CÓDIGO DE BOAS PRÁTICAS EM PROTEÇÃO DE DADOS PESSOAIS

CIRÚRGICA SANTA CRUZ

I- Informações preliminares

Empresa/Organização: CIRÚRGICA SANTA CRUZ COMÉRCIO DE PRODUTOS HOSPITALARES LTDA
CNPJ: 94.516.671/0001-53
Endereço: Rua Coronel Oscar Rafael Jost n 1955
Telefone: 5121079000
DPO/Encarregado(a) de dados pessoais: Luciane Doern
E-mail do DPO/Encarregado(a): rh@cirurgicasantracruz.com.br
Responsável pela empresa: Jeferson Schuster

II - Versionamento

Primeira publicação: 09/10/2023
Versão: 0.1

1. CONSIDERAÇÕES INICIAIS

A CIRÚRGICA SANTA CRUZ COMÉRCIO DE PRODUTOS HOSPITALARES LTDA, é empresa do ramo de distribuição de medicamentos voltada fornecimento de produtos e serviços com qualidade para promover a saúde e o bem-estar do ser humano e busca ser reconhecida como a melhor e principal empresa na distribuição de medicamentos e produtos para a saúde, atendendo plenamente as necessidades de seus clientes na sua área de atuação.

Com o advento da lei n 13.709/18 a *Cirúrgica Santa Cruz* desenvolveu um programa de adequação da empresa às regras da Lei Geral de Proteção de Dados que busca garantir a confidencialidade, integridade e disponibilidade da informação por meio da gestão dos dados pessoais e do tratamento dados a estes dados dentro da empresa.

Para viabilizar o melhor sistema de gestão dos dados pessoais a empresa através de sua direção, e com lastro no General Data Protection Regulation, da União Europeia, criou um *Comitê de Privacidade e Proteção de Dados Pessoais*, formado por integrantes dos setores de Recursos Humanos, Marketing, Direção e Tecnologia da Informação, responsáveis pelas decisões e criações de um compliance da lei nº 13.709/18.

Entre as definições do Comitê de Privacidade e Proteção de Dados Pessoais esta a criação do presente *Código de Boas Práticas em Proteção de Dados Pessoais*, como forma de propiciar o pleno desenvolvimento das práticas voltadas à privacidade e a proteção dos dados pessoais, bem como para que os processos já implementados, se consolidem com segurança, aderência à legislação e proporcionem total confiança aos clientes, funcionários, colaboradores, parceiros e a sociedade como um todo.

O *Código de Boas Práticas em Proteção de Dados Pessoais*, tem a função de ser um instrumento capaz de fomentar e fortalecer a disseminação de uma cultura de proteção de dados dentro da *Cirúrgica Santa Cruz*.

2. Das responsabilidades e dos papéis

A responsabilidade pela privacidade e proteção dos dados pessoais dentro da *Cirúrgica Santa Cruz* é compartilhada entre a direção, o encarregado de proteção de dados e os setores que compõe o *Comitê de Privacidade e Proteção de Dados Pessoais,* na pessoa que estiver na função de líder no setor, e/ou chefia e em setores que contarem com apenas um funcionário este será o responsável.

Dentre as atribuições dos responsáveis está zelar pela observação deste código, da Política de Privacidade e Proteção de Dados, gerenciar os risos inerentes ao setor sempre que houver tratamento de dados pessoais, propiciar um ambiente favorável ao desenvolvimento da cultura da prática da proteção de dados pessoais.

Cabe a cada responsável de área identificar os ativos e os processos que envolvam dados pessoais, e sempre que identificar risco a sua privacidade e segurança comunicar ao Encarregado de Proteção de Dados; Zelar e respeitar os níveis de autorização dos processos, de acordo com as definições da diretoria e do *Comitê de Privacidade e Proteção de Dados Pessoais.* Participar, sempre que propiciado pela empresa das atividades voltadas ao desenvolvimento e atualização em relação às normas, regramentos e diretrizes de privacidade e proteção de dados, das autoridades públicas e da Autoridade Nacional de Proteção de Dados - ANPD;

3. Segregação e funções

A *Cirúrgica Santa Cruz* tem com prática a segregação de funções para fins de acesso aos dados pessoais que são tratados na empresa, primando para que eles sejam acessados unicamente quando necessário para cumprir a finalidade para os quais eles foram coletados, de acordo com as bases legais do art. 7º da Lei 13.709/18.

