1. APRESENTAÇÃO

"Não devemos pedir aos nossos clientes que façam um equilíbrio entre privacidade e segurança. Precisamos oferecer-lhes o melhor de ambos. Em última análise, proteger os dados de outra pessoa é proteger a todos nós" Tim Cook, CEO da Apple.

Esta Política de Segurança da Informação poderá ser atualizada, razão pela qual a MADRID SAÚDE recomenda a consulta periódica.

- **DPO NOMEADO**: GARABED APRACHMIAN JUNIOR – SÓCIO ADMINISTRADOR - E-MAIL: dpo@madridsaude.com.br
- **CANAL DE COMUNICAÇÃO LGPD**: dpo@madridsaude.com.br ou www.madridsaude.com.br/canaldecomunicacaolgpd
- **CANAL DE DENÚNCIA**: http://tocomply.com.br/aviso.html

As informações da MADRID SAÚDE de natureza técnica, operacional, comercial, jurídica ou de qualquer forma relacionada a suas atividades, as informações compartilhadas pelos seus clientes de qualquer natureza (em conjunto, "Informações, que viabilizam suas operações enquanto empresa de Distribuição de OPME, registrada na ANVISA, requerem proteção e utilização de forma ética e sigilosa, de acordo com a legislação vigente, evitando-se o mau uso, a perda e a exposição indevida.

O efetivo cumprimento desta Política de Segurança da Informação ("Política") é uma importante ferramenta para combater ameaças a estes ativos que estão sob gestão da MADRID SAÚDE.

A observância dessa Política é fundamental, ainda, para cumprimento das disposições da legislação de proteção de dados vigente no país, em especial, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD). Os termos definidos referentes à proteção de dados nesta Política terão os mesmos significados atribuídos pela LGPD.

2. OBJETIVO

A finalidade desta política é fornecer aos nossos clientes atuais, antigos e potenciais (designados conjuntamente por "clientes" ou "você") uma compreensão geral sobre:

- As circunstâncias sob as quais nós coletamos e processamos os dados pessoais
- Os tipos de Dados pessoais coletados por nós
- Os motivos que levam à coleta destes Dados pessoais
- Como lidamos com os Dados pessoais
- O que é um operador de dados
- Os seus direitos

A Madrid Comércio de Produtos Médicos e Hospitalares Ltda – EPP está empenhada em salvaguardar a privacidade de nossos clientes/você/ que tem seus dados por nós **operados** através do recebimento via portais de cotação, e-mails e outros, da autorização de/para fornecimento de órteses, próteses e materiais especiais necessários a realização do seu procedimento cirúrgico conforme regulamentação da ANS, denominada Rol de Procedimentos e Eventos em Saúde.

Estas autorizações são enviadas a nossa empresa por cooperativas/convênios/operadoras de saúde que você possui contrato e tratadas com total sigilo. Este aviso de privacidade (o Aviso de Privacidade) estabelece nossas práticas de coleta e compartilhamento de dados pessoais para nosso site e se destina a informá-lo sobre as formas pelas quais operamos, tratamos ou usamos seus dados pessoais. Nosso site pode conter links para sites de terceiros.

Se você seguir um link para qualquer desses sites de terceiros, observe que eles têm suas próprias políticas de privacidade e que não temos qualquer responsabilidade ou obrigação por essas políticas ou pelo processamento de seus dados pessoais. Por favor verifique estas políticas antes de enviar qualquer informação pessoal a sites de terceiros.

Esta Política é um conjunto de diretrizes que visa conscientizar e orientar os colaboradores da MADRID SAÚDE para o uso seguro das Informações e Dados Pessoais, garantindo a observância aos princípios inerentes à Segurança da Informação, quais sejam:

a) **Integridade**: salvaguarda da exatidão e correção das Informações e Dados Pessoais, bem como dos métodos de processamento;

b) **Confidencialidade**: garantia que as Informações e Dados Pessoais sejam acessados somente pelas pessoas ou processos que tenham autorização para tal;

c) **Disponibilidade**: Informações e Dados Pessoais estarem acessíveis e utilizáveis sempre que necessário pelos colaboradores autorizados;

d) **Autenticidade**: garantia de que seja identificado e registrado o usuário que está enviando ou modificando as Informações e Dados Pessoais.

Especialmente no que se refere ao Tratamento de Dados Pessoais, compartilhados pelos clientes da MADRID SAÚDE ou de seus próprios colaboradores, essa Política observará os princípios dispostos na Lei Geral de Proteção de Dados, em especial:

a) Boa-fé;
b) Finalidade: realização do Tratamento de Dados Pessoais para propósitos legítimos, específicos, explícitos e informados ao Titular;
c) Adequação: compatibilidade do Tratamento com as finalidades informadas ao Titular;
d) Necessidade: limitação do Tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do Tratamento de dados;
e) Livre acesso: garantia, aos Titulares, de consulta facilitada e gratuita sobre a forma e a duração do Tratamento, bem como sobre a integralidade de seus Dados Pessoais. Sobre as consultas dos Titulares, consultar Política de Privacidade e Proteção de Dados Pessoais da MADRID SAÚDE;
f) Qualidade dos dados: garantia, aos Titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu Tratamento;
g) Transparência: garantia, aos Titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do Tratamento, observados os segredos comercial e industrial;
h) Segurança: utilização de medidas técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
i) Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do Tratamento de Dados Pessoais;
j) Não discriminação: impossibilidade de realização do Tratamento para fins discriminatórios ilícitos ou abusivos;
k) Responsabilização e prestação de contas: demonstração pela MADRID SAÚDE, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de Dados Pessoais e, inclusive, da eficácia dessas medidas.

As orientações aqui apresentadas são os princípios fundamentais e representam como a MADRID SAÚDE exige que as Informações e os Dados Pessoais sejam utilizados. Essa Política se aplica não apenas para o que está armazenado no seu ambiente tecnológico, ou seja, nos computadores, redes ou sistemas utilizados pela MADRID SAÚDE, mas, **também, o que foi impresso ou salvo em mídias digitais e, ainda, o que foi transmitido através de meios eletrônicos ou de conversas em ambientes internos e externos.**

3. DEFINIÇÕES

Profissional da Saúde: significam os profissionais que não sejam colaboradores e trabalhem em uma profissão relacionada às ciências da saúde e para efeito deste procedimento também hospitais, clínicas e planos de saúde, que atuam (direta ou indiretamente) no interesse ou em benefício da MADRID SAÚDE.

Operadoras de Saúde: É a empresa com a qual você/cliente tem contrato assinado e é responsável por fornecer, divulgar ou, de outra forma, tratar Informações pessoais, no contexto de qualquer transação de venda/autorizações de fornecimento de materiais especiais que envolvam, todo ou parte de seu negócio, ou, caso venha a ser exigido ou permitido por lei.

Agente Público: nos termos da Lei nº. 8.429/1.992, sendo todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função em qualquer dos Poderes da União, dos Estados, do Distrito Federal, dos Municípios, de Território, de empresa incorporada ao patrimônio público ou de entidade para cuja criação ou custeio o erário haja concorrido ou concorra com mais de cinquenta por cento do patrimônio ou da receita anual, bem como candidatos a cargos públicos em todas as instâncias (federal, estadual ou municipal e nos poderes executivo, legislativo ou judiciário).

Colaborador(es): significam os funcionários, estagiários, diretores, Sócios e demais representantes da MADRID SAÚDE.

Terceiro(s): significam os profissionais que não sejam colaboradores e empresas contratadas que se apresentam, em nome da MADRID SAÚDE, ou atuam (direta ou indiretamente) no interesse ou em benefício da MADRID SAÚDE, bem como os fornecedores de bens e prestadores de serviços.

