MELHOR EDUCAÇÃO DO BRASIL
CONVENIADA

FGV | EDUCAÇÃO EXECUTIVA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ORIENTAÇÕES GERAIS E PROCESSOS

MELHOR EDUCAÇÃO DO BRASIL LTDA
CNPJ: 09.153.043/0001-81

SUMÁRIO

1. INTRODUÇÃO

01 A empresa tem como missão assegurar aos clientes, qualidade em suas prestações de serviço, A MEB zela por relações éticas, transparentes, coibindo a prática de toda forma de corrupção, fraude, suborno, favorecimento e extorsão.

02 Entende que a informação corporativa é um bem essencial para suas atividades e para resguardar a qualidade e garantia dos produtos ofertados a seus clientes.

03 Compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

04 Dessa forma, a empresa estabelece sua Política Geral de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

1.1 PROPÓSITO

01 Esta política tem por proposito estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores da empresa adotar padrões de comportamento seguro, adequados às metas e necessidades.

02 Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação.

03 Resguardar as informações da empresa, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;

04 Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus empregados, clientes e parceiros.

05 Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio como resultado de falhas de segurança.

Logo, o objetivo desta política é estabelecer as regras e orientações bases para a utilização segura e ética dos recursos tecnológicos da MEB, seguindo as normativas da Lei Geral de Proteção de Dados- LGPD (Lei nº 13.709/2018) , visando a proteção dos dados pessoais de sua base de clientes, colaboradores e demais envolvidos.

A politica aqui estabelecida deve ser cumprida por todos as partes envolvidas na atividades vinculadas a MEB. Sendo esse, um documento interno, com valor jurídico e aplicabilidade imediata e indistinta a todos os seus colaboradores e parceiros que venham a ter acesso a dados pessoais e /ou recursos tecnológicos da MEB.

2. CONCEITOS BÁSICOS

a. Ameaça: Causa potencial de um incidente, que pode vir a prejudicar a empresa.

b. Ativo: Tudo aquilo que possui valor para nós.

c. Ativo de informação: Patrimônio intangível da empresa, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal natureza, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a empresa por parceiros, clientes, empregados e terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da empresa ou por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

d. COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO – CGSI: Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria da empresa, que tem por finalidade tratar questões ligadas à Segurança da Informação.

e. Confidencialidade: Propriedade dos ativos da informação da empresa, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.

f. Controle: Medida de segurança adotada pela empresa para o tratamento de um risco específico.

g. Disponibilidade: Propriedade dos ativos da informação da empresa, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.

h. Incidente de segurança da informação: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da empresa.

i. Integridade: Propriedade dos ativos da informação da empresa, de serem exatos e completos.

j. Risco de segurança da informação: Efeito da incerteza sobre os objetivos de segurança da informação.

k. Segurança da informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações.

l. Usuário da informação: Empregados com vínculo empregatício de qualquer área da empresa ou terceiros alocados na prestação de serviços, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizados a utilizar manipular qualquer ativo de informação da empresa para o desempenho de suas atividades profissionais.

m. Vulnerabilidade: Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da empresa.

n.LGPD – Lei geral de proteção de dados pessoais: Lei geral de proteção de dados pessoais: Lei geral de proteção de dados pessoais: Lei de nº 13.709/2018 que “dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”

o. Criptografia: Criptografia: é a conversão de dados de um formato legível em um formato codificado. Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados.

3. SEGURANÇA DA INFORMAÇÃO

Nos tópicos abaixo serão definidos normas, procedimentos e boas praticas de segurança da informação da MEB

3.1. REGRAS DE SEGURANÇA DA INFORMAÇÃO

Todas as informações geradas, acessadas, manuseadas, armazenadas, compartilhadas ou descartadas no exercício das atividades realizadas pelos colaboradores e parceiros, são de propriedade e direito de uso exclusivo da MEB.

As partes envolvidas devem zelar para que as informações inseridas nos sistemas, ou quando enviadas ao cliente, sejam livres de erro, transparentes e verídicas.

O acesso e o uso das informações da MEB, incluindo o e-mail, devem estar limitados a jornada de trabalho ou período contratual do colaborador, exceto quando exercer atividade justificada ou plantões específicos devidamente controlados.

