POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
COMITÊ BRASILEIRO DO ESPORTE MASTER

1. OBJETIVOS

Estabelecer diretrizes que permitam aos Funcionários e Terceiros do Comitê Brasileiro do Esporte Master observarem os padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio, de proteção legal do CBEM e do indivíduo.

Nortear a definição de normas e procedimentos específicos de Segurança da Informação e orientar as condições de uso dos Recursos de TI, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações do CBEM quanto à:

- **Integridade**: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade**: garantia de que o acesso à informação seja obtido somente porpessoas autorizadas.
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso àinformação e aos ativos correspondentes sempre que necessário.

2. ÁREAS APLICÁVEIS

Este documento aplica-se ao Comitê Brasileiro do Esporte Master, com abrangência corporativa, considerando todos os Funcionários, (membros dos poderes, contratados e estagiários), Atletas, Patrocinadores, Visitantes e Técnicos.

3. DOCUMENTOS DE REFERÊNCIA

- Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018.
- ABNT NBR ISO/IEC 27001: 2006.

- ABNT NBR ISO/IEC 27002: 2005.
- Código de Conduta e Ética do CBEM.
- Manual de Conduta das Redes Sociais.
- PRO-GD-005: Procedimento de Gestão da Documentação.

4. GLOSSÁRIO/TERMINOLOGIA

- **Acesso Físico** – acesso à infraestrutura física da organização e seus diversos mecanismos decontrole como catracas, dispositivos de biometria e câmeras de segurança.
- **Acesso Lógico** – acesso à infraestrutura da organização, como sistemas operacionais, intranet, bancos de dados e seus diversos mecanismos de controle como login e tokens autenticadores.
- **Acesso Remoto** – conexão entre um dispositivo isolado (terminal ou microcomputador) a um outro computador que não está fisicamente conectado à rede privada do CBEM.
- **Backups** – cópia das informações físicas ou digitais para fins de segurança, análise ou restauração de dados.
- **Banco de Dados** - são coleções de dados interligados entre si e organizados para fornecer informações.
- **Confidencialidade**: princípio que diz que informação deve estar disponível somente a quemde direito ou com autorização para tal.
- **Continuidade do Negócio** – conjunto de práticas com o intuito de prevenir a interrupção das operações por meio do planejamento de alternativas de ação no caso de incidentes com probabilidade baixa de ocorrer, mas que podem causar danos graves à organização.
- **Dispositivos móveis** – equipamentos tecnológicos portáteis, tais como smartphones, tabletse notebooks.
- **Incidentes de segurança da informação** – acontecimentos não planejados relacionados àSegurança da Informação.
- **Integridade** – princípio de que a informação deve se manter integra.
- **Risco** – probabilidade de uma ameaça explorar uma vulnerabilidade existente.
- **Segurança da Informação** – conjunto de práticas com intuito de proteger as informações corporativas de utilização indevida. É suportada por três pilares: Confidencialidade, Integridade e Disponibilidade.
- **Sistema** – ferramenta digital que possui função complexa diretamente relacionada com o

negócio, tal como sistemas de gestão.

- **Software** – ferramenta digital que não possui função diretamente relacionada com o negócio, apenas o suporta, tal como Pacote Office, Windows, etc.
- **Usuário/funcionário** – é aquele que usa recursos disponibilizados pela área de TI, softwaresou hardwares, para desempenhar as suas funções no trabalho.
- **Vulnerabilidade** – fraqueza que pode ser explorada por uma ameaça caracterizando um incidente.
- **VPN**: Rede privada de virtual
- **TI**: Tecnologia da Informação
- **CBEM** – Comitê Brasileiro do Esporte Master
- **RH** – Recursos Humanos
- **TIC** – Tecnologia da Informação e Comunicação
- **Ambiente de homologação** – ambiente com as mesmas características de produção, onde os sistemas (alterações e etc) são testados, com o objetivo de garantir que está em conformidade com tudo o que se propõe a fazer.
- **Ambiente de produção** – ambiente controlado contendo os itens de configuração em produção usados para entregar serviços de TI para clientes.
- **Classificação da Informação** – define os níveis de classificação da informação e o tratamentomais adequado para cada nível.

