PSI COOPANEST SC

Sumário

1. Introdução;

A Lei Geral de Proteção de Dados (Lei n°. 13.709/2018) tem o propósito de estabelecer padrões à utilização de dados pessoais e dados sensíveis de pessoas físicas, visando evitar abusos.

A Coopanest-SC, como Cooperativa de Especialidade Médica e intermediadora da relação paciente – cooperado – estabelecimento de saúde, é controladora de dados sensíveis como nomes de pacientes, boletins anestésicos, descrições cirúrgicas, guias de informações sobre procedimentos e anamnese de pacientes. Também controla dados pessoais de cooperados, colaboradores e de prestadores.

Visando adequação à Lei Geral de Proteção de Dados (LGPD), a Coopanest-SC incluiu no seu planejamento estratégico de 2020 a implantação de programa de *compliance* de dados.

Além da matriz de riscos de dados e do mapa de dados, essa Política de Segurança da Informação (PSI) tem o propósito de consolidar rotinas que garantam a segurança dos dados sensíveis geridos pela Coopanest-SC.

A operação dos dados controlados pela Coopanest-SC é feita por empresa prestadora terceirizada, que desenvolveu software de gestão da informação. A prestadora está ciente das rotinas estabelecidas nesta política e comprometido com seu cumprimento.

2. Rotinas de Segurança da Informação;

As rotinas de segurança da informação ora apresentadas são de cumprimento obrigatórios pelos colaboradores da Coopanest-SC sob pena de imposição das sanções previstas no item 4 desta PSI.

2.1. **Entrada na Coopanest-SC;**

2.1.1. A ingressar no quadro da Coopanest-SC o colaborador recebe uma chave de acesso à sua sala sede;

2.1.2. Tal chave deve ser guardada de maneira segura e não deve ser emprestada nem a terceiros nem a outros colegas;

2.1.3. A perda o extravio da chave deve ser comunicado imediatamente ao encarregado de dados;

2.2. **Visitas;**

2.2.1. Quando o colaborador for receber visitas, mesmo que de familiares, na sede da empresa deve comunicar o encarregado de dados para que registre a presença de terceiro na organização com data e horário de acesso e permanência.

2.3. **Acesso à Internet;**

2.3.1. O acesso à Internet pode ser feito via cabo ou wi-fi;

2.3.2. A senha do wi-fi da Coopanest-SC não deve ser compartilhada com terceiros que não estejam na organização no momento do uso;

2.3.3. Sites com conteúdo questionável (como pornográficos) não devem ser acessados pela rede wi-fi da Coopanest-SC;

2.3.4. Equipamentos pessoais não devem ser plugados na rede a cabo da organização.

2.4. **Senhas;**

2.4.1. As senhas de acesso aos softwares e servidores da Coopanest-SC são pessoais e intransferíveis;

2.4.2. As senhas pessoais não devem ser compartilhadas em hipótese alguma;

2.4.2.1. Alteração de alçada de senhas de acesso e operação (principalmente bancárias) serão abordadas em **política própria**;

2.4.3. As senhas devem ser alteradas com periodicidade de pelo menos noventa dias;

2.4.4. As senhas precisam ser fortes, compostas por números, letras e símbolos;

2.4.5. Não se recomenda a utilização de datas ou nomes próprios como senha pessoal;

2.4.6. As senhas não devem ficar anotadas na estação de trabalho, em post its ou blocos de notas;

2.4.7. O processo de cancelamento de login e senha de usuário pelo desligamento do colaborador ou alteração de departamento será contemplado por **política própria**.

2.5. **Estação de Trabalho;**

2.5.1. Compreende-se por estação de trabalho o espaço de labor do colaborador onde fica seu computador e demais equipamentos da organização que utiliza para a consecução de suas tarefas;

2.5.2. Para a gestão adequada da estação de trabalho, importante atentar para os cinco sensos:

2.5.2.1. Senso de utilização: consistente na seleção de quais materiais, equipamentos e ferramentas devem ser considerados importantes e quais devem ser considerados supérfluos;

2.5.2.2. Senso de organização: determina que todos os itens a serem utilizados de forma comum devem ficar disponíveis em locais determinados, facilitando seu acesso;

2.5.2.3. Senso de limpeza: visa promover o hábito de limpeza recorrente, com a eliminação dos itens que não são essenciais ao espaço de trabalho;

2.5.2.4. Senso de padronização: trata-se da promoção de consciência e ação quanto ao fortalecimento de hábitos e processos repetíveis;

2.5.2.5. Senso de autodisciplina: compromisso com os outros quatro sensos, que dependem de autodisciplina para a sua consecução.

