SUMÁRIO

1 OBJETIVO 3

2 CAMPO DE APLICAÇÃO 4

3 DOCUMENTAÇÃO DE REFERÊNCIA 4

4 DESENVOLVIMENTO 54

4.1 Avaliação e gestão de riscos 5

4.2 Classificação e controle dos ativos 5

4.3 Segurança em recursos humanos 6

4.3.1 Antes da contratação 6

4.3.2 Durante a contratação 7

4.3.3 Encerramento e mudança da contratação 7

4.4 Segurança física e do ambiente – áreas seguras 87

4.5 Segurança em equipamentos 8

4.6 Tecnologia da informação 9

4.6.1 Proteção da rede 9

4.6.2 Gestão de incidentes de segurança da informação 10

4.6.3 Cópia de segurança 10

4.6.4 Controle de acesso lógico 10

4.6.5 Segregação de funções 10

4.6.6 Captura remota 1110

4.6.7 Criptografia 11

4.6.8 Sincronização dos relógios 11

4.6.9 Reutilização ou descarte seguro de equipamentos 11

4.7 Gestão e guarda da informação 11

4.8 Informações pessoaisutilizadas ..... 12~~11~~

4.9 Serviços de terceiros..... 14~~13~~

4.10 Troca de informações 14

4.11 Gestão de incidentes de segurança da informação e comunicação de incidentes ..... 15~~14~~

4.12 Planejamento da continuidade de negócios plano de continuidade de negócios..... 15

4.13 Conformidade..... 16~~15~~

4.14Estrutura da Documentação 16

5 RESPONSABILIDADES ..... 17~~16~~

6 MUDANÇAS NA POLÍTICA E HISTÓRICO DAS REVISÕES 18

1 OBJETIVO

Este documento normativo tem por objetivo determinar a política da segurança da informação da CASA CURUMIM e suas diretrizes.

A Política de Segurança da Informação tem como objetivo “prover uma orientação e apoio da direção para a segurança da informação, de acordo com os requisitos do negócio e com as leis e regulamentações relevantes”(ABNT NBR ISSO/IEC 27002).

A CASA CURUMIM visa atingir um alto padrão de Segurança da Informação. A preocupação com a Segurança da Informação é comum aos níveis de gestão e um compromisso individual de todos.

A CASA CURUMIM é comprometida com a confidencialidade, integridade e disponibilidade de todos os ativos físicos e lógicos de informação da clínica, garantindo que os requisitos legais, operacionais e contratuais sejam cumpridos e para tanto orienta as seguintes diretrizes:

- Garantir o cumprimento da legislação em vigor, regulamentos e documentos normativos pertinentes.
- Cumprir os requisitos de confidencialidade, integridade e disponibilidade através de funcionários da CASA CURUMIM, fornecedores e outras partes envolvidas.
- Estabelecer controles para proteger os sistemas de informação da CASA CURUMIM contra roubo, invasão e outras formas de danos ou perdas, incluindo entre outras: dados de caráter pessoal e de negócios.
- Orientar gestores, colaboradores, terceirizados, e participantes a manter a responsabilidade e conhecimento sobre segurança da informação, a fim de minimizar o risco de incidentes de segurança.

- Assegurar que a CASA CURUMIM seja capaz de continuar a oferecer serviços mesmo que ocorram incidentes de segurança da informação que possam vir a impactar o negócio, garantindo a disponibilidade e confiabilidade da infraestrutura de rede e serviços .
- Cumprir os padrões internacionais de segurança da informação, por exemplo, ISO/IEC 27001, quando aplicável.
- Assegurar que os prestadores de serviços estejam em conformidade com as necessidades e requisitos de segurança da informação da CASA CURUMIM.
- Assegurar um nível aceitável de segurança para acessar sistemas de informação remotamente ou por meio de dispositivos móveis.
- Os documentos complementares, ligados à segurança da informação, devem contribuir com medidas relativas aos riscos e seus possíveis impactos.

2 CAMPO DE APLICAÇÃO

Esta política se aplica a todos os funcionários da CASA CURUMIM.

3 DOCUMENTAÇÃO DE REFERÊNCIA

ISO/IEC 27001 Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da Segurança da informação – Requisitos.

ISO/IEC 27002 Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação.

ISO/IEC 27005 Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação.

4 DESENVOLVIMENTO

A segurança da informação na CASA CURUMIM deve ser assegurada pela política em conjunto com documentos complementares, incluindo, mas não se limitando às normas e procedimentos de segurança.Visando desta forma cumprir a finalidade do tratamento de dados na CASA CURUMIM, em conformidade com as legislações.