5. DIRETRIZES / DESCRIÇÃO DO PROCESSO

5. 1 DIRETRIZES GERAIS

a) O conteúdo desta política é propriedade do CBEM e é destinado para uso e divulgação INTERNAe EXTERNA.

b) Em caso de dúvidas sobre a aplicação adequada das diretrizes constantes da presente política, os Funcionários devem consultar o seu gestor imediato, TI e/ou a área reponsável pelo *Compliance.*

c) O conteúdo desta política deve ser conhecido e observado por todos os Funcionários, Terceiros e demais que mantiverem ou venham a manter relacionamento com o CBEM, conforme aplicável, sendo o seu descumprimento passível de aplicação das medidas

legais edisciplinares no Código de Conduta e Ética do CBEM.

d) A aplicação das medidas legais e disciplinares mencionadas acima não isentam, dispensam ou atenuam a responsabilidade civil, administrativa e/ou criminal, pelos prejuízos resultantes deatos dolosos ou culposos resultantes da infração da legislação em vigor, desta política, normase procedimentos aplicáveis.

e) Esta política dá ciência a cada funcionário de que os ambientes, sistemas, computadores, tablets, e-mails, internet, redes do CBEM, pen drive (mídias), poderão ser monitorados e armazenados, conforme previsto na legislação brasileira.

f) Os casos omissos serão decididos pelo um colegiado formado por um representante de TI, Jurídico (LGPD), e da área responsável pelo *Compliance.*

g) Toda informação, confidencial ou não, é propriedade do CBEM, ressalvadas aquelas Informações Confidenciais de propriedade de Terceiros que sejam obtidas pelo CBEM através de um acordo de confidencialidade ou documento equivalente. São ativos corporativos valiosos que devem ser gerenciados com o devido cuidado.

h) Não é permitida o compartilhamento de informações do CBEM sem autorização expressa do Gestor Imediato e aprovação da área responsável pelo *Compliance.* Este processo deve ser formalizado e arquivado incluindo todas as interações e aprovações resultantes da solicitação.

i) Informações enviadas a Terceiros devem ser transportadas por portador autorizado e em envelope lacrado ou transmitidas de forma segura.

j) As informações Confidenciais devem estar sempre protegidas e guardadas evitando o acesso não autorizado a todo o momento. Também deverá ser dispensada atenção no momento daimpressão, envio e descarte das informações.

k) Quanto ao envio de Informações Confidenciais, quer seja por fax, e-mail ou outras mídias, é necessário ter certeza que o destinatário pode ter acesso às Informações.

l) Ao utilizar os meios de comunicação e ferramentas de trabalhos disponibilizados pelo CBEM, não espere que as informações enviadas ou recebidas sejam privadas. Sua atividade poderá ser monitorada e armazenada a fim de garantir que esses recursos sejam utilizados de formaadequada.

m) É responsabilidade de todos os Funcionários o descarte correto de mídias, devendo sempre utilizar fragmentador ou outro método para inutilizar o acesso as informações nelas contidas.

n) Os ativos de informação compartilhados devem ser utilizados de forma que outros funcionários não sejam afetados ou prejudicados nos critérios referentes à Confidencialidade,Integridade e Disponibilidade das suas informações. (Exemplo: acesso indevido, códigos maliciosos, quebra de sigilo, compartilhamento indevido de informações sensíveis e classificadas).

o) Em conformidade com a Lei Federal 13.709 de 2018, é automaticamente considerada como confidencial toda informação que envolva dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

p) Exceto para os fins previstos no artigo 7 da Lei Federal 13.709 de 2018, todas as informações relacionadas a pessoa natural identificada ou identificável devem ser automaticamenteconsideradas como restritas.

