POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DADOS CORPORATIVOS

DA

ASSOCIAÇÃO BRASILEIRA DE DISTRIBUIÇÃO E LOGÍSTICA DE PRODUTOS FARMACÊUTICOS – ABRADILAN

09 de junho de 2021

ÍNDICE

1. OBJETIVO 3

2. ABRANGÊNCIA 3

3. CONSIDERAÇÕES GERAIS 3

4. TERMOS E DEFINIÇÕES 4

5. PRINCÍPIOS E DIRETRIZES 5

5.1. PRINCÍPIOS 5

5.2. CLASSIFICAÇÃO DA INFORMAÇÃO 5

5.3. - PAPEIS E RESPONSABILIDADES 6

6. REGRAS DE SEGURANÇA DENTRO E FORA DAS INSTALAÇÕES DA ABRADILAN 7

6.2. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO E INFORMAÇÕES EM MEIO FÍSICO 8

6.3. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO E DE INFORMAÇÕES EM MEIO ELETRÔNICO 10

9. VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PENALIDADES 22

10. CASOS OMISSOS 23

11. CANAL DE COMUNICAÇÃO 23

12. VIGÊNCIA E VALIDADE 23

1. OBJETIVO

A Política de Segurança da Informação e de Dados Corporativos é uma declaração formal da ASSOCIAÇÃO BRASILEIRA DE DISTRIBUIÇÃO E LOGÍSTICA DE PRODUTOS FARMACÊUTICOS, (doravante denominada "ABRADILAN"), acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, mantidas em meio físico ou eletrônico, garantindo requisitos básicos de autenticidade, confidencialidade, integridade e disponibilidade.

2. ABRANGÊNCIA

Esta política refere-se a todas as informações, dados e documentos, de propriedade da ABRADILAN e/ou sob sua guarda, mantidos em meio físico ou meio eletrônico (doravante "Informação" ou "Informações").

Esta política se aplica a todos os dirigentes, gestores, empregados independentemente de cargo ou função, estagiários, trainees, menores aprendizes da ABRADILAN, os seus sócios contribuintes, sócios colaboradores e respectivos representantes, os fornecedores de bens e serviços e todos os terceiros contratados da ABRADILAN que tiveram, têm ou terão acesso às Informações e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura da ABRADILAN (em conjunto denominados "Usuários").

3. CONSIDERAÇÕES GERAIS

Todos os tratamentos de dados e operações realizadas pela ABRADILAN devem:

- estar de acordo com a legislação vigente;
- respeitar os princípios éticos da ABRADILAN;
- observar as determinações das políticas, dos procedimentos e documentos societários da ABRADILAN;

Os Usuários devem respeitar e cumprir os requisitos previstos em políticas, bem como as normas internas de segurança e, quando aplicável, devem comunicar sobre descumprimentos por meio dos canais competentes.

4. TERMOS E DEFINIÇÕES

- *Backup*: é a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais.
- *Blog*: website para adição de grandes textos de informação.
- *Criptografia*: é um mecanismo com objetivo de impedir que informações trocadas na rede corporativa sejam lidas por pessoas indevidas.
- *File Share*: é um ambiente para armazenamento de arquivos na rede corporativa.
- *Firewall:* é um dispositivo utilizado em redes de computadores para segmentar e controlar os acessos entre redes internas e/ou externas.
- *LOG*: é o termo técnico para descrever o registro das transações que ocorrem quando um software é utilizado.
- Mídias Removíveis: dispositivos que permitem a leitura e gravação de dados, tais como: CD, DVD, *Pen Drive*, cartão de memória, entre outros.
- *Modem*: é um dispositivo sem fio, com saída USB para conexão em outro dispositivo tais como *Tablets* (com suporte 4G), *notebooks, netbooks, desktops*, etc., objetivando conexão com a internet.
- *Software*: é a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada através de *softwares*.
- *Softwares* de Mensageria: são softwares que permitem a troca de mensagem (textos, imagens, sons, arquivos, etc) entre mais de um usuário através da rede corporativa (exemplo: WhatsApp, Telegram, Gtalk, Teams, Skype, etc).
- TI: tecnologia da informação
- *Twitter*: webSite para adição de pequenos trechos de frases ou artigos.
- *USB:* é um tipo de conexão em computadores que permite a conexão de uma mídia removível ou periféricos (teclado, mouse, etc).

- VPN (*Virtual Private Network*): modalidade de acesso remoto à rede corporativa estando o computador fisicamente fora das instalações da corporação.