A fim de garantir as operações de da CASA CURUMIM, mesmo depois de incidentes graves, deve ser assegurada a disponibilidade de planos de continuidade, procedimentos de backup, proteção de sua rede de trabalho, sistemas e controles de acesso à informação, gestão de incidentes e relatórios.

A violação desta política e dos relevantes requisitos de segurança constitui uma quebra de confiança entre o usuário e a CASA CURUMIM, passível de sanções disciplinares e contratuais.

4.1 Avaliação e gestão de riscos

Uma avaliação global dos riscos dos sistemas de informação deve ser realizada anualmente. As avaliações de risco devem identificar, quantificar e priorizar os riscos de acordo com os critérios relevantes para riscos aceitáveis.

As avaliações de risco devem ser realizadas quando forem efetuadas mudanças que afetam a segurança da informação. Métodos reconhecidos para avaliar os riscos devem ser empregados, como a ISO/IEC 27005 ou um padrão alternativo aplicável e adequado.

Se uma avaliação de risco revelar riscos inaceitáveis, medidas devem ser tomadas para reduzir o risco a um nível aceitável.

4.2 Classificação e controle dos ativos

A classificação a seguir engloba os ativos de informação (lógicos) e os ativos físicos. A informação coletada, tratada e armazenada pela CASA CURUMIM deve ser classificada em uma das quatro categorias de confidencialidade a seguir:

- Reservada

A informação com o mais alto nível de confidencialidade. A divulgação não autorizada da informação reservada pode acarretar consequências para a credibilidade e continuidade de negócios. O acesso é restrito e controlado.

- Restrita

Informações sensíveis, às quais somente deve ter acesso controlado um grupo reduzido de pessoas.

- Interna

Informações disponibilizadas para acesso somente pelos funcionários da CASA CURUMIM.

- Pública

Informação que pode ou deve ser disponibilizada ao público geral através dos canais de comunicação da CASA CURUMIM.

Os documentos com informações sensíveis devem ser claramente rotulados quanto à sua classificação de confidencialidade.

Deve haver o armazenamento eletrônico seguro de documentações críticas.

4.3 Segurança em recursos humanos

4.3.1 Antes da contratação

Devem ser descritas as responsabilidades de segurança para cada função dos funcionários e prestadores de serviços.

Um termo de confidencialidade deve ser assinado pelos funcionários, prestadores de serviços ou outros que possam ter acesso à informação confidencial e/ou interna.

Os critérios de acesso à plataforma de Tecnologia da Informação devem ser aceitos por todos os funcionários e terceiros, formalmente.

4.3.2 Durante a contratação

Todos os funcionários e terceiros devem receber treinamento e atualização adequados sobre a política e os procedimentos de segurança da informação.

As violações da política de segurança da informação e as premissas que a acompanham normalmente resultarão em sanções disciplinares, dependendo das leis vigentes e das condições de trabalho na CASA CURUMIM.

Equipamentos de informática de terceiros só podem ser conectados às redes da CASA CURUMIM quando expressamente permitido pela área de Tecnologia da Informação, com autorização da Diretoria.

A utilização de infraestrutura de Tecnologia da Informação da CASA CURUMIM para atividades pessoais não é permitida em nenhuma circunstância.

4.3.3 Encerramento e mudança da contratação

A responsabilidade pelo término do contrato de trabalho ou mudança nas atividades funcionais deve ser claramente definida e cumpridas as ações pertinentes quanto ao nível de acesso aos sistemas da CASA CURUMIM.

Os ativos da CASA CURUMIM em poder de funcionários, devem ser devolvidos quando não forem mais necessários para o uso ou na rescisão contratual.

A comunicação em caso de rescisão de contrato ou mudança de atividades deve ocorrer por meio de procedimentos estabelecidos no setor Administrativo.

4.4 Segurança física e do ambiente – áreas seguras

Equipamentos de informática e informações que requeiram proteção devem estar situados em áreas fisicamente seguras. As áreas seguras devem ter controle de acesso adequado para garantir que somente as pessoas autorizadas tenham acesso.

As áreas de segurança devem ser demarcadas nas plantas baixas ou explicitamente descritas em um documento separado.

Todo o espaço utilizado pela CASA CURUMIM deve ser protegido, por meio de sistemas de segurança adequados, incluindo registros de auditoria apropriados.

