas do Conglomerado Financeiro, bem como estabelece um procedimento de registro desta revisão.

5.9. AUTENTICAÇÃO

Deve ser estabelecido um nível seguro de autenticação, baseado na classificação da informação e seguindo os controles de senhas fortes, utilização de dois fatores ou duas etapas quando possível, rastreabilidade e integração com uma base centralizada e segura de usuários, de acordo com as diretrizes globais Daimler Information Security Framework (DIS-F/RISE) estabelecidas no documento "Access Control (Password) Standard" disponível na Social Intranet.

5.10. CRIPTOGRAFIA

As regras para o uso de controles de criptografia para proteção de informações são desenvolvidas e implementadas com base no programa de segurança da informação global. Controles criptográficos serão utilizados para proteger a confidencialidade, autenticidade e integridade da informação.

Em todos os ambientes do BMB, quando aplicável, a utilização de chave de criptografia segura é mandatória para informações classificadas como confidenciais. A utilização de criptografia para informações classificadas como internas é mandatória somente em ambientes externos.

5.11. PREVENÇÃO DE VAZAMENTO DE INFORMAÇÕES

A manipulação de informações classificadas como confidenciais devem ser monitoradas de forma efetiva e adequada ao porte dos serviços e sistemas do BMB. Para tanto, o BMB (através da Área de Segurança comunica regularmente, bem como alerta e treina gestores e colaboradores, ressaltando a importância de resguardar informações pessoais e informação classificada como confidencial, buscando a redução de riscos de multas, despesas com processos e danos à sua imagem.

5.12. RESPOSTA A INCIDENTES

Será estabelecida uma abordagem para a gestão de incidentes de segurança da informação, incluindo a comunicação de eventos, falhas de segurança e definição de um comitê de crise. A segurança da informação global e a segurança corporativa devem governar o processo de gestão de incidentes de segurança, que deve ser integrado ao processo de gestão de crises corporativas. Os incidentes de segurança da informação devem ser documentados e tratados de acordo com o standard "Plano de Resposta a Incidentes de segurança da informação". A equipe de Cybersecurity Local e a DMO Global Cybersecurity devem definir e aplicar procedimentos para identificação, coleta, aquisição e preservação da informação, que podem servir como evidência.

Todos os funcionários, terceiros, temporários e prestadores do BMB que utilizem sistemas de informação da Daimler devem relatar qualquer problema observado ou suspeita de segurança da informação em sistemas ou servidores de acordo com o processo de gerenciamento de incidentes. O conhecimento obtido com a análise e resolução de incidentes de segurança da informação deve ser utilizado como lição aprendida, para reduzir a probabilidade ou o impacto de futuros incidentes.

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 controles voltados à prevenção e ao tratamento dos incidentes. Todos prestadores deverão notificar o BMB em caso de incidente em até 24 horas da detecção ou publicação do incidente. Os procedimentos e controles devem ser compatíveis com os utilizados pelo BMB em nível de complexidade, abrangência e precisão.

O BMB deverá compartilhar informações sobre os incidentes relevantes, incluindo aqueles provenientes de empresas prestadoras de serviços, com Banco Central do Brasil em até 72 horas da confirmação do incidente. Essas informações poderão ser compartilhadas junto aos 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 e canal indicado pelo Banco Central.

5.13. CÓPIAS DE SEGURANÇA

O BMB é responsável pelo processo de salvaguarda dos dados necessários para completa recuperação dos seus sistemas relevantes e para atender os requisitos operacionais e legais, garantindo a continuidade do negócio em caso de falhas ou incidentes e auxiliando em sua ágil recuperação. A base para definição de processos críticos do BMB é a Análise de Impacto de Negócios, o BIA.

5.14. CONTINUIDADE DE NEGÓCIOS

O BMB possui planos de continuidade operacional e contramedidas para após uma interrupção retomar os processos críticos dos negócios em tempo hábil. Para certificar que os planos estão adequados, um ciclo de teste de eventos críticos incluindo cenários de ataques cibernéticos e de melhoria continua desses planos deve ser estabelecido. 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.

6. ACESSO USO DA INTERNET e REDES SOCIAIS

Os requisitos de uso da Internet e redes sociais se aplicam à forma como os indivíduos cobertos se comportam on-line. O BMB reserva-se o direito de monitorar todas as atividades on-line realizadas dentro da rede BMB bem como em seus sistemas, softwares e ativos de TI.

Todos os funcionários, terceiros, temporários e prestadores do BMB não podem realizar as seguintes atividades, incluindo, mas não se limitando a:

- Acessar recursos de internet que contenham material obsceno, odioso, pornográfico, ilegal, violento ou ilegal, incluindo a violação de material direitos de propriedade intelectual.
- Acessar sites que BMB ou grupo Daimler determina que não serão permitidos.
- Enviar ou postar mensagens ou imagens discriminatórias, assediando ou ameaçadoras na Internet, nas mídias sociais ou através de sistemas de e-mail ou mensagens do BMB ou da Daimler.