5. PRINCÍPIOS E DIRETRIZES

5.1. PRINCÍPIOS

A Política de Segurança da Informação e dos Dados Corporativos da ABRADILAN tem por base os seguintes princípios:

a) **Autenticidade:** garantia de que a Informação é proveniente da fonte identificada e que não foi objeto de mudanças ao longo do processo;

b) **Confidencialidade:** garantia de que a Informação é acessível somente a pessoas com acesso autorizado, conforme as políticas e regras definidas pela ABRADILAN;

c) **Disponibilidade:** garantia de que a Informação está sempre disponível para o uso legítimo e pelos Usuários autorizados pela ABRADILAN; e

d) **Integridade:** garantia da exatidão da informação e dos métodos de processamento.

Para assegurar esses princípios, a Informação deve ser adequadamente gerenciada, monitorada e protegida contra roubo, fraude, espionagem, perdas, vazamentos, ataques, e outros incidentes (doravante "Incidentes").

É fundamental para a proteção e salvaguarda das Informações que os Usuários adotem comportamento seguro, com respeito às regras definidas nesta Política.

5.2. CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do Comitê de Ética estabelecer critérios relativos ao nível de confidencialidade da Informação gerada e/ou mantida e/ou por qualquer modo acessada, de acordo com os critérios a seguir:

a) **Pública**: É uma Informação divulgada ao público em geral, de caráter informativo ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente.

b) **Interna**: É uma Informação que pode ser acessada sem restrições pelos Usuários, mas cujo acesso por parte de ex-Usuários e demais terceiros devem ser evitado.

c) **Confidencial**: É uma Informação cuja divulgação não autorizada pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à ABRADILAN. É sempre restrita a um grupo específico de pessoas, definido conforme as políticas e regras da ABRADILAN.

d) **Restrita**: É toda Informação que pode ser acessada somente por Usuários especificamente indicados pelo nome ou por área a que pertencem ou a que prestem serviços. A divulgação não autorizada dessa Informação pode causar sérios danos à ABRADILAN.

5.3. - PAPEIS E RESPONSABILIDADES

5.3.1 Comitê de Ética

É de responsabilidade do Comitê de Ética

a) analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;
b) garantir a disponibilidade dos recursos necessários para uma efetiva gestão de segurança da informação;
c) garantir que as atividades de segurança da informação sejam executadas em conformidade com esta Política de Segurança da Informação e de Dados Corporativos; e
d) promover a divulgação da Política de Segurança da Informação e de Dados Corporativos e tomar as medidas necessárias para disseminar a cultura de segurança da informação no ambiente da ABRADILAN.

5.3.2 Usuários

a) Declarar formalmente o conhecimento e o aceite integral das disposições da Política de Segurança da Informação e de Dados Corporativos, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento, assumindo a obrigação de cumprir a Política, bem como as demais normas e procedimentos de segurança aplicáveis;

b) responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido nesta Política; e

c) comunicar ao Comitê de Ética qualquer evento que viole esta Política ou coloque ou possa vir a colocar em risco a segurança das Informações.

6. REGRAS DE SEGURANÇA DENTRO E FORA DAS INSTALAÇÕES DA ABRADILAN

6.1. REGRAS GERAIS

Os Usuários devem observar as seguintes regras:

a) nunca comentar sobre as Informações que não sejam categorizadas como Públicas com familiares (cônjuges, companheiros, filhos, pais, avós, tios, sobrinhos e demais), namorados, amigos, ou qualquer terceiro;

b) nunca conversar ou comentar sobre informações que não sejam categorizadas como Públicas em locais em que a conversa possa ser ouvida por terceiros, a exemplo de elevadores, táxis, meios de transporte público, bares, restaurantes, aviões, saguões de aeroportos e hotéis, academias;

c) nunca acessar Informações que não sejam categorizadas como Públicas em locais nos quais a Informação possa ser vista por terceiros. Por exemplo, não ler documentos em papel, no computador, tablet ou celular, em aviões, mesas de restaurantes, etc;

e) nunca deixar Informações que não sejam categorizadas como Públicas em salas de reunião quando se ausentar ou em locais inseguros, a exemplo de veículos;

f) nunca deixar terceiros sozinhos nas instalações da ABRADILAN, exceto se forem prestadores de serviços devidamente autorizados;

g) a troca de informações que não sejam categorizadas como Públicas com terceiros somente pode ser feita após a assinatura de acordo de confidencialidade;

h) não é permitido gravar ou filmar reuniões presenciais ou remotas, conversas telefônicas ou por quaisquer outros meios ou equipamentos, realizadas com outros Usuários ou com terceiros, exceto com autorização expressa do Conselho Diretivo, o qual poderá definir políticas ou normas internas dispondo qual o conteúdo que poderá ser gravado, situações que dispensem a aprovação do Conselho Diretivo, a metodologia aceita de gravação, bem como os acessos e Usuários autorizados a gravarem e acessarem as gravações.