As áreas críticas de segurança devem ser apropriadamente protegidas com equipamentos de prevenção, alarmes, combate contra incêndio e agua.

Testes simulados de resposta a incêndios devem ser realizados regularmente.

Todas as portas externas e janelas devem ser fechadas e trancadas no final do dia de trabalho.

O Coordenador Administrativo é reponsável pela aprovação do acesso físico aos ambientes de segurança da empresae deve garantir que o trabalho realizado por terceiros em áreas de segurança seja apropriadamente monitorado e documentado.

Qualquer funcionário que autorizar o ingresso de visitantes na empresa, torna-se responsável pela supervisão destes durante toda a sua permanência na empresa.

4.5 Segurança em equipamentos

Equipamentos de processamento de dados com riscos classificados como "alto", devem ser protegidos contra ameaças ambientais (incêndio, inundação, variações de temperatura, etc.). A classificação dos equipamentos deve ser baseada em avaliações de risco.

As informações classificadas como "sensíveis" não devem ser armazenadas em equipamentos móveis (por exemplo, laptops, telefones celulares, cartões de memória, pen drive, etc.). Caso seja necessário o armazenamento de informações sensíveis em equipamentos portáteis, estas devem ser protegidas por senha e criptografia, em conformidade com as diretrizes da área de TI e área de Segurança da Informação.

Os equipamentos móveis devem ser transportados como bagagem de mão durante viagens.

4.6 Tecnologia da informação

A área de T.I. deve assegurar que a documentação dos sistemas de T.I. esteja de acordo com as normas e procedimentos da CASA CURUMIM. Os procedimentos devem ser documentados e a documentação deve ser atualizada imediatamente após as mudanças significativas.

4.6.1 Proteção da rede

Software especializado para proteção deve ser utilizadopelo T.I., através de procedimentos aprovados para que garanta a segurança da informação digital da CASA CURUMIM.

Visando a proteção da rede, devemser aplicadas as ações a seguir:

- Bloqueio de Scripts Maliciosos;
- Restriçãono firewall local;
- Varredura e identificação de vulnerabilidades em equipamentos de rede e servidores;
- Antispam em e-mails;
- Controle de proteção de recebimento de malwares por e-mails;
- Filtro de Internet nas máquinas;

- Implementar controles adicionais tais como: bloqueios à páginas que possam causar a saída não autorizada de informação;
- Antivírus e Proteção.
- Realizar o monitoramento de máquinas e servidor;
- Manter ativado Sistema de detecção de Invasão;

4.6.2 Gestão de incidentes de segurança da informação

Deve haver responsável por monitorar ataques DDOS, manter integridade dos sistemas de monitoração e proteção de eventuais ameaças.

4.6.3 Cópia de segurança

O Backup deve ser realizado diariamente pelo T.I., utilizando o Dropbox para armazenamento;

4.6.4 Controle de acesso lógico

O login de Administrador deve ser o único com acesso privilegiado;

Deve haver a remoção ou bloqueio imediato dos acessos do usuário com o seu desligamento da empresa;

Todos os pedidos de acesso ao servidor devem ser controlados pelo responsável pelo T.I. e solicitados pelo Coordenado Administrativo;

Para cada usuário será criado login e senha individual;

4.6.5 Segregação de funções

O acesso a áreas de rede e programas deve ser controlado de acordo com a área e o trabalho executado pelo usuário

4.6.6 Captura remota

- Somente a empresa terceira contratada para gerir a tecnologia da informação tem acesso às máquinas para acesso remoto sem a necessidade de pedido de autorização. Todos os outros devem solicitar permissão a esta empresa, com autorização do Coordenador Administrativo;

- Todos os procedimentos remotos devem ser gravados em vídeo e armazenados.

4.6.7 Criptografia

O Servidor deve ser protegido com criptografia de disco.

4.6.8 Sincronização dos relógios

A sincronização dos relógios de todas as estações de trabalho deve ser realizada e conferida habitualmente;

4.6.9 Reutilização ou descarte seguro de equipamentos

A formatação dos dispositivos com informações confidenciais deve ser realizada por profissional habilitado. No caso de dispositivo de armazenamento não poder ser reutilizado, este é destruído fisicamente.

4.7 Gestão e guarda da informação

A Gestão de documentos arquivados deve ocorrer de acordo com procedimento aprovado pelos Sócios.

Deve haver controle de acesso às informações arquivadas, de acordo com o cargo e a finalidade.

Os documentos criados e recebidos, de acordo com os procedimentos internos, devem ser digitalizados e arquivadosdigitalmente em local seguro.