As mídias sociais podem ser usadas por indivíduos cobertos para fins relacionados a negócios somente quando autorizadas pelo seu Gestor direto, área de TI e BMB Senior Management. Todos os funcionários, terceiros, temporários e prestadores do BMB não podem representar, comunicar, agir fora do escopo coberto de trabalho ou sugerir que suas opiniões são as do BMB sem previa autorização. Suponha que suas ações, comportamentos e comentários on-line estão contidos dentro de um fórum privado. A Internet é um domínio muito público e as mídias sociais devem ser usadas com julgamento e discrição como qualquer outro meio de comunicação.

7. DISSEMINAÇÃO E TREINAMENTO

Todos os funcionários e colaboradores do BMB têm fácil acesso às políticas e procedimentos, todos disponíveis no sistema "Compass" na Social Intranet, e devem aplicar as políticas de segurança da informação de acordo com os procedimentos estabelecidos. São ministrados treinamentos e atualizações regulares de políticas e procedimentos, de acordo com a relevância para a função do empregado. 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.

A política de segurança cibernética é divulgada para empresas prestadoras de serviço com linguagem clara e com o nível de detalhe e sensibilidade das informações compatíveis com as funções desempenhadas. Todos os contratados devem cumprir os requisitos de segurança da informação, de acordo com seu contrato.

8. RELATÓRIO

O BMB deve elaborar relatório anual sobre o programa de segurança cibernética, planos de ação e tratativa de incidentes relevantes com data-base de 31 de dezembro de cada ano. O relatório deve ser submetido ao comitê de risco para aprovação e apresentado à BMB Senior Management até 31 de março do ano seguinte ao da data-base.

9. GERENCIAMENTO DE FORNECEDORES

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, incluindo aqueles que prestam serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no País ou no exterior, deve seguir as diretrizes estabelecidas nos procedimentos internos vigentes no BMB. Requisitos de segurança da informação, para mitigar riscos associados ao acesso de terceiros a informações e instalações de processamento de informações da Daimler, devem ser acordados e documentados pelo responsável pelo terceiro, de forma juridicamente válida, sempre antes de qualquer liberação de acesso e seguindo as diretrizes DMO Cybersecurity no documento "Information Controls for Third Party", disponível na Social Intranet.

A gestão de entrega de serviços manterá um nível acordado de segurança da informação, previamente alinhado com o prestador. A entrega do serviço por terceiros deve ser regularmente monitorada e revisada com relação à segurança da informação. Os riscos de segurança da informação resultantes de mudanças na prestação de serviços devem ser monitorados e gerenciados pela área responsável.

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, até 10 dias após a

contratação. As alterações contratuais que impliquem modificação das informações já prestadas devem ser comunicadas ao Banco Central do Brasil, até 10 dias após a alteração contratual.

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 BMB. O departamento de Compliance e as áreas TI e Segurança cibernética devem prestar suporte.

11. RESPONSABILIDADES

A informação é um dos ativos mais importantes do BMB. As informações sobre clientes, parceiros de negócios, funcionários, projetos, finanças e processos são fundamentais para o sucesso da corporação. Isso é ainda mais verdadeiro, tendo em vista a importância estratégica da rede global e da crescente digitalização para o nosso negócio. No entanto, isso requer uma maior conscientização sobre os riscos ao lidar com informações dentro e especialmente fora do BMB e do Grupo Daimler (doravante" "Daimler"). Nossos clientes esperam que ofereçamos serviços seguros. Consequentemente, a proteção e a salvaguarda dessas informações não são apenas importantes para o nosso core business, mas também, em muitos casos, exigidas por lei; são também um componente fundamental da governação das sociedades na Daimler.

Todos os funcionários, terceiros, temporários e prestadores do BMB são responsáveis por garantir a segurança das informações que manipulam ou tem acesso. Todos são obrigados a apoiar as iniciativas de segurança da informação e cumprir os requisitos de segurança cibernética descritos nesse documento.

Cada gestor do BMB tem a responsabilidade de garantir a segurança da informação e cibernética dentro da área de sua competência. Além de assegurar um nível adequado de segurança da informação e cibernética também para os parceiros de negócios do BMB que têm acesso ou processa às informações do Banco e estão sob sua gestão.

12. CUMPRIMENTO E EXCEÇÕES

O não cumprimento da Política de Segurança Cibernética pode resultar em ações disciplinares, até e incluindo rescisão, e ação legal para violações das obrigações legais e regulamentares aplicáveis.
Todas as exceções devem ser formalmente solicitadas, aprovadas e documentadas e aprovadas pelo CIO, ISO, Compliance e BMB Senior Management.

13. VIGÊNCIA, APROVAÇÃO E REVISÃO

13.1. VIGÊNCIA, APROVAÇÃO E REVISÃO

Esta Política terá uma vigência indeterminada após a sua data de publicação, produzindo todos os seus efeitos a partir da mesma data.

13.2. APROVAÇÃO E REVISÃO

A diretoria do BMB é responsável pela aprovação desta política e suas subsequentes revisões, reforçando assim seu comprometimento com a melhoria contínua dos procedimentos relacionados com a segurança cibernética. Esta política deve ser revisada, no mínimo, anualmente.

Data aprovação e publicação: 17/12/2019
Data última atualização: 10/12/2020