6.2. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO E INFORMAÇÕES EM MEIO FÍSICO

6.2.1. Diretrizes Gerais

As instalações de processamento e arquivamento das Informações devem ser mantidas em áreas seguras, cujo perímetro é fisicamente isolado contra o acesso não autorizado.

É resguardado à ABRADILAN o direito de monitorar suas instalações, mediante a utilização de sistema de circuito fechado de televisão (CFTV). As imagens obtidas serão armazenadas e protegidas conforme a legislação em vigor.

6.2.2. Acesso e permanência nas instalações da ABRADILAN

O acesso e permanência nas instalações da ABRADILAN só são permitidos mediante a autorização prévia e expressa da ABRADILAN.

O ingresso nas instalações da ABRADILAN será realizado mediante uso de chaves pessoais e intransferíveis, que serão fornecidas aos dirigentes, gestores e empregados da ABRADILAN (ora denominados "Detentores de Chaves"), mediante a assinatura do Termo de Recebimento e de Uso de Chave, devendo a chave ser devolvida na data do término do contrato de trabalho ou de serviços, ou imediatamente, assim que o dirigente ou gestor não mais exercer as suas funções na ABRADILAN.

É expressamente vedado aos Detentores de Chaves copiar, moldar, fotografar ou de qualquer forma mapear ou gravar as chaves pessoais e intransferíveis recebidas. As chaves são pessoais e intransferíveis, não sendo permitido o seu compartilhamento.

A ABRADILAN deverá ser imediatamente informado em caso de extravio ou de qualquer incidente que comprometa a integridade ou a singularidade da chave confiada aos Detentores de Chaves.

Caso seja necessário o acesso e/ou permanência de terceiros nas instalações da ABRADILAN em horário fora do horário comercial, será feita a entrega de chave ao terceiro, condicionada à assinatura do Termo de Recebimento e de Uso de Chave pelo terceiro e à autorização prévia e expressa da ABRADILAN, devendo a chave ser devolvida imediatamente pelo terceiro sempre que ele se ausentar das instalações da ABRADILAN, ou quando for revogada a aprovação da ABRADILAN, ou cessar a finalidade para a qual a Chave foi disponibilizada.

6.2.3. Manuseio, guarda, descarte de Informações em papel

As Informações classificadas como internas, ou confidenciais, ou restritas, não deverão ser manuseadas em lugares públicos e não deverão ser deixadas expostas em qualquer lugar, ou mantidas em lugares inseguros, a exemplo de veículos. Imediatamente após o seu manuseio, o Usuário deve mantê-las guardadas em locais seguros e com acesso restrito ou descartá-las, sempre de acordo com as políticas e procedimentos determinados pela ABRADILAN.

As Informações classificadas como internas, ou confidenciais, ou restritas, quando não mais necessárias, devem ser descartadas mediante trituração/fragmentação. Sempre que encerrar uma reunião, o Usuário deverá apagar eventuais quadros/lousas utilizados e verificar se todas os eventuais documentos

e papeis utilizados estão sendo retirados do local para guarda ou destruição conforme as políticas e procedimentos determinados pelo ABRADILAN.

6.2.4 Utilização de equipamentos fotográficos, filmadoras e/ou reprodutores de imagem e voz. Divulgação de fotos, áudios ou vídeos

É proibida a realização de filmagens, de registros fotográficos ou registros de áudio, nas instalações da ABRADILAN e, fora dela, de equipamentos, hardwares, softwares, documentos ou informações não consideradas como Públicas de propriedade da ABRADILAN, ou aos quais o Usuário obteve acesso em razão de seu vínculo (qualquer que seja) com a ABRADILAN, sem a prévia e expressa autorização da ABRADILAN.

A utilização de equipamentos fotográficos, filmadoras e/ou reprodutores de imagem e voz, incluindo telefones celulares com dispositivo de câmeras, quando intencionalmente usado para tirar fotografias nas unidades da ABRADILAN, deve ser previamente autorizada pelo Comitê de Ética.