Deve haver guarda segura dos documentos físicos, regida por procedimento aprovado pelos sócios.

Deve haver descarte seguro de documentos do arquivo, respeitando sempre a legislação e a Tabela de Temporalidade Documental aprovada pelos sócios.

4.8 Informações pessoaisutilizadas

O tratamento e uso das informações pessoais coletadas deve estar de acordo com a Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018) e sempre respeitar a finalidade e prevista na coleta das informações.

Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018).

Deve haver Encarregado para tratamento de dados pessoais nomeado aprovado pela Diretoria, além de canal de comunicação que atenda às exigências da Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018).

O titular dos dados pessoais deve ter ciência da coleta de dados e da finalidade para qual são utilizados.OEscritório deve garantir o consentimento do titular através de termos de consetimento ou cláusulas contratuais, fornecidos por escrito ou outro meio, que permita o tratamento de dados pessoais e dados pessoais sensíveis, destacando sempre a finalidade.

O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Eliminar os dados pessoais coletados sempre quando a finalidade for alcançada, e os dados deixarem de ser necessários. A conservação é autorizada somente para cumprimento de obrigação legal ou regulatória peloEscritório.

Os fluxos de trabalho mapeados devem ser atualizados sempre que houver qualquer alteraçãonas rotinas de trabalho.Além dos fluxos, os dados a seguir também devem ser mantidos atualizados:

- Inventário de dados pessoais armazenados;
- Lista de terceiros em que há compartilhamento de dados;
- Quais dados pessoais são utilizados, armazenados e compartilhados em cada fluxo;
- A classificação dos Dados:
    - Dados Pessoais;
    - Dados Pessoais Sensíveis.
- Os sistemas utilizados para tratar, compartilhar e armazenar estes dados pessoais;
- Como as informações pessoais são obtidas;
- Se a CASA CURUMIM é Controlador ou Operador dos Dados Pessoais de acordo com o fluxo;
- Em quais áreas internas as informações pessoais trafegam de acordo com cada fluxo;
- Quais são os dados compartilhados e com quais empresas terceiras de acordo com cada fluxo;
- Como é realizado o compartilhamento com as empresas terceiras;
- Como os dados pessoais utilizados em cada fluxo são armazenados noEscritório;
- Qual o tempo de retenção destes dados pessoais no Escritório;
- Quais dados pessoais são armazenados por empresas terceiras em cada fluxo;

- Qual a base legal utilizada para colher os dados pessoais em cada fluxo;
- Os Gaps de cada fluxo em que há informação pessoal devem ser mantidos atualizados;
- Manter fatores de riscos atualizados.

4.9 Serviços de terceiros

A aquisição e instalação de equipamentos de TI e software devem ser aprovadas pelos sócios.

Todos os contratos de Terceiros devem incluir:

- Cláusulas de garantida da adequação do terceiro à Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018);
- Requisitos de segurança da informação, incluindo a confidencialidade, integridade e disponibilidade;
- Requisitos para a notificação de incidentes de segurança de partes;
- Uma descrição de como a CASA CURUMIM pode garantir que terceiros estão cumprindo seus contratos;
- Uma descrição do direito da CASA CURUMIM para auditar terceiros.

4.10 Troca de informações

Devem ser estabelecidos procedimentos e controles para proteger o intercâmbio de informações com terceiros, quer sejam clientes ou fornecedores. Os fornecedores devem cumprir com os procedimentos acordados com a CASA CURUMIM.

O uso de e-mail por qualquer funcionário da CASA CURUMIM deve seguir o permitido por seu cargo e função.

Deve haver procedimento aprovado e atualizado, regularizando o uso de whatsapppor funcionários da CASA CURUMIM com fins de trabalho, indicando no mínimo as situações, informações e cargos permitidos.

A CASA CURUMIM tem o direito de acessar os e-mails e outros dados pessoais armazenados na sua rede de acordo com os requisitos legais vigentes.

4.11 Gestão de incidentes de segurança da informação e comunicação de incidentes

Todas as violações da segurança, juntamente com o uso indevido dos sistemas de informações em desacordo com os procedimentos, devem ser tratadas como incidentes de segurança.

Todos os funcionários são responsáveis por comunicar as violações e possíveis quebras de segurança. Os incidentes de segurança devem ser comunicados à coordenação.

Devem ser desenvolvidos procedimentos para gestão e comunicação de incidentes de segurança.

Os procedimentos devem conter medidas para prevenir a repetição, bem como medidas para minimizar os danos.