Clientes/você/Titular de dados: Pessoa natural a quem se referem os dados pessoais

Dados Pessoais: "Dados pessoais" significa qualquer informação identificada ou identificável relacionada a uma pessoa física ("titular dos dados"); uma pessoa física identificável é aquela que pode ser identificada, direta ou indiretamente, particularmente por referência a um identificador, como um nome, número de identificação, dado de localização, identificador on-line ou por referência a um ou mais fatores específicos relacionados à identidade física, fisiológica, genética, mental, econômica, cultural ou social da referida pessoa física;

Dados Pessoais sensíveis: é todo dado pessoal que pode gerar qualquer tipo de discriminação, tais como os dados sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

4. DIRETRIZES

Como usamos seus dados pessoais:

Nesta seção, definimos as finalidades para as quais usamos os dados pessoais que coletamos através de nosso site e, em conformidade com nossas obrigações sob as legislações de proteção de dados, incluindo a 'Lei Geral de Proteção de Dados' brasileira, identificamos as "bases legais" nas quais nos baseamos para processar seus dados. A Lei Brasileira de Proteção de Dados permite que as empresas processem dados pessoais somente quando o processamento for permitido por "bases legais" específicas estabelecidas por lei (a descrição completa de cada uma dessas bases legais pode ser encontrada aqui).

Operador de dados:

O operador é aquele que realiza o tratamento de dados pessoais em nome do controlador, de uma maneira mais prática, seria aquela empresa contratada pelo controlador para desempenhar um serviço complementar, como é o caso do fornecimento de materiais cirúrgicos que vendemos necessários e imprescindíveis a realização do seu procedimento cirúrgico. Estes são os principais fundamentos legais que justificam nosso uso de seus dados pessoais como OPERADORES DE DADOS:

a) Consentimento: quando você tiver consentido com nosso uso de seus dados através de aceite dado através do contrato assinado de maneira, física ou digital através do aceite no site da empresa controladora de seus dados e que nos utiliza como operadores de qualquer serviço ou produto a ser oferecido a você na realização de um procedimento cirúrgico

b) Execução do contrato: quando seus dados forem necessários para executar o serviço ou entrega de produto que o controlador dos seus dados nos autorizou a realizar mediante contrato assinado com você.

c) Obrigação legal ou regulatória: quando precisarmos usar seus dados para cumprir com nossas obrigações legais ou regulatórias.

d) Interesses legítimos: quando utilizarmos seus dados para atingir um interesse legítimo e nossas razões para utilizá-las superarem qualquer prejuízo a seus direitos de proteção de dados.

e) Reivindicações legais: quando seus dados forem necessários para que possamos defender, processar ou fazer uma reclamação contra o controlador dos seus dados, contra você, contra nós ou contra um terceiro. Para exercer nossos direitos em contratos, procedimentos judiciais, administrativos ou arbitrais.

f) Políticas públicas: Para ajudar governos a implementar políticas públicas previstas em leis ou regulamentos, ou baseadas em contratos, acordos ou instrumentos similares.

g) Proteção da vida: para proteger a vida ou a segurança dos titulares de dados ou de terceiros.

h) Proteção da Saúde: para proteger a saúde, em procedimentos conduzidos por profissionais da saúde ou por entidades de saúde;

i) Prevenção de Fraudes: para garantir a prevenção de fraudes, e a segurança do titular de dados.

5. CONDIÇÕES GERAIS: Transmissão, armazenamento e segurança de seus dados pessoais

Segurança na Internet:

Nenhuma transmissão de dados pela Internet ou site pode ser garantida como segura contra intrusões. No entanto, mantemos salvaguardas físicas, eletrônicas e procedimentais comercialmente razoáveis para proteger seus dados pessoais de acordo com os requisitos legais de proteção de dados. Todas as informações que o convênio/operadora/cooperativa de saúde nos fornece são armazenadas em servidores seguros, em nuvem, através de serviços oferecidos pela WINOV, e são acessadas e utilizadas de acordo com nossas políticas e padrões de segurança.

Limites de armazenamento:

Conservaremos seus dados pessoais pelo tempo necessário para a(s) finalidade(s) de processamento para a(s) qual(is) foram coletados e qualquer outra finalidade vinculada permitida (por exemplo, quando formos obrigados a reter dados pessoais por mais tempo do que a finalidade para a qual os coletamos originalmente, a fim de cumprir certos requisitos regulatórios). Nossos períodos de retenção são baseados em necessidades comerciais, e dados pessoais que não são mais necessários são irreversivelmente anonimizados (as informações anônimas são retidas) ou destruídos com segurança de acordo com nossa política interna de retenção.

Os seus direitos:

Você tem o direito e nossa garantia de não utilização de nenhum de seus dados para utilização em meios de marketing.

Atualização de informações: Aplicaremos esforços razoáveis para manter seus dados pessoais precisos e protegidos em um momento tão sensível. A fim de nos ajudar nisso, você pode nos notificar sobre quaisquer mudanças em seus dados pessoais ou relativos ao procedimento caso seu médico e ou operadora permitam. Se você tiver alguma dúvida em relação ao nosso uso de seus dados pessoais, deve primeiro entrar em contato conosco. Sob certas condições, você tem o direito de nos exigir o seguinte:

a) Confirmação do tratamento de seus dados
b) Acesso e retificação dos dados tratados, se necessário;
c) Deletar, bloquear ou tornar anônimos dados desnecessários, excessivos, pertencentes a você, ou seus dados que sejam processados em violação à lei;
e) Informação sobre o compartilhamento dos dados

Seu exercício desses direitos está sujeito a certas isenções para salvaguardar o interesse público e nossos interesses. Se você exercer algum desses direitos, verificaremos essas exceções e responderemos oportunamente ao seu pedido.

Se você não estiver satisfeito com nosso uso de seus dados pessoais ou nossa resposta a qualquer exercício destes direitos, você tem o direito de reclamar junto à Autoridade Brasileira de Proteção de Dados (ANPD).

6. ABRANGÊNCIA

Esta Política se aplica a todos os colaboradores da MADRID SAÚDE cientificando-os de que os ambientes, sistemas, computadores e redes poderão ser monitorados, em qualquer tempo e circunstância.

É obrigação de cada colaborador se manter atualizado em relação a esta Política e aos procedimentos e normas a ela relacionadas, buscando orientação do seu gestor ou da área de TI sempre que não estiver seguro quanto às diretrizes aqui apresentadas.

Deverá constar em todos os contratos com os colaboradores e parceiros do MADRID SAÚDE, Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de Informações e Dados Pessoais, sob gestão da MADRID SAÚDE. O cumprimento da Política pelos colaboradores e parceiros poderá ser auditado pela MADRID SAÚDE.

7. DIRETRIZES PARA SEGURANÇA DA INFORMAÇÃO

Esta Política define as diretrizes para a Segurança da Informação, visando preservar a integridade, confidencialidade, autenticidade e disponibilidade das Informações e Dados Pessoais, sob gestão da MADRID SAÚDE. Descreve a conduta considerada adequada para o manuseio, controle e proteção contra acessos não autorizados, destruição, modificação e divulgação indevida, seja acidental ou intencionalmente.

7.1 - Propriedade das informações

Todas as Informações produzidas, acessadas, recebidas, manuseadas ou armazenadas pelos colaboradores, como resultado da atividade profissional, bem como, a reputação, a marca e demais ativos são de propriedade e de direito de uso exclusivos da MADRID SAÚDE, sendo, portanto, proibidas as cópias, reproduções ou distribuições sem a devida autorização. As exceções devem ser explícitas e formalizadas.

A utilização da marca, identidade visual e demais sinais distintivos da MADRID SAÚDE, em qualquer veículo de comunicação, inclusive na internet e nas mídias sociais, só poderão ser feitos para atender às atividades profissionais da MADRID SAÚDE.