Não é permitido realizar backup, extrair documentos ou informações – ainda que consideradas Públicas –, alterar hardwares ou softwares de equipamentos da ABRADILAN, bem como não são permitidas capturas de telas ou fotos nas quais sejam expostos equipamentos, documentos ou informações não consideradas Públicas da ABRADILAN, salvo com autorização prévia e expressa do Comitê de Ética.

É proibida a divulgação de fotos, áudios ou vídeos dos Usuários e/ou das instalações, equipamentos, hardwares, softwares, documentos ou informações da ABRADILAN em comunidades eletrônicas (Blogs, Facebook, WhatsApp, Internet, etc), salvo com autorização prévia e expressa do Comitê de Ética.

6.3. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO E DE INFORMAÇÕES EM MEIO ELETRÔNICO

6.3.1 Diretrizes Gerais

As Informações e os sistemas de informação da ABRADILAN devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a sua integridade, sigilo e disponibilidade.

Todo acesso às Informações em meio eletrônico e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado.

6.3.2 Diretrizes relativas a Sistemas/Softwares

Os Usuários devem observar as seguintes regras:

a) apenas pessoal autorizado da ABRADILAN pode instalar softwares nos equipamentos fixos ou portáteis fornecidos pela ABRADILAN. Em caso de dúvidas, Usuário deverá consultar pessoa autorizada pela ABRADILAN para instalação de softwares;

b) não executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços;

c) não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de terceiros não autorizados ou comprometer a confiabilidade e integridade da rede corporativa da ABRADILAN; e

d) não enviar Informações confidenciais ou restritas para e-mails externos sem proteção. O arquivo deve contar com a proteção de criptografia ou uma senha “robusta”;

O pessoal expressa e previamente autorizado pela ABRADILAN deverá estabelecer os aspectos de controle, distribuição e instalação de softwares utilizados.

Qualquer *software* que, por necessidade do serviço, necessitar ser instalado, deverá ser solicitado ao pessoal autorizado pela ABRADILAN, que analisará a solicitação e homologará o software, para posterior disponibilização ao requerente.

A ABRADILAN proíbe e monitora o eventual uso indevido de programas não licenciados. Dessa forma, apenas *softwares* licenciados pela ABRADILAN poderão ser instalados.

O pessoal expressa e previamente autorizado pela ABRADILAN desinstalará, sem aviso prévio, todo e qualquer software sem licença de uso eventual e inadvertidamente instalado em equipamentos da ABRADILAN.

Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas a Usuários e para processos autorizados. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado.

A documentação dos sistemas deve ser mantida atualizada. A cópia de segurança deve ser testada regularmente por amostragem e mantida atualizada.

6.3.3 Diretrizes relativas a Máquinas - Estação de Trabalho

Os equipamentos fixos (*desktops*) ou portáteis (*notebooks*) de trabalho (doravante "Estações de Trabalho") devem ser protegidos contra danos ou perdas, bem como ao acesso, uso ou exposição indevidos.

Tudo o que for executado na Estação de Trabalho é de responsabilidade do Usuário que a utiliza. Cada Estação de Trabalho possui códigos internos, os quais permitem que ela seja identificada na rede. As Estações de trabalho são monitoradas e verificadas para fins de auditoria.

O acesso à Estação de Trabalho é feito mediante a utilização de login definido por pessoal expressa e previamente autorizado pela ABRADILAN e de senha, definida pelo Usuário, conforme previsto nesta Política. O acesso à Estação de Trabalho deverá ser encerrado no final do expediente, mediante o desligamento do equipamento.

Quando se ausentar do seu local de trabalho, o Usuário deverá bloquear a Estação de Trabalho com senha.

Não é permitido o acesso à rede corporativa da ABRADILAN ou a circulação de Informações por equipamentos (computadores, celulares, tablets) que não sejam de propriedade da ABRADILAN.

Apenas o pessoal expressa e previamente autorizado pela é autorizado a fazer movimentações de equipamentos de informática e telefonia (*hardwares*) nas instalações da ABRADILAN.

Não é permitido o armazenamento de arquivos particulares (músicas, filmes, fotos, etc) nas Estações de trabalho. Esses arquivos serão excluídos por pessoal expressa e previamente autorizado pela ABRADILAN sem aviso prévio.

6.3.3.1 Boas práticas de segurança para dispositivos móveis (Notebooks, celulares e tablets)

Evite utilizar o *notebook* em locais públicos.

Quando em deslocamentos de carro, coloque o notebook no porta-malas ou em local não visível.

