Esse documento contém versão em inglês a partir da página 08
This document contains English version from 08

1. OBJETIVO

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

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.

3. DEFINIÇÕES E SIGLAS

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

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

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.

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

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.

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.

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 deste link.

5.3. Privacidade e Proteção de Dados

O tratamento de dados pessoais por terceiros em nome da CBMM ou em conjunto com a CBMM deverá ser feito de acordo as leis aplicáveis, o contrato firmado com a CBMM e as práticas aplicadas na CBMM.

5.4. 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.

5.5. 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.

5.6. 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.

5.7. 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.

5.8. 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.

5.9. 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.

5.10. 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.

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.
  A violação de qualquer das regras estabelecidas neste documento caracteriza Incidente de Segurança da Informação que será analisado pelo time de Segurança da Informação da CBMM, ficando o fornecedor responsável pelo Terceiro sujeito às penalidades previstas em contrato.

5.12. 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.

6. ANEXOS

Anexo 1 – Histórico das Revisões.

VERSÃO	ITEM	HISTÓRICO DA REVISÃO	DATA DA REVISÃO
00	Todos	Emissão inicial do documento em substituição ao PR-GSTI-29 versão 1.0.	25.01.24