As Informações compartilhadas pelos clientes da MADRID SAÚDE são de propriedade daqueles, sendo autorizado o uso para execução dos contratos e/ou atividades contratadas. De igual modo, são proibidas as cópias, reproduções ou distribuições sem a devida autorização. As exceções devem ser explícitas e formalizadas.

7.2 - Classificação das Informações

É de responsabilidade da MADRID SAÚDE estabelecer critérios relativos ao nível de confidencialidade das Informações geradas ou recebidas, de acordo com os critérios a seguir:

a) Pública: Informações da MADRID SAÚDE com linguagem e formato dedicado à divulgação ao público em geral, sendo de caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação;
b) Corporativa: Informações cujo conhecimento é de interesse da MADRID SAÚDE, podendo ser divulgada para seus clientes.
c) Uso Interno: Informações de conhecimento exclusivo dos colaboradores da MADRID SAÚDE e deve ser divulgada apenas para o público interno;
d) Restrita: Informações que pode ser acessada somente por colaboradores de áreas previamente definidas em manual específico;
e) Confidencial: Informações crítica para os negócios da MADRID SAÚDE ou de seus clientes, devendo haver indicação do nome ou cargo do colaborador responsável. A divulgação não autorizada dessas Informações pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e/ou criminais.

7.3 - Propriedade dos Dados Pessoais e Canal de Comunicação para Atendimento aos Titulares de Dados

Os Dados Pessoais pertencem à pessoa natural a quem se referem as informações, na condição de Titulares de Dados Pessoais. Todos seus direitos são previstos e assegurados pela Lei Geral de Proteção de Dados Pessoais e deverão ser observados pela MADRID SAÚDE durante o Tratamento destes.

Os Dados Pessoais deverão sempre serem classificados como: de uso interno, restrito e confidenciais. Além de conhecer essa Política, é obrigação do colaborador ter ciência dos termos da Política de Privacidade e Proteção de Dados Pessoais da MADRID SAÚDE, buscando orientação do seu gestor, sempre que não estiver seguro quanto às diretrizes lá apresentadas.

7.3.1 - Canal de Comunicação para Atendimento aos Titulares de Dados

Ao encaminhar mensagens e fornecer os dados que serão armazenados para a finalidade descrita e para fim de dar cumprimento aos direitos dos titulares previstos na LGPD – (lei 13.709/2018), o requerente declara ter conhecimento e concordar com a política de Privacidade da Madrid Saúde e autoriza o tratamento de seus dados para essa finalidade descrita em nossa política de privacidade de dados. **Suas requisições de informações para exercício de diretos como Titular dos dados pessoais podem ser realizadas pelos canais abaixo descritos. Caso seu pedido de informações não seja retornado no período determinado existe também o nosso canal de denúncias que poderá ser recorrido para o atendimento de sua solicitação.**

7.3.2 – Da divulgação e das responsabilidades do DPO nomeado

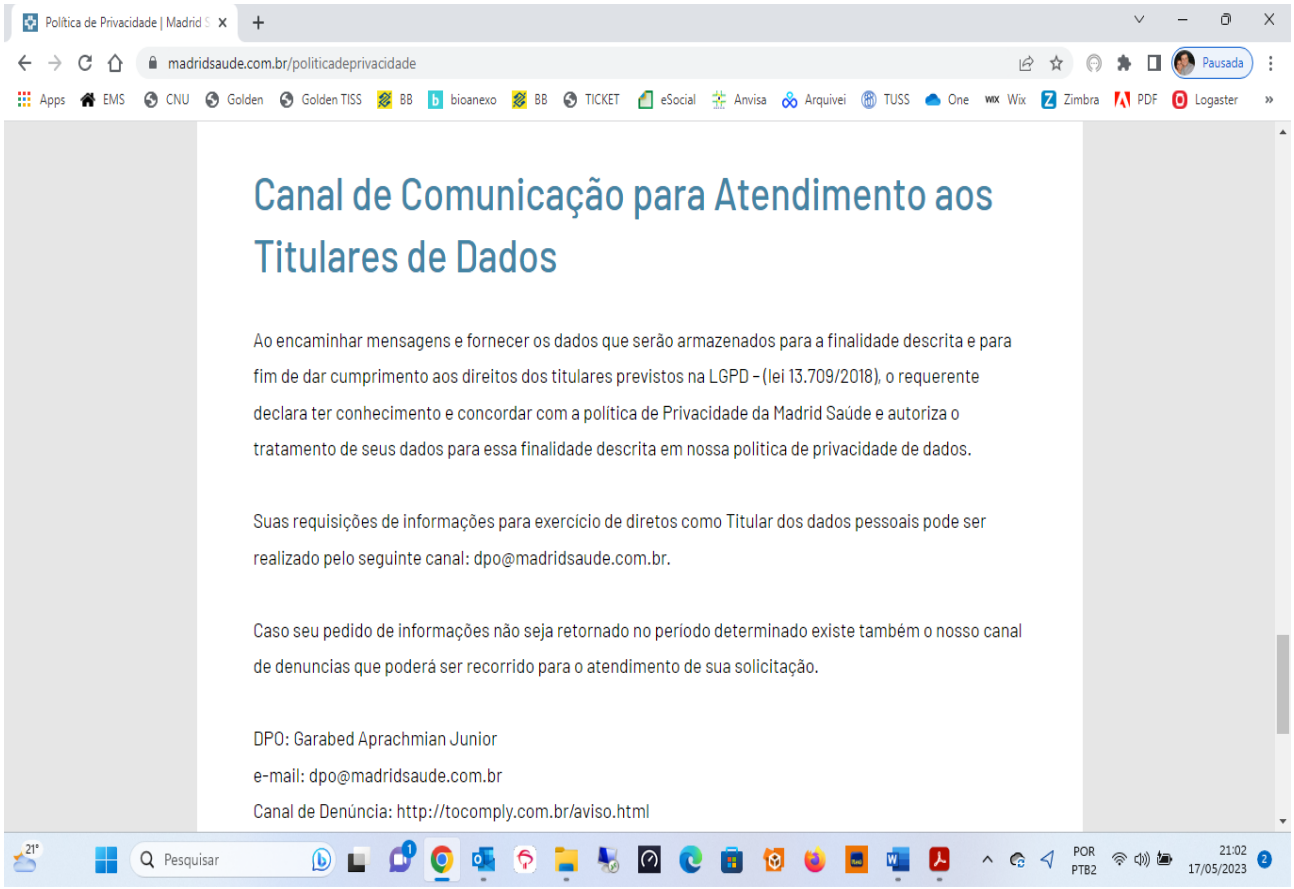
É responsabilidade do DPO nomeado abaixo monitorar, fiscalizar, orientar e fazer a ponte entre os titulares de dados e a Madrid Saúde. Conforme estabelecido pelo art. 41 da LGPD que diz: **O controlador deverá indicar encarregado pelo tratamento de dados pessoais.**

A identidade e as informações de contato do encarregado estão divulgadas publicamente, de forma clara e objetiva, no sítio eletrônico da MADRID SAÚDE: https://www.madridsaude.com.br/canaldecomunicacaolgpd

Dentre as atividades do DPO nomeado estão:

I - Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II - Receber comunicações da autoridade nacional e adotar providências;
III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e
IV - Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

DPO NOMEADO: GARABED APRACHMIAN JUNIOR – SÓCIO ADMINISTRADOR - E-MAIL: dpo@madridsaude.com.br
CANAL DE COMUNICAÇÃO LGPD: dpo@madridsaude.com.br ou www.madridsaude.com.br/canaldecomunicacaolgpd
CANAL DE DENÚNCIA: http://tocomply.com.br/aviso.html



7.4 - Utilização, Guarda e Descarte de Documentos

Documentos que contenham Informações classificadas como uso interno, restrita ou confidencial ou com Dados Pessoais não podem ficar expostos na estação de trabalho, em impressoras, scanner, telas de computadores, áreas comuns, locais de trânsito de pessoas, refeitório e nas salas de reunião. Deve-se observar a exigência e o prazo legal definido em tabela vigente à época, para manutenção dos documentos produzidos em razão de suas atividades. Decorrido o prazo para armazenamento, os documentos devem ser destruídos antes de descartados, mediante autorização prévia do DPO nomeado nesta política/responsável.

