POLÍTICA DE CONSCIENTIZAÇÃO SOBRE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Esta Política de Segurança da Informação é uma declaração formal da empresa acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores, fornecedores, clientes e Parceiros.

I. OBJETIVO E APLICAÇÃO

O objetivo desta política é estabelecer as diretrizes a serem seguidas pelas partes envolvidas no que diz respeito à adoção de procedimentos, requisitos legais e práticas aplicadas, visando manter o alinhamento da Segurança da Informação com a estratégia organizacional e as recomendações dos Órgãos Reguladores, disseminando a importância e induzindo a melhoria contínua, promovendo a proteção das informações sensíveis, propondo normas para o processo de gestão da Segurança da Informação.

As diretrizes aqui estabelecidas devem ser seguidas por todos os colaboradores, prestadores de serviço, clientes e parceiros onde se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a todas as partes interessadas de que os documentos, ambientes, sistemas, computadores e redes da empresa podem ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de todos manter-se atualizado em relação a este documento, aos procedimentos e normas relacionadas

II. USO DOS SERVIÇOS DE INFRAESTRUTURA

A utilização de recursos de informática deve ser feita de forma a preservar a segurança e integridade das informações e, para tanto, o usuário tem ciência da presente política e se obriga a segui-la com todo o rigor.

O acesso ao recurso disponibilizado para o usuário é estritamente necessário e indispensável ao exercício de suas atividades.

A política de mesa limpa e tela limpa é um conjunto de práticas de segurança que visa proteger informações e dados pessoais. O objetivo é evitar o acesso não autorizado, perda, fraude ou danos a informações, tanto digitais como impressas.

a) Posto de Trabalho

É disponibilizado para cada profissional, um posto de trabalho, composto de equipamentos e softwares, para que este desempenhe suas funções. O usuário é responsável pelas informações armazenadas na sua estação de trabalho. Para isso deve seguir diretrizes e práticas de segurança de Informação para minimizar e evitar a exposição de informações consideradas sensíveis para a organização, clientes e parceiros.

- É terminantemente proibida a cópia de qualquer informação em mídia externa que não seja para uso exclusivo da empresa ou de seus clientes;

- Ao se ausentar de seu posto de trabalho, o usuário deve bloquear a sua sessão na estação de trabalho de forma a proteger as informações que estão sob seu poder;

- É terminantemente proibido ao usuário abrir, alterar ou trocar por conta própria a configuração e/ou os equipamentos de seu posto de trabalho;

- As estações de trabalho possuem ferramentas de proteção contra software malicioso e é dever do usuário mantê-lo atualizado, assim como as atualizações do sistema operacional. Deverão ser obedecidas as normas de estilo (papel de parede, tela de login, proteção de tela, cores e estilos) definidas, não podendo colocar fotos ou outras imagens que não sejam as determinadas pela (DTI);

- Os documentos impressos e mídias eletrônicas, quando não estiverem em uso, não devem estar expostos sobre a mesa e devem sempre ser mantidos em local seguro e reservado;

- Os documentos com Informações considerados Confidenciais, devem ser guardados em local restrito e com controle de acesso;

- Anotações, recados e lembretes não devem ser deixados amostra;

- Não anotar informações confidenciais em quadros brancos, Post-it, etc;

- Não guardar documentos restrito e confidencial em local de fácil acesso;

- Destruir os documentos impressos antes de jogar fora;

- Não imprimir documentos apenas para ler;

- Sempre fazer impressão segura. Todavia, quando não for possível, ao imprimir retirar odocumento imediatamente da impressora;

- Sempre que sair de frente do computador, manter a tela bloqueada;

- Manter na tela do computador (Área de trabalho) apenas os documentos que estãosendo utilizados;

- Manter qualquer tipo de caderno, agenda, bloco de notas e etc. Que for utilizado para anotações guardados emgaveta trancada;

- Durante o trabalho obrigatório o uso do crachá de identificação;

- Caso perder crachá ou cartão de acesso comunicar imediatamente;

- Desligar as estações de trabalho ao final do expediente, garantindo a desconexão de serviços de rede ou aplicações;

- Trancar o local de trabalho ao sair, de modo a não deixar o local de trabalho aberto sem que haja um profissional presente.