Quaisquer documentos produzidos pela MEB. não poderão sair da empresa sem que seja por meio de protocolo de envio de documentos.

Sendo necessária troca de informações com os clientes para cumprimento legal de obrigações, será necessário utilizar os canais oficiais disponibilizados pela empresa. Caso seja utilizado um canal distinto, será considerado um descumprimento das regras de segurança da informação e serão tomadas as medidas cabíveis quanto ao fato.

3.2. CONCESSÃO, REVOGAÇÃO E REVISÃO

As solicitações de acesso deverão ser realizadas pelo gestor do colaborador ao responsável de tecnologia via sistema de chamados com todas as informações do usuário cadastrado.

O responsável de tecnologia se reserva do direito de revalidar as permissões, ou não, caso a concessão tenha mais permissões do que o definido em politica interna para a efetiva para concessão.

Todos os acessos concedidos serão revisados, a cada 6 meses, a fim de garantir que continuam ativos e atualizados.

A revogação de acesso deve ocorrer mediante solicitação do gestor responsável pelo colaborador ou o parceiro ao responsável de tecnologia. no entanto , os direitos de acesso podem ser alterados e/ou revogados a qualquer tempo pela MEB, sem a necessidade de aviso prévio.

O acesso aos recursos tecnológicos será revogado imediatamente em caso de encerramento das atividades entre a MEb e as partes envolvidas. Portanto, assim que algum colaborador for demitido ou solicitar demissão, um parceiro tiver o contrato encerrado ou expirado, o esparavel de TI tomará as providencias necessárias. (ver situação dos alunos

3.3. USO DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

O colaborador deve utilizar apenas softwares e hardware previamente homologados ou autorizados pelo responsável de tecnologia da MEB.

A gestão de todos os recursos tecnológicos é de responsabilidade exclusiva do responsável de tecnologia da MEB.

Todo colaborador ou parceiro que se distanciar de sua estação de trabalho ou do dispositivo móvel, deve imediatamente realizar o processo de bloqueio do equipamento.

Os equipamentos disponibilizados aos colaboradores e parceiros são de propriedade da MEB, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da organização, bem como cumprir as recomendações e normas mencionadas neste documento.

As estações de trabalho e servidores contêm softwares de antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar imediatamente o responsável de TI.

Os colaboradores devem informar ao responsável de TI qualquer identificação de dispositivo estranho conectado ao seu computador.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução ou auxílio do responsável de TI.

3.4. PERMISSÕES DIFERENCIADAS

Alguns cargos ou funções, poderão ter permissões diferenciadas para o acesso e uso dos recursos tecnológicos, a fim de atender aos objetivos de negócio da MEB.

Excepcionalmente, poderão ser concedidas autorizações adicionais, temporárias ou não, aos demais colaboradores, desde que tal solicitação seja aprovada, justificada e necessária para a execução de determinadas tarefas ou projetos.

3.5. VEDAÇÕES

Quando da utilização dos recursos tecnológicos da MEB, o colaborador ou parceiro não deve:

a. Realizar qualquer tipo de manutenção ou reparo nos recursos tecnológicos corporativos, exceto o responsável de tecnologia ou terceiro autorizado pela MEB;

b. Utilizar programas que burlem os controles de segurança e controle impostos pela MEB ou por seus normativos;

c. Desinstalar ou desabilitar softwares instalados nos recursos tecnológicos pela MEB ou por alguém à sua ordem, independentemente do motivo;

f. Burlar quaisquer sistemas de segurança;

g. Acessar informações confidenciais sem explícita autorização do responsável;

h. Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes;

i. Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

j. Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

k. Hospedar, acessar e compartilhar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país.

l. Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

m. Realizar a transferência e/ou a divulgação de qualquer software, programa ou dados para terceiros, por qualquer meio de comunicação (físico ou digital), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

n. Armazenar arquivos pessoais e/ou não pertinentes ao negócio da MEB (fotos, músicas, vídeos etc.) para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores e acumular dados pessoais não necessário as atividades da MEB. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente, facultando a empresa em comunicar previamente o usuário.