q) Serão criados normativos específicos para as solicitações de exclusão de dados pessoais do banco de dados do CBEM, conforme previsto pela Lei Federal 13.709 de 2018.

r) Observar as diretrizes, regulamentos e normas impostas pela Autoridade Nacional, prevista na Lei Federal 13.709 de 2018, quanto ao tratamento e proteção de dados pessoais, inclusiveaqueles históricos.

s) A transferência internacional de informações que contenham dados de pessoa natural deverão ser submetidos à prévia consulta do departamento jurídico do CBEM.

t) Quaisquer mudanças nos processos e rotinas do CBEM devem ser realizadas em conformidade com esta política e posteriormente devidamente divulgadas aos Funcionários e demais.

5.2 CLASSIFICAÇÃO E TRATAMENTO DAS INFORMAÇÕES

a) As informações devem ser classificadas quanto ao seu grau de sigilo e confidencialidade e nível de proteção no momento em que forem geradas, para garantir a devida confidencialidade. As informações devem ser classificadas de acordo com a Norma ABNT ISO/IEC 27001:2013 - Segurança da Informação, como: Pública, Uso Interno, Restrita, Confidencial.

- **Informação Pública**: são informações que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público. Nível de proteção: Público.

- **Informação Uso Interno**: são informações que não podem ser divulgadas para pessoas de fora da organização, mas que, caso isso aconteça, não causarão grandes prejuízos. Nível de proteção: Nível de proteção: NP-1.

- **Informação Restrita**: são informações estratégicas que devem estar disponíveis apenas para grupos restritos de funcionários. Podem ser protegidas, por exemplo, restringindo o acesso àuma pasta ou diretório da rede. Nível de proteção: NP-2.

- **Informação Confidencial**: são aquelas que, se divulgadas interna ou externamente, têm potencial para trazer grandes prejuízos financeiros, à imagem ou a estratégia a entidade. (o mais alto nível de confidencialidade). Nível de proteção: NP-3.

b) A classificação do grau de sigilo e confidencialidade das informações e o seu nível de proteção, devem ser feitas pelo gestor da área, assim como, a autorização de acesso as mesmas.

c) Os Normativos (políticas, procedimentos, normas) deverão ser classificados conforme o grau de sigilo e confidencialidade das informações. A área do Escritório de Projetos é o responsável pelo controle dos normativos, bem com, pela orientação e suporte na elaboração e/ou revisão desses documentos.

d) Os demais documentos produzidos pelo CBEM como: documentos financeiros, fiscais, processos de compras, prestação de contas que também deverão ser classificados conforme o grau de sigilo e confidencialidade das informações. A área que inclui em seu escopo a Gestão da Documentação é a responsável pelo controle, guarda e descarte desses documentos. A classificação do grau de sigilo e confidencialidade deverá ser acordada com os gestores das áreas assim como os prazos de guarda. Os prazos de guarda da documentação devem seguir a Tabela de Temporalidade de documentos do Conselho Nacional de Arquivos - CONARQ, Órgão do Arquivo Nacional, disponível no documento (PRO-GD-005: Gestão da Documentação).

e) Os e-mails corporativos também deverão ser classificados conforme o grau de sigilo e confidencialidade das informações pelo Colaborador. O gestor da área e o departamento TI sãoresponsáveis pela orientação e suporte.

f) Os e-mails corporativos devem ser enviados com a assinatura padrão disponibilizada pelo CBEM.

5.3 CONTROLE DE ACESSO

5.3.1 ACESSO FÍSICO

a) Todo funcionário, prestador de serviço, fornecedores, visitantes, devem estar devidamente identificados, utilizando identificação única, pessoal e intransferível, tal como crachá de forma visível, enquanto estiverem presentes nas dependências físicas do CBEM.

b) O crachá de identificação é de uso individual, não sendo autorizado o compartilhamento com outro funcionário ou terceiro, tampouco o seu uso fora das dependências do CBEM.