A informação é um grande patrimônio para a organização e, portanto, deve ser protegida por todos.

b) Equipamentos Pessoais e de Terceiros

Os equipamentos de uso pessoal, como *notebooks, tablets e smartphones*, devem ter o uso restrito às funções desempenhadas pelo profissional na empresa.

Na sede e filiais, a utilização de equipamentos não pertencentes à empresa deve ser pré-autorizada e seguir os padrões de segurança interna, sendo necessário identificá-los de forma diferenciada. É expressamente proibido conectar qualquer equipamento à rede de dados e telefonia, sem a prévia autorização.

A autorização deverá ser solicitada pelo superior imediato e liberada mediante registro de data limite da autorização, com respectiva justificativa. Caso a data limite de acesso do equipamento não seja informada, adota-se o prazo padrão de liberação por (24 horas).

c) Diretrizes quanto ao uso de Mídias Removíveis e da porta USB

Mídias removíveis são dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória, HDs portáteis, telefones celulares, entre outros.

A porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de informações corporativas confidenciais. Tal vulnerabilidade não pode ser contida com f*irewalls* já que os dispositivos são acoplados aos equipamentos pelos próprios funcionários da empresa.

Para minimizar os riscos de exposição e perda de dados sensíveis mantidos pela empresa e reduzir os riscos de proliferação de *malwares* nos computadores, a transferência de informações para dispositivos removíveis é bloqueada nos equipamentos da empresa.

A liberação das portas USB dos desktops e notebooks é feita somente se o uso for justificado e aprovado pelo superior imediato do solicitante. O dispositivo USB deve ser, preferencialmente, adquirido pela empresa, estar criptografado e protegido por senha.

Mesmo em equipamentos com o uso devidamente autorizado, o tráfego de dados entre as unidades USB e os computadores é monitorado através de relatórios providos pelo sistema de gerenciamento, auditorias internas e externas, e validações feitas pelo comitê de segurança da informação e *compliance.*

Sugere-se que, no ambiente da empresa se dê preferência ao armazenamento de dados nos diretórios da rede e repositório.

Os usuários de mídias removíveis nos equipamentos da empresa são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, cabendo a eles as punições citadas neste documento.

d) Correio Eletrônico Corporativo

O serviço de correio eletrônico corporativo (e-mail) permite que os profissionais possuam uma caixa postal de forma que possam enviar e receber mensagens internas e/ou externas, cientes de que as mesmas e seu conteúdo são de propriedade exclusiva da empresa.

Como forma de reduzir os riscos à segurança da informação, todos os e-mails são criptografados.

O profissional deve utilizar e divulgar seu endereço de e-mail corporativo exclusivamente para mensagens relacionadas às suas atividades na empresa, não devendo, em hipótese alguma, utilizá-lo para cadastros em sites de compras, relacionamentos, dentre outros.
Por se tratar de uma ferramenta de trabalho, as mensagens recebidas e/ou enviadas pelo profissional podem ser auditadas sem necessidade de conhecimento e/ou autorização prévia e, havendo constatação de uso inadequado poderão ser apagados de forma definitiva.

A caixa postal do e-mail corporativo do profissional é mantida em servidor da empresa, ocupando o espaço máximo a ele designado e poderá ser consultada a partir de sua estação de trabalho ou através do *webmail* em qualquer local que tenha acesso à internet, com cuidado para evitar armazenamento de assuntos ou informações desnecessárias e/ou irrelevantes, principalmente àquelas com arquivos anexos.

e) Compartilhamento de Arquivos

O servidor de arquivos permite ao profissional da empresa manter arquivos de uso comum em diretórios no servidor de rede, conforme as permissões (leitura e/ou gravação) estabelecidas para seu perfil.

Todas as pastas e arquivos com dados e documentos, sejam armazenados no servidor ou nas estações, estarão sujeitos à auditoria, sendo que aqueles de conteúdo considerado inadequado, quando não expressamente autorizados, poderão ser apagados de forma definitiva.