o. A utilização de dispositivos removíveis de armazenamento de informações (pen drives, CDs, DVDs, HD Externos) para o transporte de informações. Em extremas necessidades e exceções é necessário acionar o responsável de TI para a avaliação do caso junto ao gestor responsável, se permitido, o dispositivo deverá conter tecnologia de criptografia. Todo o conteúdo transportado deve ser armazenado na rede corporativa e apagado do dispositivo imediatamente após a utilização;

p. O consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos;

q. O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato);

r. O acesso, armazenamento, utilização ou compartilhamento a conteúdo:

i. agressivo, ofensivo, difamatório, ridicularizante, calunioso, constrangedor, violento, abusivo, homofóbico, racista ou político;

ii. Que represente uma quebra de confidencialidade das informações da MEB ou de seus clientes;

iii. Caracterize assédio moral ou sexual, ou que incitem a prática de crimes ou contravenções penais;

iv. Constitua violação aos direitos de propriedade intelectual ou industrial da MEB, a exemplo dos bancos de dados, segredos de negócio, dados contábeis ou financeiros, ou de terceiros, incluindo a proteção de suas marcas e patente;

v. Que denote ou estimule a perseguição preconceituosa baseada em cor, sexo, raça, incapacidade física ou mental, condição social, origem, religião ou outras situações protegidas pelas leis brasileiras.

3.6. GESTÃO DE INFORMAÇÕES

O colaborador deve tratar como CONFIDENCIAL toda a informação que não estiver classificada, e comunicar ao gestor imediato, ate que se defina ou se tenha conhecimento da sua classificação adequada.

O tratamento de informação classificada como CONFIDENCIAL deve atender os seguintes requisitos:

a. Autorizar acesso apenas aos colaboradores e/ou parceiros previamente identificados;

b. Aplicar medidas de proteção lógica e física que garantam o acesso exclusivo pelos colaboradores e/ou parceiros autorizados;

c. Manter sigilo sobre o conteúdo ou informação para colaboradores e pessoas não autorizadas;

d. Por meios digitais, o compartilhamento deve ocorrer somente com autorização do gestor imediato e por meio dos recursos tecnológicos da MEB;

e. Em caso de compartilhamento de documentos por meio de dispositivos de armazenamentos móveis (pendrives, HDs externos, etc), a mídia deve conter aplicação de criptografia com nível de segurança compatível com o Advanced Encryption Standard (AES) ou superior;

f. Eliminar de maneira que impossibilite a posterior recuperação e o acesso à informação.

A necessidade de sigilo profissional permanece mesmo após o término das relações profissionais entre a MEB e o colaborador. Assim, é proibido o uso ou compartilhamento de qualquer informação obtida, recebida ou gerada em decorrência do relacionamento profissional. Informação classificada como CONFIDENCIAL não deve ser publicada na Internet ou nas mídias sociais.

Não é permitido realizar o upload (transmitir arquivos) ou compartilhamento de informação, pessoais ou CONFIDENCIAIS, da MEB ou de seus clientes para serviços e aplicativos de comunicação instantânea, de armazenamento na nuvem ou repositórios digitais, a exemplo, mas não se limitando a Whatsapp, SnapChat, Viber, Facebook Messenger, Telegram, Google Drive, OneDrive, Dropbox, iCloud, Box, SugarSync, Slideshare e Scribd, com exceção dos recursos tecnológicos disponibilizados e homologados pela MEB.

Informações confidenciais não devem ser discutidas, exibidas ou compartilhadas em ambientes públicos ou de livre acesso, onde pessoas alheias à MEB possam tomar conhecimento.

Além disso, as informações contidas em papeis ou outras formas de suporte de dados não podem ficar expostas em mesas de trabalho, impressoras, *scanners*, telas de computadores e nas salas de reunião, principalmente quando não estiverem sendo utilizadas.

3.7. ACESSO A INTERNET

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita à divulgação e auditoria. Portanto, a MEB, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os colaboradores e parceiros devem estar sempre atentos ao uso da Internet e utilizar somente sites confiáveis e com o conteúdo relacionado às atividades da MEB.