5.3.2 ACESSO RESTRITO AS ÁREAS

a) As áreas de negócios ou operações do CBEM devem, preferencialmente, controlar o acesso físico. Ficam estabelecidas as seguintes áreas de acesso controlado:

- Recursos Humanos;
- Contabilidade;
- Tesouraria;
- Centro de Processamento de Dados – CPD;
- TI;
- Jurídico;
- Diretoria e Presidência; e
- Planejamento e Controle Financeiro.

b) Caso não exista separação física para estes ambientes, torna-se ainda mais imprescindível tomar os devidos cuidados com o manuseio, transmissão oral e escrita de Informações Confidenciais.

c) Cabe ao Gestor tomar todos os cuidados para que aqueles que transitem pelo recinto sejam devidamente informados de que se trata de área com acesso restrito.

d) Somente funcionários de TI ou pessoas autorizadas pela Área podem ter acesso aos Centros de Processamento de Dados (CPD) do CBEM.

5.3.3 ACESSO LÓGICO

5.3.3.1 Usuários e Senhas

a) A identificação de acesso aos Recursos de TI deve ser efetuada através de uma senha, pessoal e intransferível, criada pelo próprio Usuário, mediante a observância de regras básicas que visem a garantir a segurança do acesso e da utilização dos recursos, sendo proibido o seu compartilhamento.

b) O usuário é responsável por zelar pela confidencialidade e sigilo de suas senhas e logins.

c) Ações realizadas com identificação e senhas do Usuário, como manuseio de dados em arquivos, planilhas eletrônicas e/ou sistemas, serão de inteira e exclusiva responsabilidade

doUsuário.

d) Para evitar o acesso indevido de outras pessoas aos Recursos de TI, o Usuário deve desligar o computador ou efetuar o bloqueio (CTRL + ALT + DEL + ENTER) sempre que se afastar do equipamento.

e) Os Usuários que utilizam Dispositivos Móveis deverão obrigatoriamente manter a senha de seus dispositivos habilitada e a Área de TI poderá utilizar ferramentas que assegurem isso.

f) O uso de dispositivos e/ou senhas de identificação de outra pessoa é terminantemente proibido e está sujeito às penalidades aplicáveis. Assim, nenhum dispositivo de identificaçãopoderá ser compartilhado, em nenhuma hipótese.

g) Mecanismos automáticos implantados pela Área de TI bloqueiam as contas de Usuários após tentativas de acesso com senha incorreta. Para solicitar o desbloqueio, busque orientações junto a Área de TI do CBEM.

h) Mecanismos automáticos implantados pela Área de TI asseguram a alteração periódica de senha dos Usuários, porém os usuários podem alterar a própria senha a qualquer momento que desejarem.

5.3.3.2 Acesso a Rede Interna

a) O acesso aos recursos tecnológicos por meio de conexões externas será permitido mediante solicitação formal, autorização específica e utilização de autenticação forte. Conexões de entrada e sistemas associados devem manter um nível de segurança igual ou superior ao dasredes acessadas internamente.

b) As conexões à rede corporativa serão permitidas somente a ativos que atendam no mínimo aos critérios de segurança definidos na norma pertinente. Conexões externas à rede corporativa só serão permitidas por meio de tecnologias disponibilizadas pela área de TI.

5.3.3.3 Acesso a Internet e Rede Wi-fi

a) A internet disponibilizada pelo CBEM deverá ser utilizada para fins profissionais. Essa regra se estende às três redes wi-fi disponibilizadas pelo CBEM: corporativa, dispositivos, visitantes. São aplicadas políticas de segurança para garantir a utilização adequada dessas redes.