Referidos documentos devem ser acondicionados em armários de acesso controlado, sua destruição, quando for o caso, **deverá ser feita por meio de triturador de papel de propriedade da Madrid Saúde, após catalogar documentação a ser destruída.** Caso a MADRID SAÚDE opte por uma empresa de guarda externa deverá emitir Certificado ou Declaração de Destruição Segura dos documentos indicados pela MADRID SAÚDE.

Em relação aos documentos que contenham Dados Pessoais, estes deverão ser tratados de forma adequada e limitada pelo período em que se fizerem necessários para cumprimento do propósito especificado ao Titular de Dados Pessoais. A MADRID SAÚDE reserva-se o direito de manter armazenado uma cópia de todos os processos realizados para seus clientes, incluindo os Dados Pessoais, devendo zelar integralmente pela sua guarda e sigilo, nos termos da legislação vigente, considerando-se os prazos prescricionais dos atos praticados durante a vigência do contrato firmado entre as partes.

O prazo legal vigente na revisão desta política é de 5 anos, contados a partir do exercício seguinte ao que poderia ter ocorrido o lançamento fiscal, conforme Arts. 195 e 174, CTN.

7.4.1 ELIMINAÇÃO SEGURA DE EQUIPAMENTOS, DISPOSITIVOS E MÍDIAS.

As diretrizes, padrões e procedimentos para eliminação segura de equipamentos, dispositivos e mídias que contenham dados sensíveis, estabelecendo controles tecnológicos que apoiem o processo de descarte de mídia, definindo ferramentas de limpeza de mídias removíveis (pen-drive, hard disk – HD Externo, dispositivos móveis corporativos, dentre outros) na MADRID SAÚDE, estão definidas na PP206 – PROCEDIMENTO PREVENTIVO PARA ELIMINAÇÃO SEGURA DE EQUIPAMENTOS, DISPOSITIVOS E MÍDIAS.

7.5 - Backup (Cópias de segurança)

Os backups devem ser realizados por sistemas de agendamento e executados, preferencialmente, fora do horário comercial, período em que não há nenhum ou pouco acesso de usuários ou processos automatizados dos sistemas de informática. Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida, sugestões de melhorias, entre outros.

5. DAS CÓPIAS DE SEGURANÇA (*BACKUPS*)

5.1. As cópias para restauração dos dados serão armazenadas na estrutura vigente do *Data Center* da **CONTRATADA**, a menos que se contrate uma modalidade diferenciada do plano de b*ackup*.

5.2. Para este contrato será fornecido a Solução *Commvault* para *backup* do ambiente do cliente com recursos gerenciados pela **CONTRATANTE** via Portal *Commvault*.

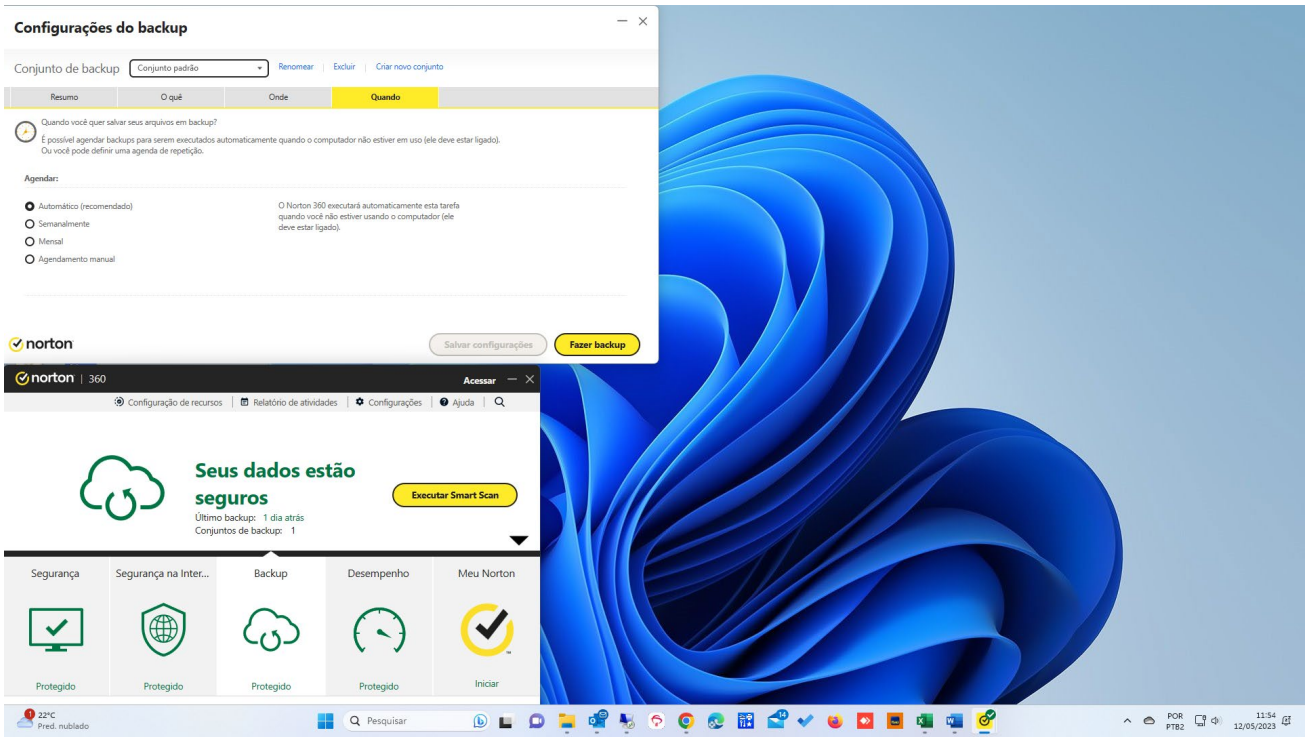
Modelos de retenção

Nível 6 HyperScale Commvault: (15 dias)

- Backup 1 ciclo (Máximo de 7 dias e no mínimo 1 dia) - Área Quente
- Backup incremental diário
- Backup full semanal (Mantendo em área quente 1 backups full)
- Backup 7 dias 1 ciclo (Máximo de 14 dias e no mínimo 7 dias) - Área Fria em Tape Library solução de alta densidade
- Backup incremental diário

Prints acima foram retirados do Contrato de Locação de Servidor Host Cloud que fazem a WINOV SOLUÇÕES EM TECNOLOGIA S.A. e MADRID COMÉRCIO DE PRODUTOS MÉDICOS E HOSPITALARES LTDA – EPP, páginas 18/42.

Além dos backups normalmente realizados no servidor, deverá ser feito backup adicional mantido em dispositivo externo com as informações codificadas (criptografadas) em ambiente seguro para armazenagem fora da MADRID SAÚDE. A rotina implementada de backup deve estar formalmente documentada para consultas e auditorias.