Da mesma forma, todo colaborador ou parceiro deve ter extrema atenção quando do recebimento de arquivos executáveis, telas para acesso automático, solicitação de informações cadastrais na Internet, promoções exageradamente vantajosas, e outras atividades suspeitas de *phishing*.

Não é permitido obter e/ou conceder acesso não autorizado, monitorar, interceptar, desativar, sobrecarregar, obstruir ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de examinar ou testar vulnerabilidades em sistemas internos ou externos à MEB.

A MEB autoriza o uso moderado da Internet desde que não prejudique a atenção do colaborador durante a execução das suas atividades e a qualidade no desempenho de suas funções.

Não é permitida a utilização dos recursos tecnológicos da MEB com fins de entretenimento, como por exemplo, acesso a blogs, fotologs, salas de bate-papo, comunicadores instantâneos ou mídias sociais, exceto se liberado previa e expressamente pela MEB.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da organização, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privados da rede, visando assegurar o cumprimento de sua política.

A MEB, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a organização cooperará ativamente com as autoridades competentes.

É proibida a divulgação e/ou o compartilhamento indevido de informações em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores e parceiros não poderão utilizar os recursos da MEB para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, ransonware, spam, assédio, perturbação ou programas de controle de outros computadores, neste caso, somente o responsável de TI tem permissão para acessar e utilizar programas de acesso remoto a outros computadores.

3.8. CORREIO ELETRÔNICO

Não é permitido o uso de correios eletrônicos particulares, a exemplo de Hotmail, Yahoo, Gmail, outros para o envio e recebimento de informações da/sobre a MEB e seus clientes.
O colaborador deve evitar que mensagens deixem de ser lidas ou fiquem sem resposta por mais de 24 horas em dias uteis.
O colaborador deve efetuar a limpeza de sua caixa postal corporativa periodicamente, com o fim de evitar problema de segurança e armazenamento, de modo a eliminar mensagens indesejáveis e que não tenham relações com o trabalho.
O colaborador deve verificar com atenção o endereço de correio eletrônico escolhido como destinado a fim de evitar mandar mensagem para pessoas erradas, ocasionando vazamento de informação da MEB, cliente e colaboradores. Caso isso venha a ocorrer, as seguintes providencias deverão ser tomadas:

a. Enviar imediatamente outra mensagem solicitando que a pessoa desconsidere a mensagem anterior e exclua, por conter conteúdo não destinado;

b. Comunicar o encarregado de dados da MEB, relatando o ocorrido.

É vedado ao colaborador/parceiro:
a. Enviar mensagem eletrônica para um número indeterminado ou excessivo de destinatários, exceto quando autorizado e desde que esteja relacionado às atividades contratadas pela MEB;

b. Divulgar o endereço de e-mail corporativo para fins de recebimento de mensagens pessoais ou de entidades alheias aos interesses ou às atividades prestadas à MEB;

c. Falsificar informações de endereçamento ou adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;

d. Apagar mensagens eletrônicas necessárias à MEB, sobretudo quando a MEB estiver sujeita a algum tipo de investigação, auditoria ou que possa ser prejudicada em procedimento judicial ou administrativo;

e. Encaminhar ou abrir mensagens consideradas suspeitas ou caracterizadas como corrente, SPAM e Phishing, sendo necessário a exclusão permanente (não deixar na lixeira);

f. Enviar mensagem com anexos contendo as seguintes extensões: .exe, .com, .bat, .pif, .js, .vbs, .hta, .scr, .cpl, .reg, .dll, .inf ou qualquer outro arquivo executável que represente um risco à segurança;

g. Veicular publicidade ou propaganda que caracterize concorrência desleal;

h. Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

i. Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou MEB ou suas unidades vulneráveis a ações civis ou criminais;

j. Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

k. Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da MEB ;

l. Enviar mensagem que vise obter acesso não autorizado a outro computador, servidor ou rede;

m. Enviar mensagem que vise acessar informações confidenciais sem explícita e devida autorização;

n. Enviar mensagem que tenha conteúdo considerado impróprio, obsceno ou ilegal;

o. Enviar mensagem que seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

p. Enviar mensagem que contenham perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;

q. Enviar mensagem que contenha fins políticos locais ou do país (propaganda política);

3.9. DISPOSITIVOS MOVEIS E ACESSO REMOTO

Todo colaborador que fizer uso de dispositivos moveis disponibilizados pela MEB, ou particulares, quando autorizados previamente e expressamente para finalidades profissionais, deve se atentar para as condições estabelecidas nessa politica.