Em hipótese alguma a empresa se responsabilizará pela perda, corrupção ou uso indevido de informações e/ou dados particulares do usuário, eventualmente armazenados na sua estação de trabalho.

É proibida a utilização dos servidores para armazenamento de fotos, vídeos, músicas ou outros dados de caráter particular do usuário.

f) Impressão

As impressoras instaladas nas estações de trabalho dos profissionais da empresa são para uso exclusivamente relacionado às suas atividades.

Deverão ser tomadas precauções para que os documentos enviados à impressora geral não sejam lá esquecidos e fiquem acessíveis a outras pessoas.

As impressões poderão ser auditadas e controladas pelos responsáveis pela empresa.

g) Telefonia

O serviço de telefonia permite ao profissional da empresa efetuar ligações telefônicas para números fixos e celulares locais, DDD e DDI, conforme o nível de acesso autorizado.

Eventualmente, pode ser autorizada a disponibilização de linhas de telefonia celular para uso individual de um profissional ou Setor, dentro dos planos corporativos mantidos com as operadoras de telefonia.

Sendo o serviço de telefonia da empresa considerado essencialmente uma ferramenta de trabalho, em casos de suspeitas de ameaças à segurança, ou de qualquer tipo de fraude ou ainda desvio de conduta profissional, a empresa poderá, a critério da sua Diretoria, efetuar gravações dos ramais telefônicos, sem necessidade de aviso prévio ao usuário, sendo que o conteúdo dessas gravações será considerado sigiloso, não devendo ser divulgado externamente pela empresa, a menos que requisitado por decisão judicial.

h) Mensageiro Instantâneo

O uso de mensageiros instantâneos externos (Skype, WhatsAPPWeb, Google Hangout, ICQ) é permitido, desde que aprovado previamente pelo superior do solicitante.

A manutenção da lista de contatos nos mensageiros instantâneos será de exclusiva responsabilidade do usuário.

A utilização de mensageiros instantâneos deve ser exclusivamente para uso profissional, de acordo com as funções do profissional na empresa.

O download de arquivos nos mensageiros instantâneos será controlado, com eventuais limitações com relação ao tipo e tamanho de arquivo.

A utilização de mensageiros instantâneos poderá ser monitorada, independente de aviso ao usuário, de forma a detectar quaisquer abusos ou riscos à segurança da empresa, em função do uso indevido por parte do usuário.

i) Acesso à Internet

O serviço de acesso à internet permite que o usuário acesse sites da WEB em apoio às suas atividades na empresa. O acesso a sites de notícias, busca, bancários ou webmail, mesmo que para uso particular, são permitidos, desde que não atrapalhe a produtividade e o desempenho das atividades do profissional.

Por ser a internet primordialmente uma ferramenta de trabalho, todos os acessos são monitorados e registrados, podendo ser negados nos sites de conteúdo inadequado e/ou que tragam risco à segurança da empresa.

São expressamente proibidos acessos a sites constantes na lista negra dos sistemas de segurança da empresa ou que possam implicar em ações criminais tais como:

- Sites de conteúdo pornográfico;
- Sites de conteúdo racista;
- Sites que façam apologia ao uso de drogas e violência;
- Sites de jogos;
- Acesso a salas de bate-papo fora dos interesses da empresa;
- Comércio eletrônico fora dos interesses da empresa;
- Propaganda proposital de vírus eletrônico;
- Redes sociais.

Os downloads de arquivos suspeitos e/ou com extensões de multimídia que provoquem alto consumo de recursos de rede, são controlados e podem ser, eventualmente, bloqueados pelos responsáveis, caso não tenham sido previamente autorizados.

j) Uso de Software

Nas estações de trabalho da empresa estão instalados somente softwares homologados. A instalação de qualquer outro software deverá ser solicitada ao responsável.

É expressamente proibida a instalação, cópia ou distribuição de programas que sejam de propriedade da empresa para instalação em qualquer computador que não integre no seu patrimônio.

III. SEGURANÇA CORPORATIVA

a) Proteção da Informação

A informação pode estar presente em diversas formas, tais como: sistemas de informação, diretórios de rede, bancos de dados, mídia impressa, magnética ou ótica, dispositivos eletrônicos, equipamentos portáteis, microfilmes e até mesmo por meio da comunicação oral.

Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada.

O profissional que receber as informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso e, bem como, limitar seu acesso a terceiros, controlar quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma. Nenhuma das informações confidenciais pode ser repassada para terceiros sem o consentimento do remetente ou da área proprietária da informação.

O uso ou revelação indevida de uma informação confidencial deverá ser registrada prontamente num incidente de segurança da informação.

São exemplos de informações confidenciais:

- Informações de profissionais que devem ser protegidas por obrigatoriedade legal, incluindo dados cadastrais (CPF, RG etc.);
- Informações sobre produtos e serviços que revelem vantagens competitivas da empresa frente ao mercado;
- Todo o material estratégico da empresa (material impresso, armazenado em sistemas, em mensagens eletrônicas ou mesmo na forma de conhecimento de negócio da pessoa);
- Todos os tipos de senhas a sistemas, redes, estações de trabalho e outras informações utilizadas na autenticação de identidades. Estas informações são também pessoais e intransferíveis.

Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.

Ao usar uma impressora coletiva, o documento impresso deverá ser imediatamente recolhido.

Não devem ser discutidos ou comentados assuntos confidenciais em locais públicos, ou por meio de mensagens de texto. Observar também quando houver outras pessoas no ambiente de trabalho que não sejam pertencentes ao departamento.

b) Autenticação e Uso da Senha

O usuário é o único responsável pelo sigilo de sua senha, e, por conseguinte, por todas as informações que a mesma lhe proporciona, podendo alterá-la a qualquer momento

A senha de acesso ao e-mail é alterada diretamente no webmail e não é sincronizada automaticamente com a dos outros ambientes e sistemas.

Em hipótese alguma o usuário poderá divulgar e/ou compartilhar sua senha.

O acesso do usuário aos serviços de infraestrutura e/ou aos sistemas de informação poderá ser bloqueado ou cancelado nas seguintes situações:

- Rescisão ou término contratual do usuário com a empresa;
- Transferência de local de trabalho do usuário;
- O usuário não mais possuir a necessidade de utilização dos serviços de infraestrutura e/ou dos sistemas de informação;
- Após ter o acesso negado por consecutivas tentativas sem sucesso;
- Em caso de suspeita de violação ou ameaças à segurança;
- Por decisão da Diretoria da empresa.

Em caso de bloqueio, o desbloqueio de acesso deverá ser solicitado pelo usuário, com prévia autorização de seu superior,

c) Acesso Físico às dependências da empresa

A responsabilidade pela segurança física e pelo controle de acesso aos dados é compartilhada entre os administradores de TI, que incluem um dos sócios da empresa com acesso administrativo à nuvem *Azure* e a empresa terceirizada de suporte técnico VSOPME VIMAN, que aplica todas as regras de segurança necessárias e gerência os controles de acesso e segurança digital.

O prédio onde a Controladora está localizada a Controladora possui um controle rigoroso de acesso de pessoas, sendo todos os visitantes e funcionários devidamente registrados, com coleta de nome, documento e foto. Somente pessoas autorizadas podem entrar em áreas específicas do prédio. Câmeras de segurança monitoram todas as entradas e saídas do prédio, proporcionando uma camada adicional de vigilância e segurança ao local.

Os escritórios que processam ou acessam dados sensíveis são monitorados e acessados apenas por pessoas expressamente autorizadas pela Controladora, através de um sistema de controle de acesso que inclui a identificação prévia dos funcionários.

