Tipo de Documento	**Política Corporativa**	Responsável: Compliance
Assunto:	**SEGURANÇA DA INFORMAÇÃO**	Vigência: Setembro/ 2022

Objetivo

A Política de Segurança da Informação é uma declaração formal da **SPH Medical** 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.

Abrangência

Colaboradores, Diretores, Executivos, Consultores, Auditores, Parceiros diversos e demais contratados que estejam a serviço e disponibilizam de ativos corporativos da **SPH Medical,** suas unidades, subsidiárias e/ou coligadas.

Missão

Garantir a integridade, confidencialidade, legalidade e autenticidade da informação necessária para a realização dos negócios da **SPH Medical.**

Documentos de Referência

- ✓ NBR ISO/IEC 17799:2005 ABNT 21:204.01-010
- ✓ Lei 9.609/98 – Lei do Software

Termos e Definições

TI: Tecnologia da Informação
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*.
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, o que pode envolver apagamentos acidentais ou corrupção de dados.
Mídias Removíveis: Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, *Pen Drive*, cartão de memória entre outros.
USB: É um tipo de conexão "ligar e usar" que permite a conexão de periféricos sem a necessidade de desligar o computador.

VPN (Virtual Private Network): Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por funcionários em trânsito.

Softwares de Mensageria: São programas que permitem a usuários se comunicarem remotamente (à distância), através de conexão com a Internet. Por meio destes programas, é possível enviar mensagens de texto entre equipamentos fisicamente distantes. Também é possível enviar arquivos ou iniciar sessões de conversação com áudio e/ou com vídeo, em tempo real.

Firewall: É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.

Modem 3G: É um dispositivo sem fio, com saída USB para conexão em outro dispositivo tais como *Tablets* (com suporte 3G), *notebooks, netbooks, desktops*, etc. objetivando conexão com a internet. O modem 3G recebe e decodifica o sinal digital de alta velocidade transmitido pelas operadoras de celulares para aparelhos portáteis (celulares, *smartphones* e *notebooks*) compatíveis com a tecnologia 3G.

Diretrizes

(i) Diretrizes de Segurança da Informação

Conforme definição da norma NBR ISO/IEC 17799: 2005, a informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegida. A Política de Segurança da Informação tem por objetivo proteger a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

A segurança da informação é aqui caracterizada pela preservação da:

- Confidencialidade, que é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;
- Integridade, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
- Disponibilidade, a Política de Segurança da Informação deve ser divulgada a todos os Colaboradores e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

É fundamental para a proteção e salvaguarda das informações que os usuários adotem a ação de Comportamento Seguro e consistente com o objetivo de proteção das informações, devendo assumir atitudes proativas e engajadas no que diz respeito à proteção das informações.
Campanhas contínuas de conscientização de Segurança da Informação serão utilizadas para monitoração e controle destas diretrizes.
A Política de Segurança da Informação da **SPH Medical** é aprovada e revisada periodicamente pelo Conselho de Administração.

(ii) Atribuições e Responsabilidades na Gestão de Segurança da Informação

Definição

Cabe a todos os Colaboradores, Prestadores de Serviços e outros cumprir fielmente a Política de Segurança da Informação; buscar orientação do gestor imediato em caso de dúvidas relacionadas à segurança da informação; proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados; assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela **SPH Medical**; cumprir as leis e as normas que regulamentam osaspectos de propriedade intelectual; e comunicar imediatamente a área em questão quando dodescumprimento ou violação desta política e/ou através do Canal de Comunicação.

Diretorias, Gerências e Coordenações

Cabe às Diretorias, Gerências e Coordenações cumprir e fazer cumprir esta Política; assegurar que suas equipes possuam acesso e conhecimento a mesma; e comunicar imediatamente eventuais casos de violação de segurança da informação através da área de TI e/ou do Canal de Comunicação.

Área de TI e Governança

Cabe as duas áreas conjuntamente propor ajustes, melhorias, aprimoramentos e modificações desta Política; convocar, coordenar, lavrar atas e prover apoio às reuniões que discutam a respeito desta Política; prover todas as informações de gestão de segurança da informação solicitadas por Gestores.

Utilização dos Recursos Computacionais

Equipamentos

Tipo de Documento	**Política Corporativa**	Responsável: Compliance
Assunto:	**SEGURANÇA DA INFORMAÇÃO**	Vigência: Setembro/ 2022

Todos os equipamentos da companhia devem ser desligados diariamente no término do expediente, a não ser que os mesmos estejam preparados para algum procedimento programado.

É absolutamente proibido efetuar ou permitir qualquer manutenção de qualquer dos recursos computacionais da **SPH Medical**, sem autorização da área de Tecnologia da Informação (TI).