O T.I. deve estar familiarizado com os procedimentos para a coleta das evidências de incidentes.

A CASA CURUMIM deve garantir que os procedimentos estejam atualizados.

4.12 Planejamento da continuidade de negócios plano de continuidade de negócios

Quando necessário, devem existir planos de continuidade e contingências que abranjam os sistemas de informação, de infraestrutura críticos e outros essenciais.

Os planos de continuidade do negócio devem ser focados nos riscos operacionais.

Os planos de continuidade devem estar alinhados com todos os planos de contingências e planos gerais da CASA CURUMIM.

Os planos de continuidade devem ser testados regularmente para assegurar a adequação, e que a gestão e os funcionários compreendem a sua execução.

4.13 Conformidade

O Escritório deve garantir o cumprimentode seucódigo de etica e conduta,diretrizes internas, bem como outras diretrizes externas, por exemplo:

As leis e regulamentações trabalhista, relativas ao ambiente de trabalho, horário de trabalho, proteção do emprego, etc.

Regulamentos relacionados às atividades de saúde, ambientais e de segurança nas empresas.

Leis e regulamentações relativas ao tratamento de dados de caráter pessoal.

Legislação aplicável ao setor em que atua.

Requisitos contratuais.

4.14 Estrutura da Documentação

A CASA CURUMIM tem uma estrutura para os documentos que descreve sua arquitetura de segurança:

• A política de segurança da informação, a definição de metas, objetivos, a responsabilidade e os requisitos globais. Adicionalmente, fornece uma visão geral sobre os documentos de governança em matéria de segurança da informação e sua importância.

• Política de gestão de dados visa determinar regras de coleta, finalidade de processamento, compartilhamento, armazenamento e eliminação de dados pessoais.

•

•Procedimentos de segurança e operacionais para a segurança da informação. Contém detalhes relacionadas à implantação e evidências da aplicação.

5 RESPONSABILIDADES

Posição	Responsabilidade
Sócios	Tem a responsabilidade geral pela gestão dos valores da CASA CURUMIM de forma eficaz e satisfatória, em conformidade com a legislação em vigor, requisitos e contratos.
Empresa tercerizada TI	Tem a responsabilidade executiva pela segurança da informação nas conexões com sistemas de TI e infraestrutura. Realizar os procedimentos de backup que garantam que informações críticas não sejam perdidas.
Administrativo	Tem a responsabilidade executiva pela segurança da informação relacionada com os sistemas de RH, Financeiro e Administrativo e segurança física conforme consta neste documento.
Funcionários, Estagiários	Tem a responsabilidade pela segurança da informação relacionada com os sistemas que armazenam dados dos processos jurídicos e segurança física conforme consta neste documento.
Administrador de sistema	Os administradores de sistemas junto com a área de TI são pessoas que gerenciam os sistemas de informação da CASA CURUMIM e/ou as informações confiadas à empresa por outras partes. Cada tipo de informação e sistema pode ter um ou mais administradores. Estes são responsáveis por proteger as informações, incluindo a

	implementação de sistemas de controle de acesso a fim de proteger a confidencialidade. Eles irão executar, operar e manter os sistemas de segurança, de acordo com a política. O administrador de sistema deve definir quais usuários ou grupos terão o acesso autorizado à informação e em que consiste o uso desta informação. Cada sistema pode ter mais de um administrador do sistema.
Usuários	Todos os usuários são responsáveis por familiarizar-se e cumprir com os regulamentos de segurança da informação da CASA CURUMIM. Questões relacionadas com a administração de vários tipos de informação devem ser submetidas ao proprietário da informação, ou ao administrador do sistema.
Consultores e parceiros contratuais e Prestadores de Serviços	Parceiros contratuais e consultores contratados devem assinar um acordo de confidencialidade antes de acessar informações confidenciais e Termo de Privacidade. O proprietário do sistema é responsável por garantir que isto seja implementado.

6 MUDANÇAS NA POLÍTICA E HISTÓRICO DAS REVISÕES

A CASA CURUMIM está sempre buscando melhorar os serviços prestados e a forma como opera, e esta Política pode passar por atualizações para refletir as melhorias realizadas. Desta forma, recomenda-se a visita periódica desta página para que se tenha conhecimento sobre as modificações efetivadas.

Versão	Data de início da vigência	Modificações	Elaborado por:	Revisado por:
01	07/01/2022	Documento inicial.		

Aprovado por _____

Nome:

Sócio proprietário e administrador da Clínica Curumim