2.5.3. Para garantir a segurança dos dados contidos em cada equipamento, os computadores são programados para bloquear automaticamente a tela quando ficar por cinco minutos sem movimentação;

2.5.4. É vedado:

2.5.4.1. Fixar na tela do computador, mesa ou divisórias informações confidenciais como senhas de acesso aos sistemas da organização;

2.5.4.2. Ausentar-se da estação de trabalho sem bloquear o acesso da máquina, trancar gavetas e armários;

2.5.4.3. Deixar sobre a mesa documentação sigilosa enquanto não estiver na estação de trabalho;

2.5.4.4. Deixar folhas impressas visíveis na bandeja da impressora ser dar descarte adequado;

2.5.4.5. Burlar o sistema de bloqueio automático de tela.

2.5.5. Num sentido de promoção da responsabilidade ambiental da organização, além da segurança da informação, recomenda-se que seja evitada a impressão de documentos, sempre que possível.

2.6. **Utilização da máquina corporativa e periféricos;**

2.6.1. O computador fornecido pela organização deve ser utilizado exclusivamente no seu interesse a partir das regras contidas neste item;

2.6.2. É vedada a utilização do computador da empresa para fins pessoais;

2.6.3. É vedada a utilização da impressora da empresa para fins pessoais;

2.6.4. É vedado o armazenamento de arquivos e informações exclusivamente na máquina, devendo, para tanto, ser utilizado o servidor;

2.6.5. A utilização de arquivos compactados (rar., zip., etc.) precederão de autorização do encarregado de dados;

2.6.6. É vedada a utilização de periféricos nas máquinas, a exemplo de pendrives, HD externo e celulares;

2.6.7. O antivírus deve ser atualizado com periodicidade mínima de 30 (trinta) dias;

2.6.8. Caso surja alguma dificuldade na atualização do antivírus pode ser solicitado o apoio do encarregado de dados;

2.6.9. É vedada a abertura do computador pelos colaboradores para qualquer tipo de reparos. Havendo problemas técnicos, o encarregado de dados ou a TI devem ser acionados;

2.6.10. É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela equipe de TI;

2.6.11. É proibida a instalação de softwares que não possuam licença e/ou não sejam homologados pela equipe de TI;

2.6.12. Não serão permitidos os acessos a softwares *peer-to-peer* (a exemplo do *Kazaa, BitTorrent, µtorrent* e afins);

2.6.13. É vedado deferir acesso remoto ao equipamento da organização, mesmo para fins de manutenção. As manutenções nos equipamentos da organização devem ser presenciais;

2.6.14. É vedado acessar whatsapp® pessoal no computador corporativo vai versão web;

2.6.15. É vedado acessar redes sociais pessoais no computador corporativo.

2.7. **Utilização de e-mail corporativo;**

2.7.1. O e-mail corporativo deve ser utilizado exclusivamente no interesse da organização;

2.7.2. É vedada a utilização do e-mail corporativo para fins pessoais;

2.7.3. É vedado preencher cadastros pessoais utilizando o e-mail corporativo;

2.7.4. É vedado realizar compras na internet usando o e-mail corporativo;

2.7.5. É vedado acessar o e-mail corporativo em máquinas externas a organização ou não homologadas pelo encarregado de dados;

2.7.6. E-mails suspeitos não devem ser abertos, mesmo que tenham sido enviados por destinatários conhecidos;

2.7.7. É proibido abrir arquivos com origens desconhecidas anexados a mensagens eletrônicas;

2.7.8. Os e-mails enviados ou recebidos de endereços externos poderão ser monitorados com o intuito de bloquear *spams*, *malwares* ou outros conteúdos maliciosos que violem a Política de Segurança da Informação;

2.7.9. É proibido enviar, com endereço eletrônico corporativo, mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo “corrente”, campanhas ou promoções;

2.7.10. O e-mail pessoal não deve ser manuseado nas máquinas da Coopanest-SC, para que não as deixe expostas a qualquer antígeno que possa chegar pelos e-mails pessoais, como vírus;