Os equipamentos são restritos aos colaboradores previamente autorizados não sendo permitido o uso de dispositivos moveis disponibilizados para outros colaboradores ou terceiros não autorizados.

É vedado o uso de dispositivos moveis particulares para finalidades profissionais, exceto quando previamente autorizado.

Quaisquer danos eventualmente ocorridos no dispositivo móvel corporativo por má utilização do colaborador serão de sua responsabilidade, incluindo os custos decorrentes para a manutenção ou substituição do equipamento.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pelo responsável de tecnologia.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela organização constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É expressamente proibido a captura e divulgação de imagens pelos dispositivos móveis que contenham informações confidenciais, de clientes ou colaboradores.
Além disso, deverão ser adotadas todas as formas de segurança nas redes sociais e nos equipamentos (bloqueios de tela, confirmação em duas etapas, autenticação de dois fatores, etc)

3.10. BACKUP

O responsável de TI criará as definições e executará os procedimentos e manuais operacionais específicos, conforme as características das informações, dos sistemas e das ferramentas de geração de backup, devendo considerar as seguintes diretrizes:

a. O armazenamento seguro e ambientalmente adequado em instalações locais e remotas das mídias, incluindo a eventual geração de backups redundantes como suporte às estratégias de contingência operacional e de continuidade de negócios;

b. Utilização de criptografia e restrição de acesso ao material salvaguardado;

c. O transporte seguro das mídias que terão armazenamento remoto;

d. O descarte seguro de mídias e ferramentas de geração de backups obsoletos, depreciados e danificados, considerando a eliminação definitiva de seu conteúdo e, quando necessário, a destruição do suporte físico.

4. PROTEÇÃO DE DADOS

A MEB adota as seguintes ações para minimizar os riscos associados ao acesso indevido, perda ou destruição de informações durante e fora de seu expediente:

a) Manter a sua mesa organizada;

b) Ao se ausentar da mesa, guardar qualquer documento que possa conter dados pessoais ou estratégicos da MEB e de seus clientes;

c) Não deixar exposto informações estratégicas, dados pessoais e senhas em *postit's* ou papeis colados em sua mesa;

d) No final de expediente, recolher papeis e documentos da sua mesa, eliminando aqueles que não possuem mais uso.

e) não utilização de folhas de rascunho que possam conter dados pessoais.

Esta norma tem como objetivo definir ações que reduzam o risco de um incidente de segurança causado por documentos expostos nas instalações da MEB e de seus clientes.

5. PAPEIS E RESPONSABILIDADES

Abaixo serão elencadas as responsabilidades dos envolvidos na política da segurança da informação e proteção de dados da MEB:

Diretores, Diretores, sócios e ócios e ócios e gestores estores estores
a. Aprovar os normativos da MEB;
b. Orientar e acompanhar o estabelecimento e a observância dos controles estabelecidos, além de analisar as questões específicas apresentadas pelos colaboradores da MEB.

