SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PARA TERCEIROS

Esse documento contém versão em inglês a partir da página 10
This document contains English version from 10

1. OBJETIVO

Estabelecer diretrizes de Segurança da Informação a serem observadas por Terceiros.

Estabelecer diretrizes e práticas para garantir a proteção dos dados pessoais tratados por fornecedores e terceiros em nome da CBMM ou em conjunto, em conformidade com as legislações de proteção de dados aplicáveis e outras regulamentações pertinentes.

2. CAMPO DE APLICAÇÃO

Aplica-se a Terceiros, assim entendidos como todas as pessoas físicas e/ ou jurídicas que não sejam colaboradoras da CBMM, que executem atividades para a CBMM de forma remota e/ou presencialmente na planta e/ou escritórios da CBMM e que tenham acesso às informações ou sistemas de informação da CBMM. Aplica-se também a todos os fornecedores, parceiros, prestadores de serviços, consultores e qualquer outra entidade terceira que trate dados pessoais em nome da CBMM ou em colaboração com ela.

3. DEFINIÇÕES E SIGLAS

Ameaça: causa potencial de um incidente inesperado, que pode resultar em danos aos ativos de informação da CBMM.

Anonimização: técnica de processamento de dados que remove ou modifica informações que possam identificar uma pessoa. Essa técnica resulta em dados que não podem ser associados a nenhum indivíduo em específico.

Ativo: Algo que tenha valor para os negócios da CBMM e precise ser protegido.

Bases Legais: Hipóteses trazidas pela lei que autorizam a realização de atividades de tratamento de dados pessoais com finalidades especificas e devidamente informadas aos titulares de dados pessoais.

Controlador: Pessoa natural ou jurídica, de direito público e privado, a quem competem as decisões referente ao tratamento dos dados pessoais.

Dados Pessoais: Informações relacionadas a uma pessoa natural identificada ou identificável.

Dados sensíveis: Dados pessoais relacionados a origem racial, étnica, convicção religiosa, opinião política, filiação a sindicato ou qualquer organização

de caráter religioso, filosofo ou político, além de dados referentes à saúde, vida sexual, dados genéticos ou biométricos.

Encarregado de Proteção de Dados (DPO): Pessoa indicada pela CBMM para atuar como ponto de contato entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.

Incidente de Segurança da Informação: Ocorrência que pode causar danos à CBMM e impactar os ativos de informação da CBMM devido a perda de confidencialidade, disponibilidade e integridade.

ITSM: ferramenta de gestão de serviços de Tecnologia da Informação para abertura de chamados.

Malware: Qualquer tipo de programa indesejado, instalado sem o consentimento e que pode trazer danos aos ativos de informação da CBMM, como estações de trabalho, servidores, infraestrutura e rede.

MFA (Múltiplo fator de autenticação): método para atestar a identidade de alguém para concessão de acesso a informações, sistemas, aplicativos, entre outros.

Operador: Pessoa natural ou jurídica, de direito público e privado, que realiza o tratamento de dados pessoais em nome do controlador.

Risco: Combinação da probabilidade de ocorrência de algum evento e seus respectivos impactos.

ROPA: Registro das operações de tratamento de dados pessoais.

Terceiros: Todas as pessoas físicas e/ou jurídicas que não sejam colaboradoras da CBMM, que executem atividades para a CBMM de forma remota e/ou presencialmente na planta e/ou escritórios da CBMM e que tenham acesso às informações ou sistemas de informação da CBMM.

Titular dos Dados: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Transferência Internacional: transferência de dados para um país estrangeiro ou organismo internacional do qual o país seja membro.

Tratamento de Dados: Qualquer operação realizada com dados pessoais, como coleta, armazenamento, uso, processamento, compartilhamento ou eliminação.

Vulnerabilidade: Fragilidade de um ativo da CBMM que pode ser explorada e gerar danos à CBMM.

4. RESPONSABILIDADES E AUTORIDADES

4.1. Terceiros

- Seguir as diretrizes estabelecidas neste documento.

4.2. Gestor do contrato

- Garantir que o Terceiro cumpra as diretrizes aqui aplicadas;
- Esclarecer eventuais dúvidas dos Terceiros;
- Garantir o direcionamento e treinamento de orientações relacionadas às demandas operacionais referentes à prestação de serviço.

4.3. Segurança da Informação

- Definir boas práticas, bem como promover a atualização e manutenção de tais práticas;
- Monitorar, acompanhar e tratar os Incidentes de Segurança da Informação.