Com esta prática busca-se reduzir as oportunidades de tratamentos inadequados e/ou fora do escopo para os quais foram coletados e/ou se tenha autorização, bem como o compartilhamento indevido, preservando a integridade, confidencialidade e disponibilidade dos dados pessoais.

São utilizados sistemas de senhas de acesso com níveis de permissões de acesso diretamente relacionado a necessidade de acesso e tratamento de dados pessoais neles contidos.

Tabela de Segregação

Sistemas	Setores que acessam
NL	Todos os setores (observado os níveis de acesso de cada setor/função)
MOBILE	Vendedores externos, Contas a Receber, Direção e TI
MANAGER	Vendas internas, TI
SKIPE	Todos os setores (observado os níveis de acesso de cada setor/função)
INTRANET	Todos os setores (observado os níveis de acesso de cada setor/função)

4. Contato com autoridades

Sempre que houver risco aos dados pessoais tratados dentro da empresa Cirúrgica Santa Cruz, que ensejem comunicação com autoridades, o Encarregado de Proteção de Dados será imediatamente informado e participará deste contato, garantindo o correto registro dos incidentes que possam ter ocorrido ou vir a ocorrer em razão do incidente, para que este tome as providências necessárias e faça os comunicados especificados em lei.

5. Segurança da informação no gerenciamento de projetos

O desenvolvimento de projetos pela *Cirúrgica Santa Cruz* deverá, obrigatoriamente, contemplar de forma metodológica, em todas as fases de seu desenvolvimento a privacidade e proteção dos dados pessoais, deverá ter como objetivo do projeto *garantir a privacidade e proteção dos dados pessoais*, deverá ser adotada, já na fase inicial, a avaliação dos riscos de segurança para identificar os controles que serão necessários.

5.1 *Segurança da informação*

Para manter o níveis de segurança da informação e evitar acesso indevidos e demais incidentes de segurança a empresa adota a rastreabilidade e a gestão de log, antivírus, Firewall, VPN, além de níveis de acesso por setor e por função, o servidor possui filtros de anti-spam e outras ameaças.

A empresa possui programa de gerenciamento de seus ativos e esporadicamente auditorias internas, utiliza a prática de NDA para cargos de acesso a informações críticas.

6. Política de Uso de dispositivos móveis

A Cirúrgica Santa Cruz disponibiliza aos seus funcionários computadores e celulares para realização das atividades institucionais e mantém registro destes dispositivos móveis. Os colaboradores devem primar pela proteção física dos equipamentos e a utilização através do uso de senhas e evitando deixá-los dentro do

carro quando não houver ninguém, em ambiente sem chave e/ou vigilância da empresa, quando utilizados em *home office* guardar em local seguro preferencialmente com tranca.

Todos os dispositivos disponibilizados pela Cirúrgica Santa Cruz possuem antivírus e o acesso aos dispositivos é restrito a questões relacionadas ao trabalho e os aparelhos não são compartilhados com terceiros, nem mesmo em ambiente familiar.

Quando utilizados fora da empresa os computadores tipo notebook tem ativada a função VPN para permitir o acesso em uma conexão segura, os trabalhadores externos e direção possuem seus próprios equipamentos institucionais já programados com esta função, demais funcionários que necessitam destes dispositivos devem solicitar ao setor de Ti que providenciará a ativação da função VPN.

Quando não estão em uso os dispositivos possuem bloqueio de tela, o uso de senha para acesso é obrigatório e revisto periodicamente, o acesso à internet por rede pública como quartos de hotéis, centros de conferência, locais de reunião externos, devem ser evitados, as exceções devem ser comunicadas ao responsável pelo setor e ao encarregado de proteção de dados, sempre que possível a empresa disponibilizará dispositivo neutro, que não possua contato direto com nenhuma base de dados pessoais.

Os dispositivos móveis não devem conter dados pessoais de clientes, colaboradores e/ou parceiros e terceiros, estes dados são mantidos na base de dados da empresa que encontra-se no google drive, havendo necessidade de baixar algum arquivo que contenha dados pessoais, este será apagado logo após ser incluído na base do google drive;.

7. Seleção/Termos e Condições de Contratação

Os processos seletivos da *Cirúrgica Santa Cruz* são conduzidos através do setor de Recursos Humanos da empresa e ocorre pelo envio de currículos de forma voluntaria, site e agências de recrutamento; Todos os candidatos que enviam currículos, ainda que fora de um período específico de processo seletivo, recebem um e-mail onde constam todas as informações sobre as condições de permanência dos seus dados pessoais, quando houver vagas, e com as orientações sobre os canais para imediata exclusão quando for de seu interesse, não havendo prazos nem limitações ao pedido de exclusão dos dados pessoais.