- A rede corporativa é disponibilizada para os funcionários acessarem a internet e os recursos da rede interna através dos dispositivos móveis.
- A rede dispositivos é disponibilizada para os funcionários acessarem a internet através dos dispositivos móveis.
- A rede visitantes é disponibilizada o acesso dos visitantes a internet durante a permanência nas instalações do CBEM.

b) Os Funcionários não devem enviar e-mail contendo Informações Confidenciais para as suas contas de e-mail pessoais nem salvá-las em seus computadores pessoais ou outros dispositivos eletrônicos que não sejam do CBEM.

c) É proibido acessar, nos Dispositivos Móveis e demais ferramentas disponibilizadas pelo CBEM, as seguintes categorias de sites: apostas, propaganda, adultos, com material obsceno/ofensivo, atividades criminais/ilícitas, armas, violência, expressões de ódio, encontros, jogos, bate-papo (chat), sites que façam ou permitam controle remoto de computadores, hacking, fóruns, blogs, sites com transmissão de som e vídeo, que não sejampara fins profissionais, e outras que vierem a ser bloqueadas.

d) As regras mencionadas nesta política para uso dos Dispositivos Móveis devem ser respeitadas também quando utilizados fora do CBEM.

5.3.3.4 E-mail

a) O e-mail corporativo deverá ser utilizado exclusivamente para este fim. Sendo assim, não sãopermitidos envio de correntes, e-mails de despedida, com palavras de uso inapropriado e/oucom brincadeiras, entre outras sem fins corporativos.

b) Todos os assuntos de negócios devem ser conduzidos pelo sistema de correio eletrônico (e- mail) do CBEM e/ou por sistemas de mensagens homologados pela Área de TI. Não

devem ser utilizadas contas de e-mail pessoal, SMS, MMS ou qualquer serviço de mensagens instantâneas e sites de mídia social.

c) A área de TI fixará limites quanto ao tamanho das caixas postais, volume total de mensagens enviadas, quantidade de mensagens armazenadas nos servidores de e-mail, número de destinatários, tamanho e tipo de anexos e tamanho de cada mensagem enviada com a finalidade de garantir o bom funcionamento do serviço de acordo com os recursos disponibilizados, segurança e confidencialidade.

d) A qualquer momento que julgar necessário, a área de TI pode utilizar mecanismos para bloqueio, na entrada ou saída de mensagens, por tamanho, por anexos e download de arquivos que não sejam condizentes com as atividades do CBEM.

e) O usuário não deve abrir e-mails suspeitos ou de endereços de envio desconhecidos.

5.4 RECURSOS DE TI

5.4.1 RECURSOS DE TI INSTITUCIONAIS (CBEM)

a) Os recursos de TI fornecidos pelo CBEM(computadores, sistemas, internet) são utilizados pelos funcionários para a realização de atividades profissionais para as quais foram designados e são de propriedade do CBEM.

b) As permissões de acesso aos recursos de TI do CBEM devem ser baseadas nas necessidades denegócio, considerando-se o perfil funcional dos Usuários.

c) É responsabilidade de cada Gestor, a solicitação formal de liberação, alteração, suspensão ourevogação de acesso dos membros de sua equipe a qualquer recurso de TI.

d) É responsabilidade do RH, a solicitação formal de qualquer recurso de TI, para admissão de novos funcionários, afastamento e demissão, mudanças de áreas de atuação, função ou cargo, através da central de atendimento de TI.

e) A fim de haver um controle quanto aos privilégios de acesso dos Usuários, qualquer afastamento, seja temporário ou permanente, incluindo a mudança de área de atuação,

deverá ser informado, formalmente pelo RH, para que sejam tomadas as medidas cabíveis quanto ao cancelamento ou suspensão provisória e permissão do acesso.

f) Toda solicitação de acesso aos Recursos de TI deverá ser documentada formalmente e justificada quanto à sua real necessidade.

g) Cada gestor é responsável pela solicitação da liberação, alteração, suspensão ou revogação de acesso a qualquer recurso de TI para seus Terceiros contratados, em caso de: Contratação; Alteração do escopo dos serviços; Encerramento das atividades.

h) Os acessos concedidos a Terceiros deverão ter caráter provisório sendo obrigatório ao gestor responsável pelo mesmo indicar, no ato da solicitação, o prazo para utilização dos recursos.

i) Todo equipamento de TI deve ser homologado pela área de TI.