2.7.11. É proibido enviar qualquer mensagem por meios eletrônicos que torne a Coopanest-SC vulnerável a ações civis ou criminais;

2.7.12. Deve-se utilizar linguagem formal na comunicação via e-mail corporativo;

2.7.13. Não devem ser aplicadas gírias e emojis em comunicação via e-mail corporativo;

2.7.14. Não será admitida, sob qualquer hipótese, a manutenção ou arquivamento de mensagens de conteúdo ofensivo, discriminatório, pornográfico ou vexatório, sendo a responsabilidade apurada de forma específica em relação ao destinatário da mensagem.

2.7.15. O e-mail corporativo só pode ser utilizado dentro da jornada de trabalho do colaborador autorizado.

2.8. **Utilização de celular corporativo;**

2.8.1. O celular corporativo deve ser utilizado exclusivamente no interesse da organização.

2.8.2. É vedado abrir *whatsapp®* pessoal no celular corporativo;

2.8.3. É vedado baixar aplicativos no celular corporativo sem autorização expressa do encarregado de dados;

2.8.4. É vedado emprestar o celular corporativo para pessoas não autorizadas;

2.8.5. É vedado utilizar o número corporativo para cadastros pessoais em sites de compra ou qualquer outra finalidade;

2.9. **Utilização de *whatsapp®* corporativo;**

2.9.1. O *whatsapp®* corporativo é para uso exclusivo no interesse da Coopanest-SC.

2.9.2. A comunicação pelo *whatsapp®* corporativo deve ser feita com linguagem formal, atendendo as demais regras de redação de e-mail corporativo, contidas no item 2.7.

2.9.3. A fotografia do *whatsapp*® corporativo não deve ser do colaborador autorizado a operá-lo, mas sim uma imagem padrão de identidade visual da organização.

2.9.4. O *whatapp*® corporativo deve ser manejado exclusivamente pelo colaborador autorizado, que não pode solicitar a terceiros que digitem as mensagens para si;

2.9.5. O *whatsapp*® corporativo só pode ser utilizado dentro da jornada de trabalho do colaborador autorizado.

2.10. ***Bring your own device*** **(BYOD);**

2.10.1. A sigla BYOD significa *bring your own device*, traduzida para o português como *traga seu próprio equipamento*.

2.10.2. A utilização de equipamento pessoal para a gestão de tarefas da organização será possível apenas mediante autorização expressa do encarregado de dados.

2.10.3. O encarregado de dados fará o cadastro e homologação de todos os equipamentos pessoais que forem utilizados no interesse da organização.

2.10.4. A inspeção no equipamento pode ser necessária para confirmar a sua integridade para gerir e/ou armazenar informações da organização.

2.10.5. O equipamento pessoal, para que seja autorizada a sua utilização para fins corporativos, precisa estar em cumprimento às determinações contidas no item 2.6. desta PSI.

2.10.6. O equipamento pessoal em que transitam informações da organização não pode ser utilizado para acessar e-mail pessoal, *whatsaap*® pessoal ou qualquer outro programa que coloque em risco a integridade das informações controladas pela Coopanest-SC.

2.11. **Documentos físicos;**

2.11.1. Pela exposição maior ao extravio, recomenda-se primar pelo arquivamento de informações em formato digital – atendendo-se, neste sentido, todas as recomendações para que se mantenha sua segurança e integridade.

2.11.2. Caso seja necessário arquivar documentos em formato físico, devem ser cumpridas as seguintes rotinas:

2.11.2.1. O documento não deve ficar exposto, sobre a mesa ou em gavetas não protegidas por chave;

2.11.2.2. Os documentos devem sempre ser mantidos sob guarda em locais com chave ou fechadura digital;

2.11.2.3. Cada documento físico terá seu status de fragilidade avaliado pelo encarregado de dados;

2.11.2.3.1. Aqueles documentos que forem avaliados como de grau máximo de fragilidade deverão ser guardados em cofre.

2.11.3. Os documentos físicos não devem ser descartados antes de transcorridos cinco anos do seu recebimento.

2.11.4. O descarte anterior ao prazo estabelecido no item 2.11.3. depende de autorização expressa e documentada do titular do dado.