7.6 - Controles de Acesso/Logins

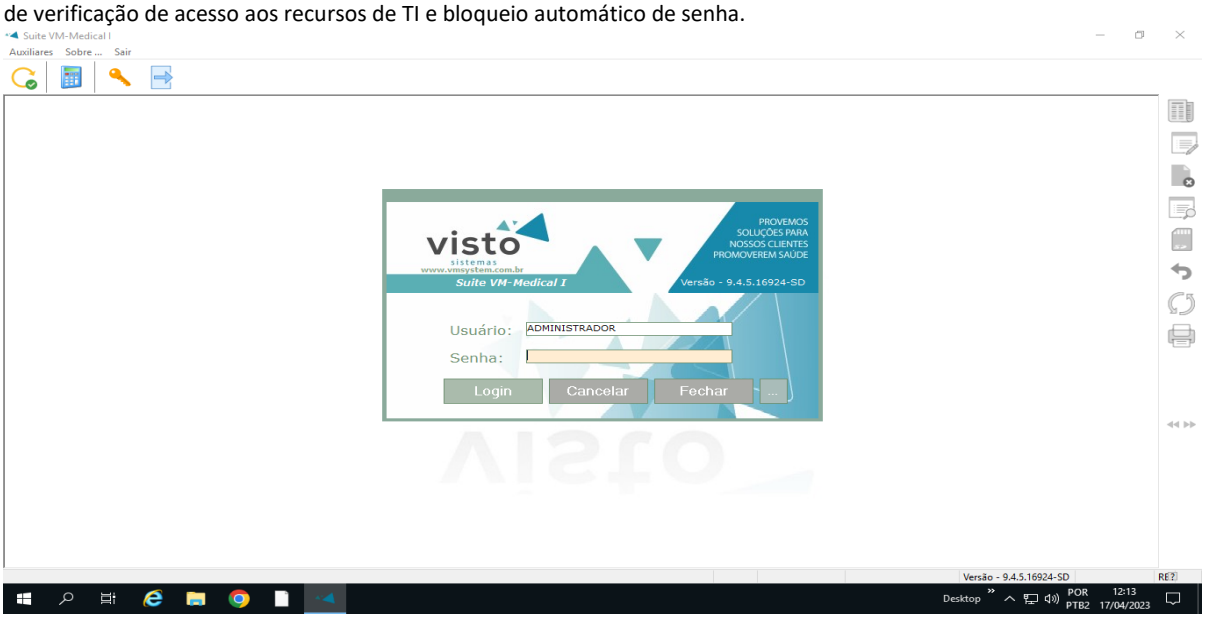
Para cada colaborador da MADRID SAÚDE deverá ser fornecido dispositivos de identificação pessoal, como crachá, códigos de acesso e senhas, os quais, não poderão ser compartilhados, divulgados ou transferidos a outra pessoa. O colaborador é responsável por todas as atividades desenvolvidas por meio de seus dispositivos de identificação pessoal. É vedada, a qualquer colaborador, a utilização de dispositivos de identificação pessoal de outro colaborador mesmo quando cedida por este.

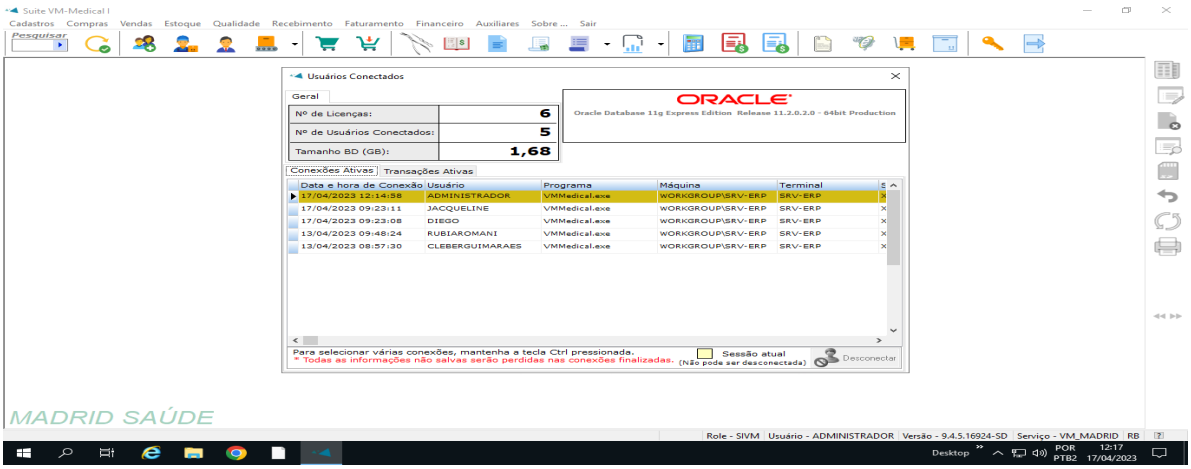
É de responsabilidade de cada colaborador a guarda dos dispositivos de identificação que lhe forem designados, bem como, a memorização de sua própria senha, não devendo anotar ou armazená-las em arquivos eletrônicos sem utilizar um meio de proteção definido pelos gestores e área de TI como, por exemplo, criptografia. As senhas não devem ser baseadas em informações pessoais, como o próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras. As senhas de acesso deverão ser trocadas ao menos semestralmente.Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a MADRID SAÚDE e a legislação (cível e criminal) será dos colaboradores que dele se utilizarem. A concessão de acessos deverá seguir o critério de menor privilégio, no qual os colaboradores tenham acesso apenas às Informações e Dados Pessoais imprescindíveis para o pleno desempenho de suas atividades, de acordo com as classificações dadas pelos gestores.

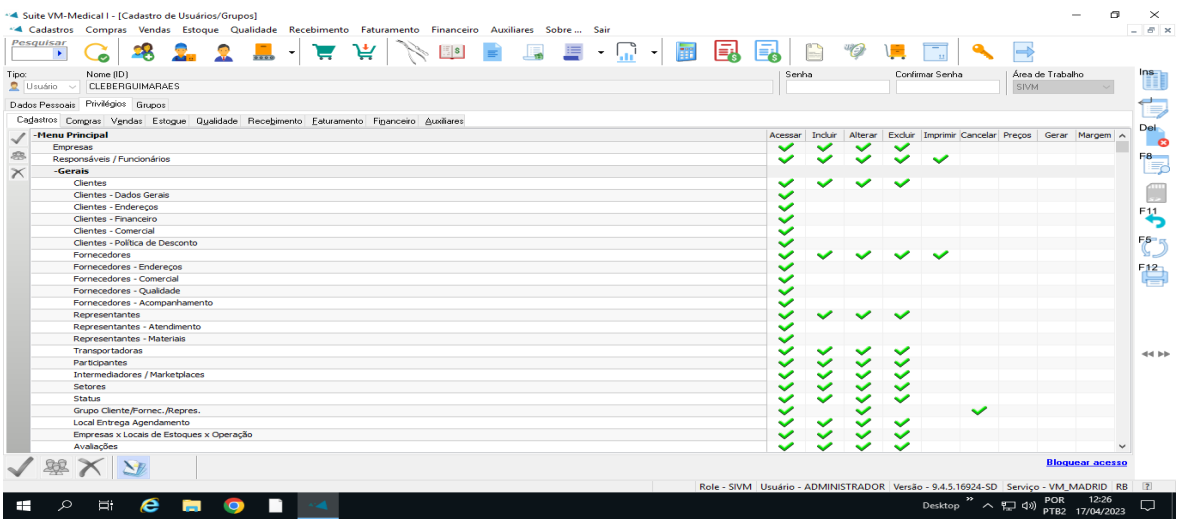
O gestor deverá, através de e-mail, solicitar à equipe de TI inclusões, alterações ou exclusões de acesso a usuários, definindo os serviços que deverão ser incluídos, alterados ou excluídos e justificando quanto à necessidade da solicitação.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, por ocasião do desligamento de qualquer colaborador, o responsável de TI deverá providenciar o imediato cancelamento de todas as suas senhas de acesso a

equipamentos e sistemas corporativos bem como de seu e-mail. A equipe de TI deverá, pelo menos semestralmente, efetuar testes de verificação de acesso aos recursos de TI e bloqueio automático de senha.