As áreas que contêm dispositivos críticos, como *switches de rede* e equipamentos de telecomunicações, são acessíveis somente por funcionários qualificados e previamente autorizados pela equipe de TI e pela empresa VSOPME VIMAN. Tais áreas são protegidas por fechaduras com controle de acesso eletrônico, que registram todas as entradas e saídas.

d) Descarte de mídia

O processo de eliminação da informação é tão ou mais importante que a sua geração ou armazenamento. Por isso, o descarte de mídias ou eliminação de conteúdos de informação sensível ou sigilosa deve atender aos seguintes procedimentos para o descarte seguro:

Com vistas a garantir a eliminação segura de mídias digitais e equipamentos tecnológicos, de forma a proteger informações confidenciais e garantir a conformidade com a legislação de proteção de dados, sejam eles de ex-funcionários, dispositivos obsoletos ou equipamentos com defeito, sejam higienizados e descartados de forma que os dados se tornem inutilizáveis e inacessíveis, conforme exigências da Lei Geral de Proteção de Dados (LGPD), a “MEDICINEBH” segue os seguintes procedimentos:

- Higienização de Dados: Antes que qualquer máquina de ex-funcionário seja descomissionada ou realocada, o equipamento é submetido a um processo de formatação completa do sistema operacional. Esse procedimento inclui a reinstalação e formatação total do sistema operacional Windows, seguindo o processo padrão de instalação/formatar o disco rígido da máquina. Esse processo garante que todos os dados outrora armazenados sejam sobrescritos, de forma que sejam permanentemente removidos e se tornem inacessíveis.

- Descarte Seguro de Discos Rígidos com Defeito: Os discos rígidos que apresentam defeitos e/ou por qualquer outra razão não puderem ser formatados, serão removidos dos equipamentos e submetidos a um processo de destruição física por perfuração. A perfuração é realizada em pontos estratégicos do disco, o que deforma permanentemente os pratos internos e, por consequência, impede qualquer tentativa de acesso aos dados outrora arquivados no dispositivo.

- Descarte Apropriado e Sustentável: Após a destruição por perfuração dos discos rígidos, os componentes físicos são enviados a empresas especializadas em reciclagem de eletrônicos certificadas, com o objetivo de promover o descarte ambientalmente correto de materiais eletrônicos. Isso garante que os materiais sejam processados em conformidade com as normas de sustentabilidade e proteção ambiental.

e) Registros de Incidentes de Segurança

Um incidente de segurança da informação é indicado por um ou mais eventos de que caracterizem violação ou não cumprimento de qualquer item desta política de segurança de informação.

Todos os incidentes de segurança detectados deverão ser relatados imediatamente ao DPO (*Data Protection Officer*), Carlos T. M. Bergamaschi (inscrito no CPF/MF sob o nº 389.439.608-32), cujas responsabilidades incluem a supervisão e desenvolvimento de políticas e procedimentos de privacidade, alinhados com as leis e regulamentações aplicáveis, sendo ele o responsável pelo contato primário para coordenar as respostas aos incidentes e assegurar que todas as ações necessárias sejam tomadas de forma adequada e em tempo hábil.

O Sr. Carlos T. M. Bergamaschi (DPO) é conhecido por todos os funcionários como o ponto de contato para o relato de eventos de segurança da informação. O contato dele é amplamente divulgado internamente por meio de comunicações oficiais e manuais de procedimento.

Os incidentes críticos devem ser relatados ao DPO e à equipe de segurança em um prazo máximo de 24 (vinte e quatro) horas após a detecção do problema. Incidentes menos críticos devem ser reportados ao DPO em até 48 (quarenta e oito) horas.

O contato oficial para que sejam relatados violações e eventos de segurança da informação é o e-mail: suporteti@morebr.com.br . Este e-mail é constantemente monitorado para garantir uma resposta rápida a qualquer incidente reportado.

Os procedimentos de escalonamento adotados pela Controladora incluem o encaminhamento dos incidentes para níveis hierárquicos superiores e especialistas técnicos da empresa terceirizada VSOPME VIMAN, que fornece suporte de TI e aplica as regras de segurança necessárias.

Todas as evidências relacionadas a incidentes de segurança são coletadas e mantidas de forma que a integridade dos dados seja preservada. Procedimentos de cadeia de custódia são aplicados para assegurar que as evidências sejam protegidas contra alterações ou acessos não autorizados durante a investigação.

De forma periódica, são realizados testes e simulações de resposta a incidentes, com uma frequência mínima de uma vez por semestre, de modo a garantir que a equipe seja eficiente e capacitada para lidar com diferentes tipos de incidentes e, bem como, para melhorar continuamente a eficácia dos procedimentos de resposta.