4.4. Governança de TI

- Garantir a atualização deste documento em conjunto com a área responsável.

4.5. Escritório de Privacidade

- Definir boas práticas de Privacidade e Proteção de Dados;
- Solucionar dúvidas de terceiros e parceiros através do canal disponibilizado neste documento.

5. DISPOSIÇÕES GERAIS

5.1. Introdução

A informação é um ativo estratégico para a CBMM e abrange três pilares básicos da Segurança da Informação:

- Confidencialidade: Informações devem ser disponibilizadas somente a pessoas autorizadas;
- Integridade: Informações não devem alteradas de forma indevida ou sem autorização;
- Disponibilidade: Informações devem estar acessíveis a qualquer momento, para uso legítimo das pessoas autorizadas.

5.2. Orientações Iniciais

Os Terceiros devem:

(i) Observar os princípios de Segurança da Informação aqui dispostos, cumprir as diretrizes estabelecidas neste documento e a documentação porventura associada.

(ii) Em caso de dúvidas relacionadas a este documento, buscar orientação de seus superiores, do Gestor do contrato e/ou da área de Segurança da Informação da CBMM.

(iii) Proteger as informações da CBMM contra qualquer acesso não autorizado, modificação, destruição ou disseminação, assegurando que os recursos tecnológicos sejam utilizados de maneira adequada.

(iv) Abster-se de utilizar qualquer informação da CBMM sem prévia autorização da CBMM.

(v) Endereçar questões relacionadas à privacidade e proteção de dados pessoais ao Escritório de Privacidade CBMM por meio do e-mail dpo@cbmm.com.

5.3. Monitoramento

- A CBMM poderá, por meio do seu time de Segurança da Informação, monitorar, inspecionar e registrar o uso da sua rede, sistemas e da internet, incluindo o acesso, recebimento e transmissão de informações, para fins de (i) garantir a integridade dos dados e das informações; (ii) auditoria; e (iii) identificação de possíveis ameaças cibernéticas.
- Os Terceiros devem respeitar o nível de acesso aos sistemas, redes, equipamentos, programas, softwares, arquivos informatizados, informações e instalações conforme que lhes for atribuído.

5.4. Segurança Física

- Os Terceiros devem respeitar as medidas de segurança para acessar as instalações da CBMM (quando aplicável).
- Os Terceiros poderão acessar áreas restritas somente em companhia de um colaborador responsável. Este colaborador será responsável por orientá-lo durante toda sua estada no ambiente restrito.
- É proibido:
- Qualquer tipo de gravação fotográfica, áudio ou vídeo das áreas internas sem autorização prévia da CBMM;
- Conectar qualquer dispositivo à rede corporativa ou qualquer outra rede disponível sem autorização prévia da equipe de TI (via chamado no portal ITSM).
- O Terceiro é responsável pelo crachá de identificação utilizado para acessar as dependências da CBMM. Em caso de perda, roubo ou extravio, o Terceiro deverá comunicar imediatamente a CBMM e o Gestor do contrato.

5.5. Cuidados com Credenciais

Os usuários devem empregar boas práticas de segurança da informação com relação às suas senhas;

- As senhas não devem ser anotadas em papel ou arquivos;
- O usuário e senha não podem ser distribuidos, divulgados, expostos ou compartilhados com outras pessoas por meio de qualquer canal, seja verbalmente, por escrito ou eletronicamente;
- O usuário e senha são pessoais e intransferíveis e devem ser devidamente protegidos;
- Os usuários deverão utilizar múltiplo fator de autenticação em todos os sistemas em que o recurso puder ser utilizado;
- As senhas não deverão conter dados pessoais, data de nascimento, endereço, time de futebol, entre outras informações do usuário;
- Senhas usadas para fins particulares não deverão ser utilizadas para fins corporativos;
- O comprometimento da senha é considerado um Incidente de Segurança da Informação. Se houver qualquer indicação de comprometimento da senha, o Terceiro deverá (i) alterar a senha imediatamente e (ii) reportar o incidente na ferramenta de ITSM.

5.6. Acesso Remoto

- Qualquer conexão feita para se acessar informações no ambiente CBMM deverá ser protegida. É mandatória a utilização de soluções de VPN, de Desktop virtual ou solução homologada pelo time de TI da CBMM;
- É mandatório o uso do múltiplo fator de autenticação sempre que possível.