Quando, de forma voluntária, algum titular de dados pessoais enviar seu currículo por outro canal, não autorizado pela Cirúrgica Santa Cruz , como redes sociais ou para o e-mail diretos de algum colaborar e/ou diretor, o recebedor do e-mail deverá descartar o e-mail e informar o titular de que os currículos somente são recebidos pelo setor de RH e ou deve enviar ao Encarregado de Proteção de Dados pelo e-mail específico lgpd@cirurgicasantacruz.com.br o qual responderá ao titular lhe orientando sobre a manutenção e/ou exclusão de seus dados em banco de dados de currículos.

8. Conscientização e treinamento

A Cirúrgica Santa Cruz possui programa constante de treinamento e revisão das políticas de proteção de dados, fazendo parte da agenda anual da empresa, quando são reafirmados aos colaboradores as boas práticas de privacidade e proteção dos dados pessoais, além da conscientização dos novos contratados no dia da Integração, onde os novos funcionários são acolhidos e recebem a Política de Privacidade e Proteção de Dados o Código de Boas Práticas em Proteção de Dados Pessoais, e um treinamento específico sobre a Lei Geral de Proteção de Dados.

9. Desligamento de funcionários

Em caso de desligamento de funcionários a *Cirúrgica Santa Cruz* possui um processo voltado a garantir a privacidade dos dados pessoais dos funcionários desligados disponibilizando através do setor de TI acesso aos arquivos das estações de trabalho para coleta e eliminação de eventuais arquivos da sua esfera pessoal (em regime de exceção, visto que os funcionários não são autorizados a utilizar os dispositivos móveis e as ferramentas de e-mails para fins pessoais).

Os dados pessoais dos ex-funcionários serão mantidos junto ao setor de Recursos Humanos para fins de garantir o cumprimento das obrigações legais e regulatórias, garantir o exercício de direito das partes quando esta se prorrogar no tempo em razão de demandas judiciais, para o exercício de regular de direitos em processos judiciais, administrativos e/ou arbitrais, e para todos os fins que representem o interesse legítimo do controlador e as garantias dos direitos dos titulares.

Para proteção dos dados pessoais que o antigo funcionário teve acesso, será feita a imediata restrição dos acessos aos dados pessoais que tratava e/ou poderia tratar em razão do desempenho de sua atividade, esta prática se dará pelo bloqueio e/ou eliminação de senhas; A empresa comunicará por meios eletrônicos aos demais funcionários sempre que houver um desligamento e/ou contratação de funcionários novos, para fins de evitar o acesso e o compartilhamento indevido de informações com pessoas não autorizadas; Quando pertinente a função, a empresa poderá comunicar aos clientes e parceiros de negócios, de acordo com a indicação do *Comitê de Privacidade e Proteção de Dados Pessoais*.

10. Tratamento de mídias móveis

A empresa adota política própria de procedimentos a serem adotados para o gerenciamento de mídias que tem como objetivo prevenir a divulgação não autorizada, modificação e remoção ou destruição da informação contendo dados pessoais.

A empresa possui seus arquivos em nuvens que permitem o compartilhamento entre toda a equipe, de acordo com o nível de acesso de cada profissional, e a regra é pela não utilização de mídias móveis, os casos de exceção seguirão o seguinte padrão;

a) quando necessário baixar arquivos (download) de arquivos que estão na nuvem que contenham dados pessoais deve se fazer a exclusão da máquina imediatamente após a utilização;

b) quando necessário para realizar correções de erros, atualizações e melhorias, somente o setor de TI poderá realizar a operação e sempre ocorrerá com base em dados anonimizados, havendo exceções neste processo os dados salvos em mídia deverão ser imediatamente excluídos após o uso.

c) quando necessário à utilização de mídias móveis fora do contexto da empresa, considerando-se neste contexto as atividades, deve ser requerida autorização junto ao setor de TI e comunicado ao Encarregado de Proteção de Dados, e observadas as regras deste código para à ***Política de Uso de dispositivos móveis.***

d) a utilização de mídias removíveis não é praticada na empresa e a mesma possuiu sistemas em todas as máquinas que bloqueia o acesso a conexão de dispositivos USB.

e) o descarte de mídias removíveis deve ser precedido de uma checagem para confirmação de que não há nenhum conteúdo salvo, e deve ser feita de forma segura, em caso de dúvidas deve-se buscar orientação junto ao Encarregado de Proteção de Dados.

f) as mídias removíveis, quando necessárias e autorizadas pelo TI, serão armazenadas em local seguro, preferencialmente com chaves, sempre que nelas conter dados pessoais.