Ao movimentar-se com o notebook, se possível, não utilize malas convencionais para notebook e sim mochilas ou malas discretas.

Não coloque o *notebook* em carrinhos de aeroportos, nem o despache como bagagem.

Em locais públicos (recepção de hotéis, restaurantes e aeroportos, dentre outros), mantenha o notebook próximo e sempre à vista, não se distanciando do equipamento.

Nos hotéis, sempre que possível, guarde o *notebook* no cofre do seu apartamento.

Avalie se em pequenas viagens é realmente necessário levar o *notebook*.

Utilize sempre o bloqueio de tela com senha nos equipamentos.

Se possível, utilize a opção de criptografia para cartões SD utilizados em tablets e celulares.

Não conecte os dispositivos em redes Wi-Fi desconhecidas ou redes públicas, porque essas redes podem conter mecanismos para captura de dados do seu dispositivo.

6.3.4 Utilização de equipamentos particulares / terceiros nas instalações da ABRADILAN

Computadores particulares não podem ser utilizados nas instalações da ABRADILAN e/ou para acesso à rede corporativa da ABRADILAN, exceto após a prévia aprovação por escrito de pessoal expressa e previamente autorizado pela ABRADILAN.

É de responsabilidade do gestor do contrato incluir no contrato de terceiros/prestadores de serviço cláusula declarando a responsabilidade do terceiro/prestador de serviços sobre todo e qualquer *software* instalado nos seus equipamentos.

É de responsabilidade do gestor do contrato requerer ao pessoal expressa e previamente autorizado pela ABRADILAN os acessos dos terceiros contratados à rede corporativa da ABRADILAN, indicando os acessos necessários, com base nas políticas e regras definidas pela ABRADILAN.

6.3.5 Boas práticas de segurança para Impressões

O uso de equipamentos de impressão e reprografia deve ser feito exclusivamente para a impressão/reprodução de documentos que sejam de interesse da ABRADILAN ou que estejam relacionados com o desempenho das atividades profissionais do Usuário.

Documentos enviados para a impressão deverão ser retirados imediatamente das impressoras pelos responsáveis após à sua impressão.

É proibido o reaproveitamento de páginas já impressas. Elas devem ser descartadas mediante a fragmentação/trituração.

6.3.6 Diretrizes quanto à utilização da Rede Corporativa

A rede corporativa da ABRADILAN só pode ser utilizada para o desempenho de atividades da ABRADILAN, não sendo permitida a utilização para o desempenho de atividades particulares dos Usuários.

A rede corporativa da ABRADILAN é monitorada e verificada para fins de auditoria.

Não é permitido o armazenamento de arquivos particulares (músicas, filmes, fotos, etc) na rede corporativa da ABRADILAN. Esses arquivos serão excluídos pela área de TI da ABRADILAN sem aviso prévio.

É expressamente proibido expor, armazenar, distribuir, editar ou gravar material relativo a pornografia e/ou práticas ilícitas ou moralmente reprováveis nos equipamentos e recursos computacionais da rede corporativa da ABRADILAN.

A responsabilidade pelo controle, gerenciamento e revogação das permissões de acesso à rede corporativa da ABRADILAN compete ao pessoal expressa e previamente autorizado pela ABRADILAN.

Somente as pessoas que estão devidamente autorizadas para tanto podem falar e escrever em nome da ABRADILAN em sites de Blogs, Twitter, Facebook, LinkedIn ou Grupos de Discussão (fóruns, newsgroups).

Todos os arquivos devem ser gravados na rede, nas pastas específicas das áreas da ABRADILAN, porque os arquivos gravados no computador (local) não possuem cópias de segurança (*backup*) e não estarão disponíveis aos demais Usuários que eventualmente necessitem deles. Não é permitida a gravação de arquivos na Pasta Public da rede.

Os arquivos gravados na rede devem ser apagados após a sua utilização pelo Usuário, observados os prazos e regras definidos pela ABRADILAN e pela legislação em vigor.

É expressamente proibido causar violações de segurança ou interrupções nas comunicações de rede. As violações de segurança incluem, mas não estão limitadas, ao acesso a dados dos quais o Usuário

não é um destinatário ou login em um servidor ou conta em que o Usuário não está expressamente autorizado a acessar. A interrupção inclui, mas não se limita a, *sniffing* de rede, *pinged floods*, *spoofing* de pacotes, negação de serviço e informações de roteamento forjadas.