5.7. Descarte e Armazenamento de Informações

O Terceiro deverá devolver ou descartar informações ou dados pessoais em sua posse ou sob seu controle nas seguintes situações:

- Se não for mais necessário para a finalidade proposta;
- Se não houver obrigação legal que demande o armazenamento;
- Após o término do contrato firmado com a CBMM.

Informações consideradas relevantes para a continuidade das operações deverão ser armazenadas em repositórios corporativos da CBMM.

5.8. Mesa Limpa e Tela Limpa

- Os Terceiros devem garantir que nenhuma informação confidencial seja acessada por pessoas não autorizadas;

- Caso o Terceiro não esteja na sua estação de trabalho, todos os documentos em papel assim como informações consideradas restritas e confidenciais devem ser guardados para impedir o acesso não autorizado;
- Antes de se ausentar da estação de trabalho, o Terceiro deve bloquear a tela do seu equipamento;
- Documentos contendo informações restritas ou confidenciais deverão ser removidos imediatamente das impressoras e copiadoras;
- Quadros brancos, flipcharts e outros devem ser apagados imediatamente após sua utilização.

5.9. Uso Aceitável de Recursos de Tecnologia

- A conta de e-mail CBMM deverá ser utilizada somente para fins corporativos;
- É vedada instalar ou inserir qualquer tipo de equipamento, programa, software ou arquivo informatizado sem a prévia autorização por escrito da CBMM, seja em equipamentos da CBMM, pessoais ou fornecidos pelas empresas contratadas da CBMM;
- O Terceiro deverá colaborar e cooperar proativamente com o time de Segurança da Informação CBMM em caso de suspeita de ou de efetivo Incidente de Segurança da Informação;
- É vedado o uso de equipamento, programa, software ou arquivo informatizado para fins pessoais, incluindo, mas não se limitando ao armazenado de informações de cunho pessoal.
- É vedado o uso de qualquer tipo de tecnologia utilizada para gravar ou transcrever informações relacionadas à CBMM ou sob sua responsabilidade sem aviso prévio e sem a devida autorização.

5.10. Privacidade e Proteção de Dados

5.10.1. Obrigações dos fornecedores e parceiros

Serão considerados como premissa a todos os fornecedores e parceiros CBMM quando do tratamento de dados pessoais:

- Adotar medidas técnicas e administrativas e de segurança das informações tratadas, de forma a proteger os dados contra acessos indevidos ou não autorizados de acordo com o contrato regente. Estas medidas podem incluir, mas não se limita a:
- Gestão e rastreabilidade de acessos as informações e dados;
- Uso de medidas técnicas para proteção dos dados pessoais (antivírus, criptografia, MFA (quando possível), entre outros);
- Planos de comunicação de incidentes relacionados a segurança das informações, incluindo requisitos de proteção de dados, conforme orientação da Autoridade Nacional de Proteção de Dados.
- Agir conforme as instruções da CBMM, jamais utilizando os dados tratados para fins e vantagens comerciais ou finalidades não previstas em contrato.

- Assegurar que as obrigações de sigilo, segurança da informação e proteção dos dados pessoais tratados se estendam aos colaboradores, contratados e subcontratados.
- Assumir integralmente a responsabilidade por quaisquer danos, sejam eles diretos ou indiretos, que resultem do tratamento inadequado dos dados pessoais de maneira irregular ou contrária ao estabelecido em contrato, devendo inclusive, ressarcir em caso de descumprimento.
- Cooperar com a CBMM para resolução de questões envolvendo a garantia de conformidade sob os dados tratados, respondendo os questionários e avaliações solicitadas e provendo documentação necessária para demonstrar o cumprimento das obrigações legais e as obrigações estabelecidas em contrato.
- Cooperar e prestar assistência a CBMM, dentro dos limites das obrigações impostas, em caso de atendimento a Autoridade Nacional de Proteção de Dados, ao titular, ou qualquer outra autoridade governamental, sobre questões relacionadas ao tratamento dos dados pessoais.
- Documentar os processos e manter o inventário (ROPA) atualizado de todas as operações de tratamento de dados pessoais realizadas, abrangendo também a indicação de transferências internacionais de dados pessoais eventualmente realizadas além da garantia e mecanismos adotados para proteção das informações.
- Efetuar somente o tratamento de dados pessoais minimamente necessários para atingir aos propósitos de negócio da CBMM, responsabilizando-se no caso de tratamento de dados pessoais realizados em desacordo com as leis e/ou com o contrato acordado.
- Garantir por meio de um canal formal, o contato do Encarregado de Proteção de Dados, autorizado a responder dúvidas e/ou consultas relacionadas ao tratamento de dados pessoais.
- Garantir que o tratamento de dados pessoais, especialmente dados pessoais sensíveis e/ou dados pessoais de crianças e adolescentes sejam realizados observando todos os princípios da lei, e conferindo as medidas de proteção adequadas e compatíveis com a sensibilidade dos dados.
- Garantir que nenhum dado pessoal decorrente da execução do contrato seja armazenado de forma descentralizada ou em dispositivos sem as devidas medidas de segurança adequadas. Equipamentos locais devem ser evitados, salvo somente se tiver sido implementadas técnicas de criptografia.
- Garantir que transferências internacionais de dados pessoais, quando aplicáveis, sejam realizadas única e exclusivamente com os serviços estabelecidos em contrato, observando todos os mecanismos previstos pela legislação de proteção de dados e demais leis aplicáveis.
- Prestar auxílio e/ou notificar assim que identificado (via e-mail dpo@cbmm.com) qualquer violação ou incidente de segurança da informação envolvendo os dados pessoais tratados, informando inclusive sobre as providencias adotadas para minimização de impactos em primeiro momento. Para este item favor observar as diretrizes disponíveis pela Autoridade Nacional de Proteção de Dados.