11. Controle físico do ambiente

A Cirúrgica Santa Cruz , possui em sua sede, filial e escritórios, um nível de segurança física desejável, com portaria de identificação, os visitante só acessam as dependências da empresa devidamente acompanhado do funcionário e/ou diretor que o convidou, até a chegada do responsável todos os terceiros aguardam na sala da recepção, não sendo permitida a entrada desacompanhado.

A empresa possui câmeras de monitoramento com a finalidade de segurança pessoal dos funcionários e terceiros que circulam pela empresa, como também para assegurar que pessoas não autorizadas acessem locais não permitidos e dispositivos que possam conter informações críticas e dados pessoais.

Os setor de Recursos humanos possui armário com chave para maior segurança das pastas que contém os dados de seus funcionários e terceiros, o qual possui nível de acesso e só pode ser aberto por pessoa autorizada pelo setor de recursos humanos.

12. Manutenção de equipamentos

A manutenção de equipamentos é realizada pelo setor de TI, somente em casos excepcionais as maquinas são enviadas para fora da empresa. Pelo modelo de trabalho que privilegia a manutenção dos arquivos em nuvem, os dispositivos eletrônicos da Cirúrgica Santa Cruz em rega não possuem dados pessoais.

Em caso de exceção, onde os equipamentos tiverem que ser encaminhados para conserto em um prestador de serviços especializado fora da empresa, este procedimento deve ser realizado pelo setor de TI que deve comunicar o Encarregado de Proteção de Dados para que o serviço possa ser executado por terceiros, neste caso o Encarregado de Proteção de Dados se deverá aprovar a empresa terceira indicada de acordo com seu nível de adequação a lei nº 13.709/18.

Quando houver necessidade de manutenção em dispositivos eletrônicos, o funcionário responsável pelo dispositivo deverá checar seu equipamento para garantir que não houve algum salvamento (download), antes de entrega-lo ao setor de TI.

13. Tela/Mesa limpa

Para garantir a privacidade e proteção dos dados pessoais a empresa adota o procedimento onde todos devem manter os computadores com suas telas bloqueadas quando não estiverem no uso, ou desligados de acordo com a conveniência e dinâmica das atividades.

No tratamento de dados pessoais em meio físico os referidos documentos não devem ser deixados sobre as mesas, balcões e ou locais de acesso e circulação de público, quando não estiverem em uso pelo funcionário e/ou sua vigilância. Sempre que possível guardar em local seguro, gaveta e ou arquivos com chaves.

14. Descarte

Os documentos físico contendo dados pessoais devem ser triturados, os setores são responsáveis por organizar uma caixa de coleta, a qual deve ser encaminhada para descarte seguro, conforme agendamento com o EPD sempre que necessário.

15. Do Backup

A Cirúrgica Santa Cruz para fins de manter a integridade, confidencialidade e proteção dos dados pessoais adota a prática de armazenamento de backups dos servidores e do sistema NL, os quais são feitos em nuvem e em meio físico (HD Externo).

16. Compartilhamento de informações

Toda e qualquer informação contendo dados pessoais as quais o funcionário tiver acesso no exercício de sua atividade laboral, seja de colegas, clientes, fornecedores, colaboradores, prestadores de serviços e/ou terceiros em geral, só podem ser utilizados e/ou compartilhado para desempenho da atividade para qual foi contratado, sendo expressamente proibido sua divulgação e/ou compartilhamento, ainda que no âmbito familiar; Sendo esta informação considerada sigilosa e a violação desta regra será considerada violação ao contrato de trabalho, podendo gerar a demissão por justa causa e/ou a rescisão do contrato em caso de terceiros, prestadores de serviços, estagiários, aprendizes e/ou outro vínculo que o violador ostentar naquele momento.

III - Aprovação

Nesta seção o objetivo é formalizar a aprovação do CBPPDP por meio da obtenção das assinaturas do Encarregado de proteção de dados pessoais e pelas pessoas que representam o agente de tratamento. O CBPPDP deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela instituição.

Responsável:
Jeferson Schuster

DPO/Encarregado(a) de dados:
Fabiane Rush