6.3.7 Diretrizes quanto ao uso de Mídias Removíveis

Não é permitido o uso de mídias removíveis - cartão de memória, disco óptico, Blu-ray, CD, DVD, disk pack, Pen Drive/Pen USB, exceto se autorizadas previamente e por escrito por pessoa expressa e previamente indicada pela ABRADILAN**.**

O uso de internet móvel (modem) nas Estações de trabalho não é permitido, exceto se autorizadas previamente e por escrito por pessoa expressa e previamente autorizado pela ABRADILAN.

Os Usuários que descumprirem a norma e utilizarem mídias removíveis, além de responderem pela inobservância da Política de Segurança da Informação, conforme definido nesta Política, serão também responsabilizados pelos danos que eventualmente causarem a ABRADILAN, seus associados ou terceiros.

Informações devem ser transmitidas usando as ferramentas corporativas da ABRADILAN (e-mail, rede de dados, software de mensageria) que são homologadas expressa e previamente pela ABRADILAN. Não é permitida a utilização de ferramentas online de terceiros para transmissão de informações, como DropBox e semelhantes.

Caso seja necessário e seja autorizado o transporte de arquivos em mídias removíveis (HD Externo ou PenDrive), os arquivos devem ser criptografados e apagados posteriormente, a fim de evitar vazamento de Informação.

6.3.8 Diretrizes quanto ao uso da Internet

A internet deve ser utilizada apenas para o desempenho das atividades da ABRADILAN. O acesso à internet pelo Usuário é monitorado pela ABRADILAN.

O acesso às páginas e *websites* é de responsabilidade de cada Usuário, sendo vedado o acesso a *websites* com conteúdos impróprios, legalmente proibidos e de relacionamentos.

O uso da internet para assuntos pessoais deve ser restrito, sem comprometer as atividades dos Usuários, sendo este o responsável pelo tráfego dos seus dados pessoais.

6.3.9 Armazenamento remoto (nuvem)

A ABRADILAN se utiliza de provedor de nuvem para armazenamento remoto dos arquivos de propriedade da ABRADILAN na nuvem.

Não é permitido o uso de qualquer outra solução de armazenamento na nuvem, que não seja a oficialmente homologada e adotada pela ABRADILAN.

Não é permitido o armazenamento de arquivos particulares na ferramenta de nuvem disponibilizada pela ABRADILAN.

Os arquivos gravados no provedor de nuvem devem ser apagados após a sua utilização pelo Usuário, observados os prazos e regras definidos pela ABRADILAN e pela legislação em vigor.

6.3.10 Recomendações sobre o uso do Correio Eletrônico (E-Mail)

O uso do correio eletrônico para envio e recebimento de e-mail corporativos deverá ocorrer apenas por meio do correio eletrônico da ABRADILAN. O Correio Eletrônico da ABRADILAN é monitorado e verificado para fins de auditoria.

Os Usuários devem observar as seguintes regras de utilização do correio eletrônico da ABRADILAN:

a) é proibido o uso do Correio Eletrônico para envio de mensagens que possam comprometer a imagem da ABRADILAN e/ou Usuários, ou possam causar prejuízo à ABRADILAN e/ou Usuários;

b) é vedada a utilização do e-mail corporativo da ABRADILAN para assuntos pessoais;

c) o e-mail não deve conter comentários inadequados, ofensivos, difamatórios, fraudulentos, mensagens de natureza sexual, racial, pornográfica, ou de assédio, ou que possam causar qualquer dano ou embaraço, ou que não estejam em conformidade com as políticas da ABRADILAN;

d) não é permitido o envio ou o reenvio de e-mail do tipo corrente, esquemas Ponzi, de pirâmide, ou outros de qualquer tipo, de propagandas políticas, pedido de votos, oferta de produtos ou serviços;

e) é proibida a bisbilhotice eletrônica (*electronic snooping*);

f) a despeito do direito da ABRADILAN de acessar mensagens, as mensagens devem ser tratadas como confidenciais pelos Usuários e acessadas somente pelo destinatário pretendido. Os Usuários não devem recuperar ou ler quaisquer mensagens de correio eletrônico que não sejam enviadas diretamente a eles, a menos que o destinatário pretendido tenha dado autorização prévia e por escrito para que outros acessem seu correio;

g) não executar ou abrir arquivos anexados a emails enviados por remetentes desconhecidos ou com características suspeitas. Em caso de dúvidas, o Usuário deve comunicar a pessoa expressa e previamente indicada pela ABRADILAN;

h) Não executar ou abrir links/endereços de e-mails suspeitos, como por exemplo de bancos solicitando alguma informação pessoal. Verificar sempre se o e-mail ou o endereço do link são realmente de fontes conhecidas. Em caso de dúvidas, o Usuário deve comunicar a pessoa expressa e previamente indicada pela ABRADILAN;

i) não utilizar o e-mail para enviar grande quantidade de mensagens (*spam*) que possam comprometer a capacidade da rede. Em caso de dúvidas, o Usuário deve contatar a pessoa expressa e previamente indicada pela ABRADILAN;

j) utilizar o e-mail para comunicações oficiais internas, as quais não necessitem obrigatoriamente do meio físico escrito. Isto diminui custo com impressão e aumenta a agilidade na entrega e leitura do documento.