7.7 - Segurança do Ambiente Físico

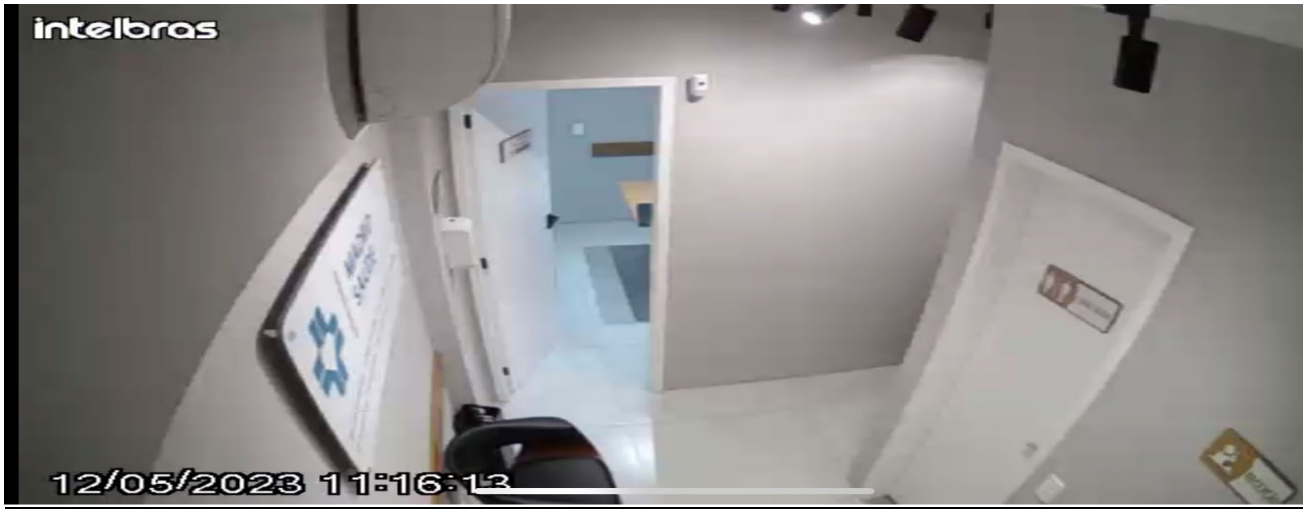
É vedado o acesso de pessoas não autorizadas às instalações da MADRID SAÚDE. O acesso de visitantes à MADRID SAÚDE deverá ser supervisionado por gestor ou colaborador.

É fundamental que, durante a jornada de trabalho e nas dependências da MADRID SAÚDE, os colaboradores utilizem crachá de identificação. As áreas de acesso restrito, somente podem ser acessadas por colaboradores devidamente autorizados.

O acesso às dependências da MADRID SAÚDE com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, para fins de gravação dos ambientes de trabalho só é permitido mediante autorização por escrito do DPO nomeado.

O acesso diário de colaboradores será realizado, após cadastro e autorização da MADRID SAÚDE, na forma de tokens de acesso fornecidos pela empresa VERISURE registrados no relatório de atividades enviado mensalmente pelo fornecedor de segurança corporativa.

Todo acesso será monitorado também pela utilização do aplicativo de monitoramento por câmeras MIBO-INTELBRÁS com funcionamento 24horas por dia, 7 dias por semana com gravação em DVR e nuvem para caso necessário, utilizar a consulta de imagens a qualquer momento.



Não é permitido aos colaboradores tirar fotos, gravar, filmar, publicar elou compartilhar imagens dos ambientes internos da MADRID SAÚDE que possam:

a) Comprometer a segurança dos demais colaboradores;
b) Comprometer o sigilo das Informações e Dados Pessoais;
c) Impactar negativamente a imagem da MADRID SAÚDE, outros colaboradores, clientes, parceiros e/ou visitantes.

7.8 - Mesa Limpa/Tela Limpa

Deve ser seguido o princípio estabelecido na Norma ABNT NBR/ISO/IEC 27.001 da "Mesa limpa/ Tela limpa". Este princípio tem como objetivo a redução dos riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente.

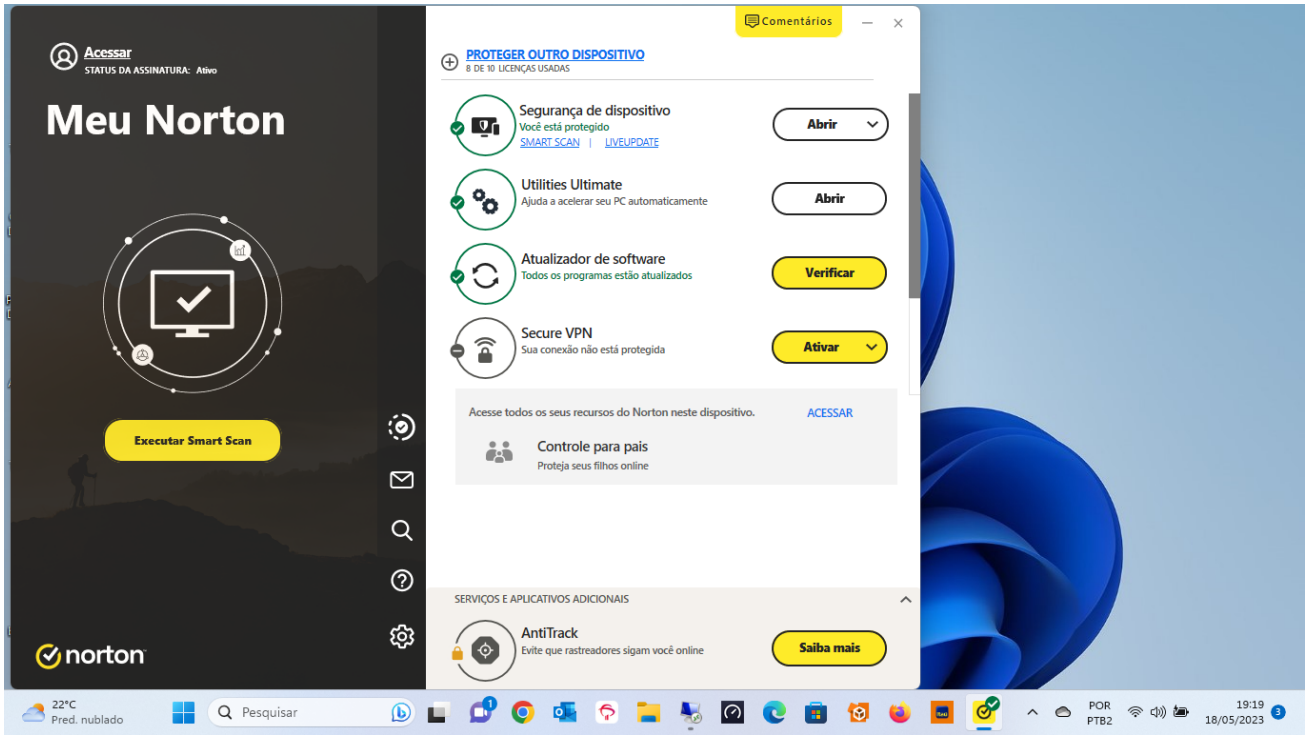
A política de "Mesa Limpa/Tela Limpa" busca resguardar a MADRID SAÚDE, bem como o próprio usuário contra o acesso não autorizado a Informações e Dados Pessoais. Assim, sinteticamente, entre outros:

a) Papéis, anotações e lembretes devem ser mantidos, sempre que possível, fora da superfície da mesa (mesa limpa);
b) Informações restritas ou confidenciais e/ou Dados Pessoais devem ser trancadas em local separado (idealmente em um arquivo, armário ou gaveteiro) quando não necessárias, especialmente quando o ambiente fica vazio;
c) Computadores e notebooks não devem ser deixados autenticados/registrados quando não houver um colaborador junto e devem ser protegidos por senhas e outros controles quando não estiverem em uso (tela limpa);
d) Utilização de protetor de tela que solicite uma senha para acesso deve ser sempre usado;
e) Informações restritas ou confidenciais e/ou Dados Pessoais, quando impressos, devem ser retiradas da impressora imediatamente pelo colaborador que solicitou a impressão;
f) Ao final do dia, ou no caso de ausência prolongada, a mesa de trabalho deve ser limpa; e
g) Todos os documentos e meios eletrônicos, no final do dia de trabalho, devem ser devidamente guardados/organizados, com proteção adequada.