5.11. Violações das Diretrizes

As violações a estas diretrizes incluem, mas não se limitam a:

- Falta de reporte imediato nos casos em que a tal comunicação deva ser feita conforme estabelecido neste documento;
- Quaisquer ações ou omissões que tenham o potencial de acarretar perda financeira e/ou danos à imagem da CBMM;
- Uso dos dados, informações, equipamentos, programas, softwares, arquivos informatizados, sistemas ou outros recursos tecnológicos para propósitos ilícitos, incluindo mas não se limitando a violação de legislações, regulamentos internos, e ao Código de Ética e Conduta da CBMM disponível na intranet;
- Uso de softwares não licenciados e/ou equipamentos sem notas fiscais;
- Uso ou armazenamento indevido de dados bem como divulgação não autorizada de informações confidenciais, segredos comerciais ou outras informações, sem a autorização prévia e por escrito da CBMM.
- Deixar de observar os requisitos legais mínimos aplicáveis para a adequação dos processos relacionados ao tratamento de dados pessoais, conforme previsto na legislação;
- Disponibilizar, compartilhar ou transferir dados pessoais tratados à terceiros que não sejam contratados ou subcontratados (quando aplicável) e que não faça parte das atividades previstas em contrato;
- Utilizar de meios inadequados ou inseguros para transferir ou compartilhar os dados pessoais tratados;
- Tratar dados pessoais fora do escopo do contrato acordado ou após a extinção do contrato. O fornecedor deverá proceder com a exclusão definitiva ou implementar técnicas de anonimização quando possível, após o término do contrato ou quando solicitado pela CBMM, salvo exceções para retenção dos dados como fundamento legal ou obrigações legais.

5.12. Infrações

Em caso de descumprimento, a CBMM poderá adotar a seu critério todas as medidas legais e contratuais cabíveis.

5.13. Considerações Finais

Dúvidas relacionadas ao cumprimento deste documento deverão ser direcionadas ao time de Segurança da Informação da CBMM ou ao Gestor do contrato. O documento está sujeito a mudanças e atualizações que, assim que transmitidas ao Terceiro, deverão ser imediatamente observadas.
Em caso de dúvidas relacionadas as obrigações e responsabilidades enquanto agente de tratamento entre em contato conosco através do dpo@cbmm.com

6. ATUALIZAÇÕES

Este documento, juntamente com outros procedimentos complementares ou aplicáveis deverão ser revisados com periodicidade máxima de 02 (dois anos)

ou quando mudanças significativas que afetem as diretrizes ou gestão das medidas técnicas e administrativas se fizerem necessárias.

7. ANEXOS

Anexo 1 – Histórico das Revisões.

VERSÃO VERSION	ITEM	HISTÓRICO DA REVISÃO HISTORY OF REVISION	DATA DA REVISÃO REVIEW DATE
00	Todos *All*	Emissão inicial do documento em substituição ao PR-GSTI-29 versão 1.0 *Initial issuance of the document replacing PR-GSTI-29 version 1.0*	25.01.24 *01.25.24*
01	Todos *All*	Revisão geral e inclusão do item 5.10 *General review and inclusion of item 5.10*	29.08.24 *08.29.24*