6.3.11 Uso de *Softwares* de Mensageria

Recomenda-se a utilização do Zoom, Microsoft Teams, Skype, como ferramenta de comunicação e realização de reuniões entre Usuários e de Usuários com terceiro.

É vedada a utilização de sistema de reuniões para atividades pessoais.

A utilização de sistema de reuniões é monitorada e verificada para fins de auditoria.

A instalação de *software* de mensageria de terceiros e a liberação do acesso não é permitida, exceto mediante prévia autorização escrita por pessoa expressa e previamente indicada pela ABRADILAN.

6.3.12 Controle de Acesso a VPN

O uso do acesso à rede corporativa da ABRADILAN via VPN é restrito a Usuários cujo cargo ou função exige acesso à rede corporativa fora das instalações da ABRADILAN. Exceções deverão ser aprovadas por escrito por pessoa expressa e previamente indicada pela ABRADILAN.

6.3.13 Controle de Acesso Lógico (Baseado em Senhas)

Para acessar a Estação de trabalho e a rede corporativa, todo Usuário deve ter uma identificação única, pessoal e intransferível (Login), definida e informada por pessoa expressa e previamente indicada pela ABRADILAN qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação e uma senha pessoal, definida pelo Usuário. O Usuário assume a responsabilidade quanto ao sigilo da sua senha pessoal.

A distribuição de senhas (inicial ou não) aos Usuários pela pessoa expressa e previamente indicada pela ABRADILAN deve ser feita de forma segura. A senha fornecida pela pessoa expressa e previamente indicada pela deve ser trocada pelo Usuário no primeiro acesso.

A senha deve ter pelo menos oito caracteres contendo número, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos) e não deverá utilizar informações pessoais fáceis de serem obtidas,

como por exemplo o nome, o número de telefone ou data de nascimento do Usuário. A senha deve ser alterada a cada 90 (noventa) dias.

A senha não deve ser anotada em papel ou digitalmente, em hipótese alguma.

A senha não deve ser incluída em processos automáticos de acesso ao sistema, por exemplo, armazenadas em macros de planilhas e navegadores.

A troca de uma senha bloqueada só será liberada pela pessoa expressa e previamente indicada pela ABRADILAN .

7. MONITORAMENTO PELA ABRADILAN

A ABRADILAN implementou uma série de políticas e procedimentos consistentes com a legislação aplicável para proteger a confidencialidade, integridade e disponibilidade dos Sistemas e Tecnologia de Informação da ABRADILAN, da arquitetura de tecnologia da informação, rede e recursos de informação da ABRADILAN. Para tanto e observada a legislação aplicável, a ABRADILAN poderá monitorar, acessar, interceptar, divulgar qualquer conteúdo ou informação existente em qualquer instalação da ABRADILAN ou nos sistemas de tecnologia de informação da ABRADILAN ou transmitidos através da rede da ABRADILAN.

O pessoal expressa e previamente autorizado pela ABRADILAN conduz investigações que são necessárias para resolver qualquer mau funcionamento dos sistemas de tecnologia de informação da ABRADILAN que possa prejudicar seu funcionamento ou sua integridade.

O pessoal expressa e previamente autorizado pela ABRADILAN pode acessar remotamente todas as estações de trabalho. O pessoal expressa e previamente autorizado pela ABRADILAN acessará as estações de trabalho somente com a autorização expressa do Usuário. No contexto de atualizações e melhorias dos sistemas de tecnologia de informação da ABRADILAN, e quando nenhum Usuário estiver conectado a sua estação de trabalho, a pessoa expressa e previamente autorizada pela ABRADILAN pode ter que atuar no ambiente técnico das estações de trabalho, mas é proibido o acesso ao conteúdo da estação de trabalho.