7.9 - Segurança dos Equipamentos

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento da área de TI ou de quem está determinar.

Os sistemas e computadores devem ter versões de software antivírus instalados, ativados e atualizados permanentemente. Em caso de suspeita de incidência de vírus ou problemas de funcionalidade de hardware ou software, o colaborador deverá acionar a área de TI da MADRID SAÚDE. Vide **Evidência do Norton Antivírus.**



Os colaboradores deverão proteger o acesso a seus computadores por meio de tela de bloqueio a ser liberada mediante senha, quando eles não estiverem em uso. Ao final do expediente de trabalho diário, o computador deverá ser desligado.

7.10 - Utilização da Rede

A MADRID SAÚDE possui uma rede integrada de computadores com servidores e um microcomputador para cada colaborador e o acesso à rede da MADRID SAÚDE só poderá ser efetivado após o registro obrigatório de computadores e usuários, de acordo com os sistemas de registro implementados.

O colaborador é responsável pelas atividades realizadas por intermédio de sua conta de usuário e senhas de acesso. Os colaboradores da MADRID SAÚDE não deverão obter ou disponibilizar material sem a licença adequada através da rede.

O usuário é responsável pela própria e devida autenticação nos sistemas de redes disponibilizados pela MADRID SAÚDE, não podendo fornecer e/ou compartilhar seu usuário, senha e/ou acesso à rede com outros usuários. O usuário está comprometido a utilizar as redes públicas e/ou privadas da MADRID SAÚDE para uso exclusivo de atividades relacionadas ao setor no qual o usuário pertence.

É vedada a utilização de proxies que permitam o tráfego de informações a redes privadas externas. Os usuários devem administrar suas pastas, excluindo arquivos desnecessários.

Material sexualmente explícito ou contrário à legislação brasileira não podem ser expostos, armazenados, distribuídos, editados ou gravados, através do uso dos recursos computacionais da rede corporativa da MADRID SAÚDE.

Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos etc.) nos drivers de rede, pois estes ocupam espaço comum limitado. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente, sem prévia comunicação.

7.11 – Descrição e utilização dos Sistemas Corporativos:

Os Sistemas Corporativos são os sistemas utilizados na gestão da MADRID SAÚDE, os quais buscam trazer maior transparência, tempestividade e confiabilidade para as informações, abrangendo todos os seguimentos da administração da empresa e permitindo o gerenciamento isolado de cada parte e a interligação desta com o todo, produzindo relatórios analíticos, sintéticos e estatísticos, sendo acessados por meio de uma rede interna ou externa. É expressamente proibida a divulgação e/ou o compartilhamento indevido das informações contidas nos Sistemas Corporativos da MADRID SAÚDE. Todos os usuários dos ativos de Informações de propriedade da MADRID SAÚDE, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse dele, mantendo conduta profissional. O acesso às informações contidas nos Sistemas Corporativos deve ser efetuado sempre através de identificação segura (chave e senha e para cada usuário serão atribuídas permissões específicas, por módulo e/ou operação). A concessão de acesso às bases de dados para prestadores de serviço e colaboradores deverá sempre seguir o critério do menor privilégio possível.

7.11.1 - SERVIDOR HOST CLOUD: Evidência: cláusula 13.6., pag.: 11 – contrato WINOV X MADRID.

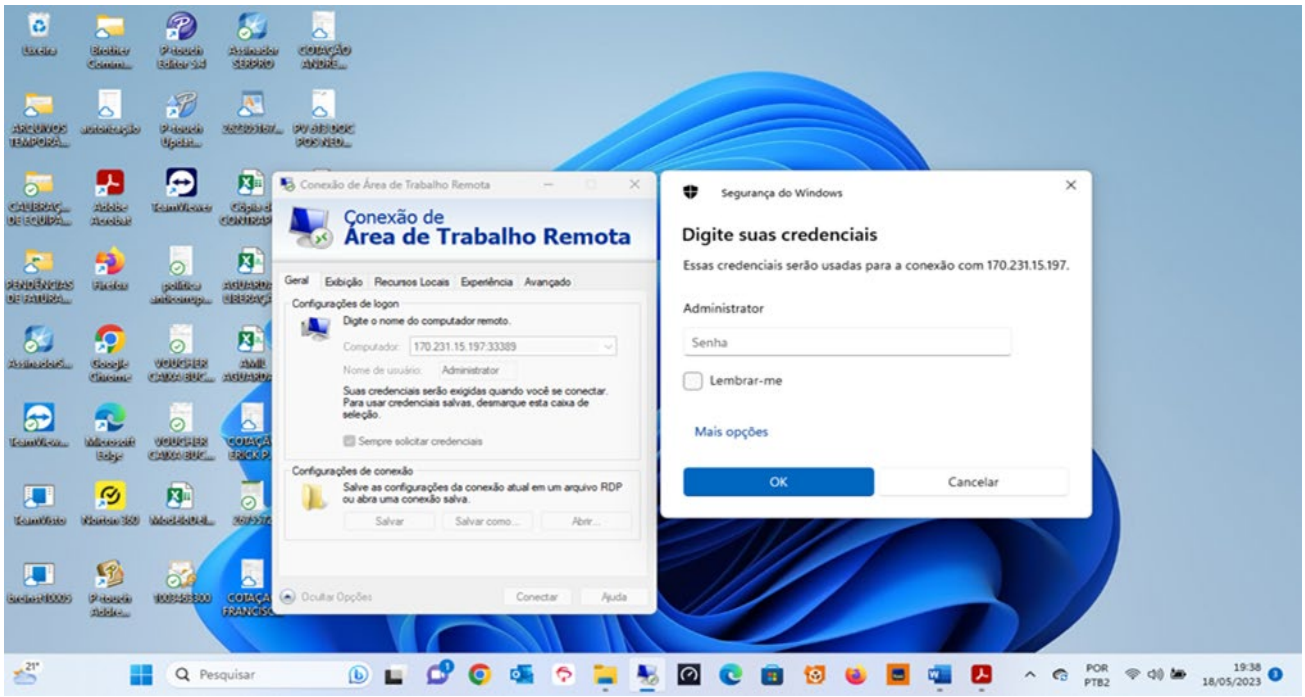
É feito através de acesso identificado com senha, alterada mensalmente sob contrato com a WINOV SOLUÇÕES EM TECNOLOGIA S.A., Constitui objeto do presente contrato a locação de servidor CLOUD COMPUTING , denominado HOSTCLOUD (“Solução Winov”) , bem como a customização e implantação deste, de acordo com as cláusulas e condições descritas na proposta comercial e no ANEXO I - DOS SERVIÇOS (o qual se constitui parte integrante e indissociável deste contrato como se aqui estivesse transcrita em todos os seus termos). As partes deste contrato acordaram que, sobre o tratamento das informações confidenciais, elas obrigam-se a restringir o acesso e manter sigilosas as informações confidenciais transmitidas entre elas, divulgando-as somente com aqueles funcionários e/ou prepostos que delas necessitam para o desempenho das funções que lhe sejam atribuídas por força do presente contrato, firmando com eles, em termo próprio, compromisso de sigilo quanto às informações recebidas.