j) Apenas os funcionários de TI ou pessoas autorizadas pela Área podem realizar a instalação e/ou desinstalação, assim como a parametrização, de hardware dos equipamentos corporativos.

k) A utilização de equipamentos de tecnologia para a utilização fora do CBEM será permitida mediante autorização formal e deverá considerar os riscos pertinentes de sua utilização fora da infraestrutura de segurança do CBEM.

l) O Usuário é o responsável pela conservação, integridade, utilização e informações constantes nos Dispositivos Móveis que utiliza. Cuidados como desligar o computador, inclusive o monitor, ao final do dia e não manter líquidos próximo aos equipamentos são fundamentais para garantir que a vida útil dos mesmos não seja reduzida.

m) O Usuário para o qual for disponibilizado notebook e/ou celular corporativo deverá assinar o Termo de Responsabilidade específico para estes equipamentos.

n) Nenhum Usuário pode utilizar os recursos do CBEM para deliberadamente propagar

qualquer tipo de vírus, worm, spam ou programas de controle de outros computadores.

o) Nenhum Usuário pode utilizar os recursos do CBEM para fazer o download ou distribuição de software pirata. Assim como, não é permitido efetuar Upload de qualquer software licenciado ao CBEM ou de dados de propriedade deste ou de seus clientes, sem expressa autorização do gestor responsável pelo Software ou pelos dados.

p) A área de TI disponibilizará, através de dispositivos fornecidos pelo CBEM, acesso aos sistemase e-mails corporativos como uma facilidade aos Funcionários em deslocamento e como medida de contingência de acesso.

q) O Funcionário que utilizar qualquer tipo de Dispositivo Móvel próprio para acesso aos sistemas e e-mails corporativos do CBEM deverá observar esta política.

5.4.2 RECURSOS DE TI PARTICULAR

a) Os recursos de TIC particulares previamente autorizados a acessar os conteúdos fornecidos pelo CBEM devem ser protegidos com uso de métodos de bloqueios de acesso e ferramentas de segurança, como antivírus e firewall, a fim de mitigar os riscos de exposição da instituiçãoa ameaças.

b) Em uma eventual necessidade de acessar os recursos tecnológicos disponibilizados pelo CBEM, através de notebooks pessoais, deve ser utilizado os sistemas na versão web, não sendopermitido efetuar download dos arquivos do CBEM nos dispositivos pessoais e instalações locais dos sistemas, visto que nosso licenciamento contempla esse modelo de utilização e também os acessos ficam aderentes as questões de segurança implementadas.

c) Todo recurso de TIC particular trazido para as dependências do CBEM é de inteira responsabilidade de seu proprietário, incluindo os dados e softwares nele armazenados ou instalados.

d) O CBEM não tem responsabilidade por qualquer perda, furto ou avaria dos recursos de TIC particulares.

5.5 MÍDIAS SOCIAIS

É terminantemente proibido fazer, divulgar ou compartilhar comentários, mensagens ou discussões sobre o CBEM, seus clientes e informações referentes a qualquer estratégia, feitas através de redes sociais, salas de bate-papo, wikis, mundos virtuais e blogs (Mídias Sociais), a menos que expressamente autorizado pela Diretoria de Comunicação e Marketing. Para questões de condutas devem ser observados o Código de Conduta e Ética do CBEM e formulados os questionamentos às áreas responsáveis.

5.6 ARMAZENAMENTO DE INFORMAÇÕES

a) Todas as informações corporativas, devem ser armazenadas na rede de dados do CBEM, em seus respectivos diretórios.

b) Não deve ser mantida nenhuma Informação, arquivo ou dado corporativo em discos locais ou qualquer outro meio de armazenamento senão aqueles disponibilizados pela Área de TI.

5.7 BACKUP

O backup dos diretórios de rede é realizado diariamente pela área de TI através de processo automatizado, podendo ser utilizado serviços de terceiros para a salva guarda dos dados.