Eventualmente, pessoas autorizadas pela ABRADILAN podem acessar ou monitor conteúdos de estação de trabalho - incluindo informações armazenadas e uso do computador da ABRADILAN ou outros dos sistemas de tecnologia de informação da ABRADILAN - para a segurança de terceiros ou quando for julgado necessário, sempre em conformidade com a legislação vigente.

8. DESLIGAMENTO DE EMPREGADOS

Se o contrato de trabalho de um empregado terminar, por qualquer motivo, o departamento de Recursos Humanos informará à pessoa expressa e previamente autorizada pela ABRADILAN a data de saída do empregado. A data de encerramento da conta de usuário e acessos aos sistemas da ABRADILAN do empregado será informada pelo seu gestor ao departamento de Recursos Humanos e comunicada pelo departamento de Recursos Humanos à pessoa expressa e previamente autorizada pela ABRADILAN.

Ao deixar a ABRADILAN, o empregado será informado do encerramento iminente de sua conta de usuário. Se um empregado possuir equipamento pertencente à ABRADILAN que tenha sido disponibilizado exclusivamente para sua atividade profissional, incluindo, mas não limitado a, um computador laptop ou telefone celular, o empregado é obrigado a devolver o equipamento na data do seu desligamento. O empregado deve apagar os arquivos pessoais e dados particulares. As contas e os dados pessoais do empregado serão apagados no prazo máximo de um ano após a partida do empregado. Quaisquer cópias de documentos ou comunicações profissionais e para o desenvolvimento das atividades e atingimento das metas e objetivos da ABRADILAN que o empregado deseje reter devem ser autorizadas previamente por escrito pelo seu gestor.

Se um empregado for demitido pela ABRADILAN e for obrigado a deixar as instalações da ABRADILAN imediatamente, o departamento de Recursos Humanos informará à pessoa expressa e previamente autorizada pela ABRADILAN. A pessoa expressa e previamente autorizada pela ABRADILAN mudará imediatamente a senha na conta de usuário do empregado e restringirá o acesso a essa conta somente ao gestor do empregado. Uma resposta automatizada será configurada para notificar os remetentes de e-mails ao empregado que ele não está mais trabalhando para a ABRADILAN. A conta de usuário será mantida ativa pelo tempo necessário para assegurar a continuidade dos negócios e proteger os direitos

da ABRADILAN no caso de uma reclamação contra a ABRADILAN por parte do empregado ou de terceiros. O gestor do empregado acessará os arquivos na conta de usuário durante esse período e somente para esses fins. Ao final desse período, a conta de usuário do empregado será apagada.

9. VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PENALIDADES

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de investigação e penalidades aos Usuários infratores, que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa aos colaboradores, a rescisão por justa causa do contrato com os prestadores de serviços, a advertência, suspensão e exclusão dos sócios-contribuintes ou sócios-colaboradores da ABRADILAN.

No caso do infrator ser um colaborador, a aplicação de penalidades será realizada conforme a análise do Comitê de Ética, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o Comitê, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

No caso de prestadores de serviço, o Comitê de Ética deve analisar a ocorrência e deliberar sobre a efetivação das penalidades conforme termos previstos no contrato assinado.

No caso dos sócios-contribuintes, sócios-colaboradores e seus representantes, o Comitê de Ética deve analisar a ocorrência e enviar o seu parecer ao Conselho Diretor, que tomará as providências conforme previsto nos estatutos da ABRADILAN.

O infrator será responsabilizado, ainda, pelos prejuízos causados à ABRADILAN, e/ou Usuários e/ou terceiros.

10. CASOS OMISSOS

Os casos omissos serão avaliados pelo Comitê de Ética para posterior deliberação.

As medidas estabelecidas nesta Política e nas demais normas e procedimentos de segurança não são exaustivos, em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, elas constituem rol meramente exemplificativo, sendo obrigação do Usuário adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir a proteção das Informações.

11. CANAL DE COMUNICAÇÃO

O cumprimento desta Política de Segurança da Informação da ABRADILAN é de responsabilidade de todos os Usuários.

Quaisquer descumprimentos ou indícios de descumprimento desta Política devem ser comunicados imediatamente para o Comitê de Ética, pelo e-mail reclamacoes@abradilan.com.br.

12. VIGÊNCIA E VALIDADE

A presente política é válida por tempo indeterminado, podendo ser revisada e alterada a qualquer momento pela ABRADILAN, sem aviso prévio, sempre que julgar necessário, ou conforme determinação legal. As novas versões serão publicadas no website da ABRADILAN. Recomenda-se que os Usuários revejam esta Política com regularidade.