Ao averiguar qualquer problema de mau funcionamento de qualquer equipamento da **SPH Medical**, os usuários desses recursos deverão comunicar a área de Tecnologia da Informação (TI), para os devidos reparos.

É absolutamente vedada a abertura de computadores para qualquer tipo de reparo, verificação, limpeza ou qualquer outra situação. Pessoal técnico terceirizado só poderá ter acesso aos recursos computacionais da **SPH Medical** devidamente autorizados pela área de Tecnologia da Informação (TI).

Não é permitida a alteração das configurações de rede e inicialização das máquinas, bem como, modificações que possam trazer algum problema no desempenho.

Não é permitido o manuseio, troca, substituição ou mudança de local de conjuntos completos de equipamentos ou de seus acessórios, por qualquer que seja o motivo, sem a anuência da área de Tecnologia da Informação (TI).

É vedado o acesso e manuseio dos equipamentos e instalações computacionais, ao usuário que portar alimentos e/ou bebidas, devendo esses permanecer em locais apropriados. Qualquer acidente, que coloque em risco a integridade dos recursos computacionais da **SPH Medical** será considerado atitude irresponsável e cabível de sanções trabalhistas.

Utilizações de E-mail

É vedada a utilização de e-mail organizacional, em lojas virtuais, listas de discussões, ou qualquer outra utilização de internet, em ambiente fora da **SPH Medical**.

É proibida a distribuição voluntária ou despercebida de mensagens não desejadas, como circulares, correntes, pirâmides ou outros esquemas que possam prejudicar o trabalho de terceiros, causar excessivo tráfego na rede ou sobrecarregar os sistemas operacionais.

É proibido o uso do spam, sendo considerado o envio simultâneo de mensagens eletrônicas não solicitadas, de conteúdo similar para mais de 20 caixas postais.

Não fazer uso dos recursos para finalidades políticas, tais como o uso do correio eletrônico para circular propaganda de candidatos políticos ou denegrir a imagem de outros.

Não visualizar, armazenar, transferir ou enviar materiais pornográficos, eróticos, indecentes, ofensivos, que incentivem a violência, uso de drogas, discriminação de raça, credo entre outros.

Ao sair de férias, a área de Tecnologia da Informação (TI), deverá ser informada, para que a mesma possa fechar a caixa postal do usuário ou redirecioná-la para a caixa postal de outra pessoa.

Utilizações da Internet

É proibida a divulgação de informações confidenciais da **SPH Medical** em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei. Sendo do interesse da companhia que os seus Colaboradores estejam bem informados, o uso de sites de notícias ou de serviços de notícias é aceitável, desde que o seu uso não comprometa o uso de banda da rede, nem perturbe o bom andamento dos trabalhos. Poderá ser utilizada a Internet para atividades não relacionadas com a atividade fim durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta Política da empresa em uma máquina específica para tal finalidade.

Não utilizar a Internet para acessar salas de bate-papo (chat) e sites de lazer que se contraponham às regras de uso definidas nesta Política. A instalação ou utilização de qualquer tipo de jogos é proibida, inclusive jogos locais do Windows.

É vedada a instalação e utilização de comunicadores instantâneos, a não ser o comunicador “Skype”, com autorização / criação de usuário e configuração, feita mediante solicitação a área de Tecnologia da Informação (TI).

Não é permitida a instalação ou utilização de qualquer tipo de programa que toque, armazene ou baixe músicas ou vídeos.

Não será permitida a utilização de serviços de streaming, tais como rádios on-line e afins.

Utilização de Dados e Programas

Tipo de Documento	**Política Corporativa**	Responsável: Compliance
Assunto:	**SEGURANÇA DA INFORMAÇÃO**	Vigência: Setembro/ 2022

Somente utilizar sistemas, software e materiais protegidos por direitos autorais, de acordo com a lei. Nunca instalar sistema(s), software e outros sem o controle de procedência e dos direitos autorais e por intermédio da área de Tecnologia da Informação (TI). Sem uma aprovação / autorização específica de TI, os usuários não

podem remover, dos recursos computacionais, nenhum documento de propriedade da organização ou por ela administrado.

Os usuários não devem, deliberadamente, efetuar ou tentar qualquer tipo de acesso não autorizado a dados dos recursos computacionais da companhia, ou tentar sua alteração, como por exemplo, ler mensagens pessoais de terceiros ou acessar arquivos confidenciais.