5.8 ANTIVÍRUS

Com o objetivo de proteger arquivos e informações eletrônicas do CBEM de vírus eletrônicos, a área de TI deve manter atualizada a ferramenta de controle de prevenção e detecção destes vírus, respeitando no mínimo a periodicidade recomendada pelo fabricante.

5.9 SISTEMAS DE INFORMAÇÃO

a) Cabe a área de TI homologar soluções técnicas e aos Usuários homologar as funcionalidadesdos sistemas.

b) As solicitações para desenvolvimento ou contratação de novos sistemas devem ser encaminhadas a área de TI, que deverá observar as melhores práticas de Segurança da Informação.

c) Os ambientes de homologação e produção são segregados, garantindo, assim, a integridade dos dados.

d) O CBEM deve, através de seus Gestores, estabelecer prazos e procedimentos para arquivamento e descarte de Informações, estabelecendo um ciclo de vida dos dados, cumprindo com os requisitos legais e regulamentares aos quais é submetida.

e) Todos os programas instalados são registrados e licenciados para a utilização corporativa, nãosendo permitido ao Usuário Final a instalação para utilização particular.

f) Não é permitido instalar qualquer tipo de software que não seja homologado e autorizado pelo Gestor responsável pela área de TI.

g) Não é permitido desativar ou mudar a configuração e/ou parametrização dos programas instalados nos equipamentos disponibilizados.

h) A reprodução não autorizada dos softwares instalados nos equipamentos disponibilizados constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

5. 10 ALTERAÇÃO MANUAL DE DADOS

a) Para segurança das informações registradas e armazenadas pelo CBEM, não será permitida a alteração de dados diretamente no banco de dados. Os dados imputados na interface dos sistemas estão armazenados de forma segura, consistente e privada para garantir sua proteção, evitando quebra de integridade e rastreabilidade das informações corporativas para fins de auditoria.

b) Caso a informação armazenada contenha erro em decorrência de falha humana ou tecnológica, que possa trazer prejuízo ao CBEM, deverão ser necessariamente observados os seguintes passos:

i. Verificação junto aos departamentos do CBEM da real necessidade de alteração da informação, e da possível remediação do erro de outras formas que não a alteração de

dados;

ii. Caso o problema não possa ser solucionado pelo passo descrito no item acima, abrir solicitação de TI justificando a necessidade de alteração, encaminhando para aprovação de seu diretor funcional, e posterior aprovação do Conselho Diretor;

iii. Após aprovação pelo Conselho Diretor, o departamento de TI da CBEM fará a alteração, anexando ao processo a justificativa técnica pertinente e a aprovação do Conselho Diretor.

5.11 GESTÃO DE VULNERABILIDADES TÉCNICAS

Cabe a área de TI, o monitoramento contínuo da segurança de dados e sistemas, através da identificação das fragilidades e vulnerabilidades da exposição de dados, que possam acarretar algum risco para o CBEM, bem como, elaborar e acompanhar os planos de respostas.

5.12 INCIDENTES DE SEGURANÇA INFORMAÇÃO

a) Todo o incidente que coloque em risco a Segurança da Informação, incluindo perda, furto ou roubo, deve ser reportado formalmente e imediatamente ao gestor da área responsável pela informação, ao gestor da área de TI e à área responsável pelo *Compliance* para avaliação da situação e adoção das medidas necessárias.

b) Todos os incidentes devem ser registrados formalmente para análise posterior. Tais registros de incidentes deverão ser utilizados como insumos para uma análise crítica e plano de ação, caso necessário, pela área de TI.

c) A adoção de medidas de ajuste relacionadas à Segurança da Informação que se fizerem necessárias em decorrência dos incidentes ocorridos será de responsabilidade do Gestor da área de TI, cabendo ao próprio operacionalizá-las mediante aprovação do Conselho Diretor das medidas e/ou investimentos necessários.

5.13 PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS PRINCIPAIS SISTEMAS E SERVIÇOS

A estrutura de tecnologia da informação possui mecanismos de contingência, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Estes mecanismos são detalhados através de documentos normativos, incluindo por meio de um plano de contingência.