3. Sanções;

3.1. O descumprimento comprovado de qualquer disposição desta política poderá acarretar na imposição de sanção ao colaborador que incorrer no desvio.

3.2. O procedimento de apuração será conduzido pelo encarregado de dados, deferido espaço de justificativa da conduta pelo colaborador em suspeita de desvio.

3.3. As sanções poderão ser: advertência verbal, advertência por escrito e demissão.

3.4. A advertência verbal será aplicada na hipótese de descumprimento cometido por colaborador primário e que não tenha implicado em vazamento de dados sensíveis.

3.5. A advertência por escrito será aplicada na hipótese de reincidência de colaborador em conduta que não tenha implicado em vazamento de dados sensíveis.

3.6. A demissão poderá ser aplicada na segunda reincidência em conduta que não tenha implicado vazamento de dados.

3.7. A demissão será aplicada para o colaborador que incidir em conduta que implique em vazamento de dados ou que torne inviável a entrega de comunicação a contento ao titular ou a Autoridade Nacional de Proteção de Dados.

4. Atuação do encarregado de dados:

4.1. Qualquer evento adverso, confirmado ou sob suspeitam, deverá ser informado ao encarregado de dados, tais como:

4.1.1. Evento adverso confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, bem como estruturas físicas e lógicas associadas, que comprometa a confidencialidade, a integridade e a disponibilidade do ambiente da organização;

4.1.2. Vazamento de informações confidenciais (informações de clientes, informações estratégicas, outros);

4.1.3. Tentativas interna ou externa de ganhar acesso não autorizado a sistemas, a dados ou até mesmo comprometer o ambiente da TI;

4.1.4. Uso ou acesso não autorizado a um sistema;

4.1.5. Compartilhamento de senhas.

5. Atuação da TI;

5.1. A empresa que atua como prestadora de serviços de tecnologia da informação deverá estar ciente e concorde com os termos da PSI.

5.2. Cabe apenas a TI a manutenção dos equipamentos da Coopanest-SC, sendo vedado aos colaboradores que contatem pessoa diversa do TI designado pela organização.

5.3. É vedado aos colaboradores tentarem prestar suporte aos equipamentos sem supervisão adequada do TI designado.

5.4. O TI designado ficará encarregado de monitorar as atualizações de firewall e antivírus.

5.5. O TI designado ficará encarregado de proceder aos backups e demais arquivos da documentação e informação controlada pela Coopanest-SC.

5.6. O cenário ideal à estrutura de segurança da informação é a ausência de intercorrências, mas é essencial a previsão por esta PSI do procedimento a ser conduzido na hipótese de suspeita de ocorrência de qualquer sinistro.

5.7. Todos os colaboradores devem notificar imediatamente ao encarregado de dados eventual vazamento ou uso inadequado de informação, para que seja possível o controle de potenciais resultados.

5.8. O encarregado de dados contará com o suporte do TI para a resolução de eventuais sinistros ocorridos.

5.9. O histórico de sinistros e procedimento a sua resolução serão documentados para evitar episódios futuros, servindo como procedimento padrão de contensão de novos eventos.

6. Fornecedores e parceiros;

6.1. Fornecedores e parceiros deverão estar cientes e comprometidos com esta PSI.

6.2. Os contratos firmados com fornecedores e parceiros conterão cláusulas relacionadas às diretrizes de segurança da informação que devem ser conduzidas por eles internamente visando viabilizar a relação jurídica.

6.3. A negativa em subscrever termos de ciência e compromisso com a PSI justifica tanto a não celebração de contrato quanto a rescisão.

6.4. Justifica-se a rescisão contratual com empresas prestadoras ou parceiras que não estejam se adequando à LGPD.

7. Considerações Finais;

7.1. As regras contidas nesta Política de Segurança da Informação são cogentes e obrigam todos os colaboradores da Coopanest-SC.

7.2. Todos os colaboradores tiveram acesso e participaram de treinamento a respeito das rotinas desta Política de Segurança da Informação, não podendo justificar seu descumprimento ao argumento de falta de ciência de seu conteúdo.

7.3. A ciência e domínio a respeito das regras de segurança da informação aqui contidas pode ser utilizadas como critério de contratação e promoção de colaboradores.

7.4. Treinamentos periódicos podem ser realizados visando reforçar as premissas desta PSI, aos qual todos os colaboradores estão obrigados a participar.