Os recursos computacionais da **SPH Medical** não podem ser utilizados para constranger, assediar ou ameaçar qualquer pessoa. Esses recursos não podem ser usados para alterar ou destruir recursos computacionais de outras empresas / instituições. Se a partir de uma conta, um usuário estiver, de qualquer maneira, interferindo no trabalho de outro, este deve comunicar o fato ao responsável pelo equipamento onde está a conta, o qual, a seu critério, e sem prejuízo de outras sanções, poderá determinar a imediata suspensão temporária da conta de onde parte interferência, comunicando o caso a área de Tecnologia da Informação (TI).

Os usuários não podem violar ou tentar violar os sistemas de segurança dos recursos computacionais da companhia, como quebrar ou tentar adivinhar identificação ou senhas de terceiros, interferir em fechaduras automáticas ou sistemas de alarme.

Os usuários não podem interceptar ou tentar interceptar transmissão de dados não destinados ao seu próprio acesso, seja monitorando barramentos de dados, seja através da rede, exceto quando autorizados explicitamente pelo Presidente da companhia.

Os usuários são responsáveis pela segurança de suas contas de acesso e de suas senhas. A conta e a respectiva senha são atribuídas a um único usuário e não devem ser compartilhadas com mais pessoas sem a autorização expressa a área de Tecnologia da Informação (TI). Os usuários devem relatar imediatamente a essa área, qualquer suspeita de tentativa de violação de segurança.

Os usuários, a menos que tenham uma autorização específica da área de Tecnologia da Informação (TI) para este fim, não podem tentar permitir ou causar qualquer alteração ou destruição de ambientes operacionais, dados ou procedimentos de processamento ou comunicações. Essas alterações incluem, mas não se limitam à alteração de dados, reconfiguração de chaves de controle ou parâmetros.

Material sexualmente explícito (em especial pedofilia), racista, político, religioso, ou quaisquer tipos de discriminação, não podem ser expostos, armazenados, distribuídos, editados ou gravados através do uso dos

recursos computacionais e de comunicação. Se qualquer um dos Colaboradores tomar conhecimento da prática de algum dos atos ilícitos, aqui já elencados, deverá informar a área em questão, para que sejam tomadas as devidas providências junto às autoridades competentes.

Não é permitida a cópia ou instalação de programas licenciados para a **SPH Medical** emequipamentos de terceiros.

Nos recursos computacionais da **SPH Medical**, será garantido o maior grau possível de confidencialidade no tratamento dos dados dos usuários, de acordo com as tecnologias disponíveis, entretanto, os Colaboradores da área de Tecnologia da Informação (TI), poderão acessar arquivos de dados pessoais ou corporativos nos sistemas, sempre que isso for necessário para backups ou diagnóstico de problemas nos sistemas, inclusive nos casos de suspeita de violação de regras.

Antivírus

Antivírus dos servidores e estações são atualizados automaticamente.
A varredura por vírus é feita diariamente / periodicamente nas estações e nos servidores.

Controle de Acesso Lógico (Baseado em Senhas)

Todo usuário deve ter uma identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal.
Utilizar senha de qualidade, com pelo menos oito caracteres contendo números, letras (maiúsculas e minúsculas) e caracteres especiais (símbolos), e não deverá utilizar informações pessoais fáceis de serem obtidas como, o nome, o número de telefone ou data de nascimento como senha.

Controle da Utilização dos Recursos Computacionais

Para garantir o cumprimento das normas mencionadas acima a **SPH Medical** se reserva no direitode:

- Implantar softwares e sistemas que podem monitorar e gravar o uso da Internet através da rede e das estações de trabalho da entidade;
- Inspecionar qualquer arquivo armazenado na rede esteja no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta política.

Tipo de Documento	**Política Corporativa**	Responsável: Compliance
Assunto:	**SEGURANÇA DA INFORMAÇÃO**	Vigência: Setembro/ 2022

Das Punições

Para garantir a adequada utilização dos recursos computacionais da **SPH Medical,** fica autorizado aplicar penalidadesaos que violarem a legislação em vigor e as dispostas nesta Política.

As penalidades a serem aplicadas por infração às normas indicadas no "caput" são aplicação de advertências que variam de 1 (uma) no mínimo, e de 3 (três) no máximo, dependendo da gravidade da infração e de justa causa, nos termos do artigo 482 alíneas "b" e "h" da Consolidação da Legislação Trabalhista.

Sempre que julgar necessário para a preservação da integridade dos recursos computacionais da empresa, dos serviços aos usuários ou dos dados, a área de Tecnologia da Informação (TI) poderá suspender temporariamente qualquer conta, seja ou não o responsável pela conta de alguma violação.

O usuário suspeito de violação dessas normas será notificado das irregularidades e terá a oportunidade de se pronunciar antes de qualquer decisão a ser tomada pela companhia.

Canal de Comunicação: Tecnologia / Governança

Atendimento telefônico: [11] 4302-6868

E-mail: compliance@sphmedical.com.br

* * *