Responsável de Responsável de TI
a. Definir com as demais áreas da MEB os requisitos e controles adequados para a proteção das informações e recursos tecnológicos da MEB;
b. Avaliar periodicamente os sistemas e equipamentos, com o intuito de verificar o cumprimento dos normativos da MEB;
c. Implementar os controles de segurança previstos nesta norma para proteção das informações e dos recursos tecnológicos;
d. Manter os softwares de proteção instalados, ativos e atualizados;
e. Adquirir, de acordo com o orçamento da MEB, recursos tecnológicos quando autorizado pela Diretoria;
f. Tomar as medidas cabíveis em caso de perda, furto ou roubo de qualquer recurso tecnológico da MEB;
g. Proceder com a manutenção, instalação, análise, configuração ou remanejamento de quaisquer recursos tecnológicos da MEB;
h. Estabelecer mecanismos de identificação e autenticação de forma que possibilite a rastreabilidade das atividades do colaborador ou parceiro;
i. Fornecer a senha ao colaborador ou parceiro de forma segura, sigilosa e de maneira que a sua alteração seja exigida no primeiro acesso;
j. Auxiliar no processo de revisão de acessos concedidos;
k. Conceder, ajustar ou revogar o acesso do colaborador ou parceiro, quando solicitado formalmente ou em caso de encerramento das atividades;
l. Realizar e testar o backup das informações e recursos tecnológicos críticos para a MEB;
m. Realizar o monitoramento e manter o valor probatório dos registros para fins legais, preservando a confidencialidade, integridade, autenticidade, legalidade e disponibilidade das informações. ou de qualquer incidente de segurança da informação, sob pena de sua conduta ser considerada omissa, negligente ou conivente;

Colaboradores e parceiros e parceiros e parceiros

a. Cumprir e manter-se atualizado com relação a esta Política;
b. Utilizar de forma ética, segura e de acordo com a legislação nacional vigente todos os ativos corporativos, respeitando os direitos e as permissões de uso concedidas pela MEB;
c. Zelar para que todas as informações inseridas nos recursos tecnológicos da MEB, ou quando enviadas ao cliente, sejam necessárias, livres de erro, transparentes e verídicas;
d. Utilizar as informações e os recursos tecnológicos da MEB somente para finalidades profissionais e restritas as atividades contratadas;
e. Classificar e rotular todas as informações confidenciais no momento da sua criação ou recebimento;
f. Tratar a senha de forma individual, sigilosa e intransferível, não compartilhando ou divulgando a terceiros;

Encarregado de dados Encarregado de dados

a. Aceitar reclamações, comunicações e solicitações dos titulares de dados, prestar esclarecimentos e adotar providências;

b. Receber comunicações da autoridade nacional e adotar providências;

c. Orientar os colaboradores e os contratados da MEB a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

d. Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares referente a LGPD

e. Está definido que a senhora Daiane Patricia Messer responde como Encarregado de Dados (DPO) da MEB e o e-mail para contato é o daiane.fgv@mebbrasil.com.br

6. PROCESSO DISCIPLINAR

O colaborador que tomar atitudes antiéticas, ilícitas, não autorizadas ou contrárias ao recomendado pela MEB deverão ser consideradas violações por si só e estão sujeitas às sanções cabíveis, podendo variar desde advertência verbal ou escrita, até a rescisão do contrato por justa causa.

A tentativa de burlar às diretrizes e controles estabelecidos pela MEB deve ser desestimulada e, quando constatada, será tratada como violação às normas da empresa.

Atos de desonestidade, incontinência de conduta ou mau procedimento, negociação habitual por conta própria ou alheia sem permissão, concorrência desleal, desídia, embriaguez habitual ou em serviço, violação de segredo da empresa, indisciplina ou insubordinação, abandono de emprego, lesão contra a honra ou boa fama de qualquer pessoa ou ofensas físicas nas mesmas condições e prática de jogos de azar, enquadrados no art. 482 da Consolidação das Leis do Trabalho – CLT, ao ocorrerem serão punidos com demissão por justa causa, obedecendo os preceitos legais.

No caso de parceiros que prestam serviços a MEB, terão as rescisões contratuais solicitadas de forma forçada por descumprimento da política ora mencionada.

7. DISPOSIÇÕES FINAIS

Esta política encontra-se disponível na Escola e será enviada para todas as partes envolvidas nas atividades diárias da MEB, deverá estar disponível para os titulares de dados sempre que necessário, ou em caso de indisponibilidade, pode ser solicitada para o encarregado de dados da MEB.

Em caso de dúvidas, o colaborador ou parceiro pode solicitar os esclarecimentos necessários por meio do e-mail ao encarregado de dados da MEB.

Esta política deve ser revista e atualizada em intervalos não superiores a 2 (dois) anos, visando garantir que todos os requisitos de segurança técnicos e legais implementados estejam sendo cumpridos, atualizados e em conformidade com a legislação vigente no Brasil.