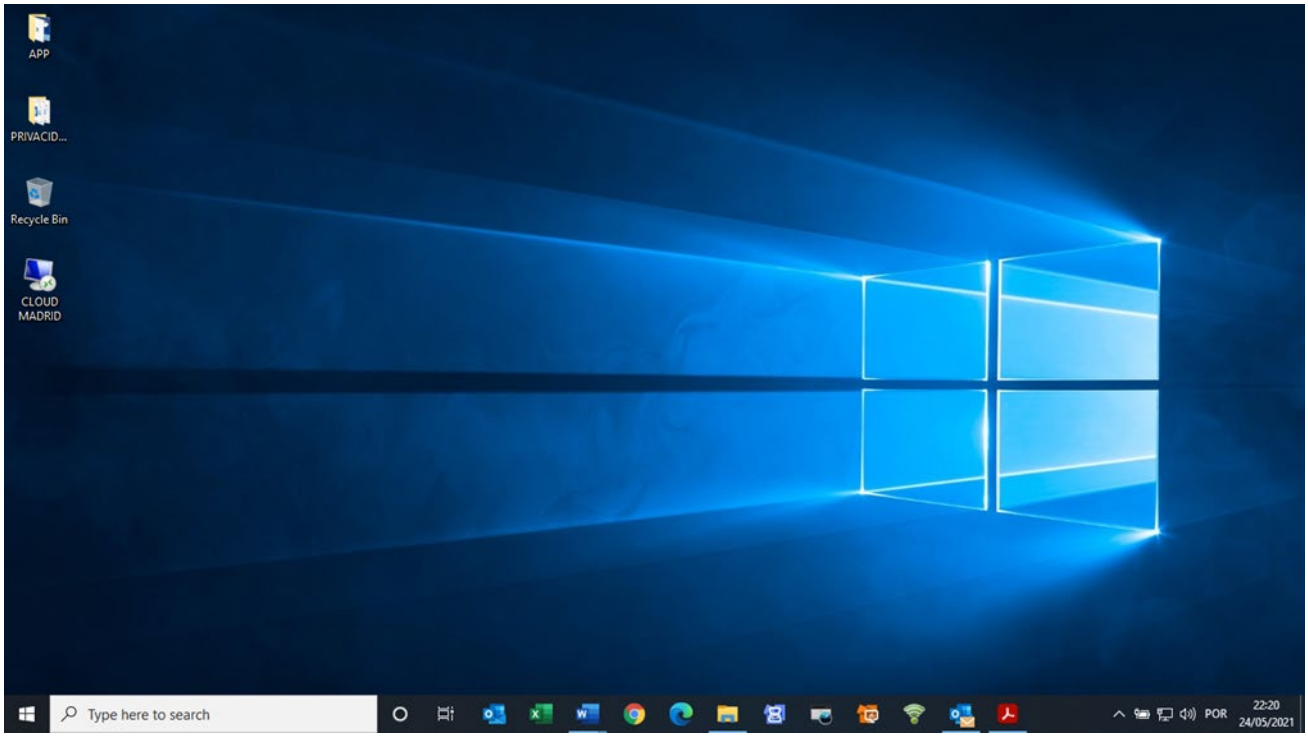
Para garantia da integridade dos dados da MADRID SAÚDE e utilização em caso de contingência, as informações armazenadas na rede interna devem estar replicadas em servidores virtuais externos (nuvem). O acesso a redes remotas permite ao usuário acessar, utilizar e executar aplicações e sistemas operacionais disponibilizados naquele ambiente, desde que tenham acesso autorizado para isto.

A boa utilização destes serviços é de responsabilidade de cada usuário, os que utilizam a rede da MADRID SAÚDE e/ou terceiros que utilizam serviços de acesso remoto. Cabe ressaltar que os serviços estão disponibilizados para o uso estritamente profissional e de interesse da empresa.

a) Por se tratar de solução de contingência devem ser utilizados de acordo com o estabelecido nos normativos específicos;

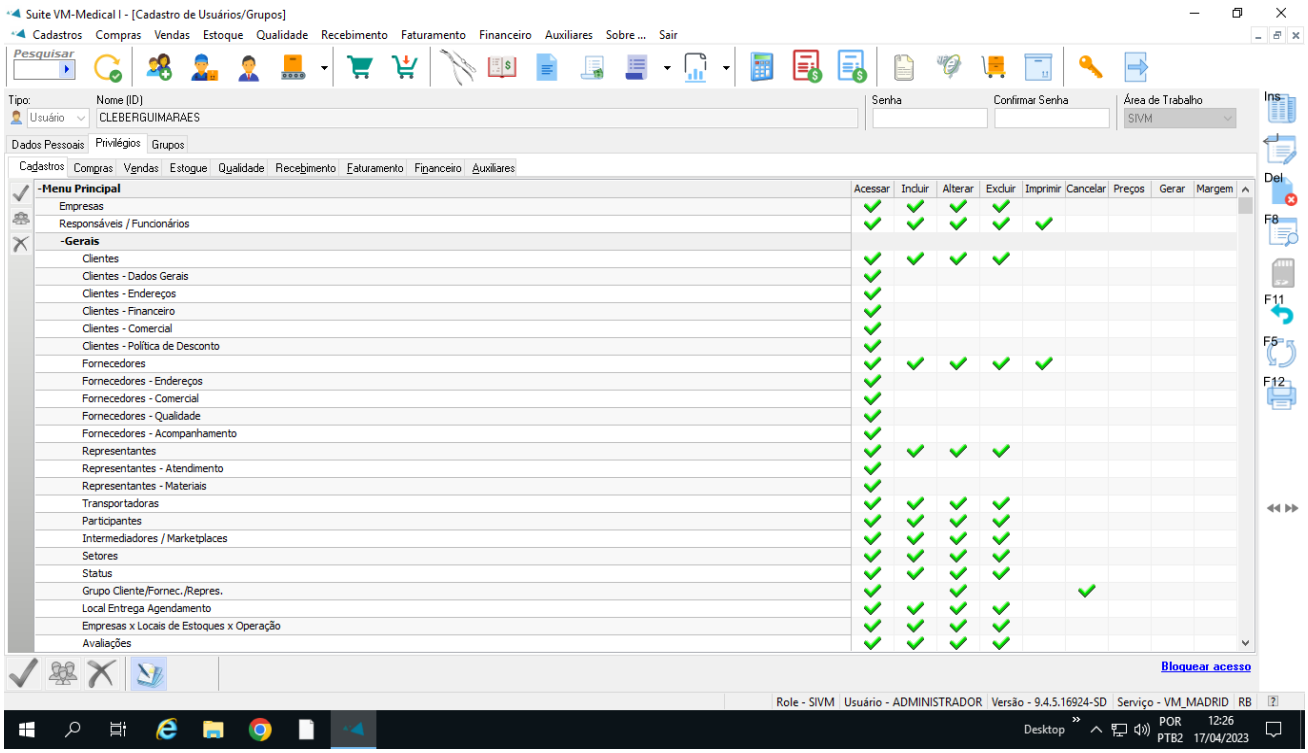
b) O usuário somente poderá realizar as atividades em período estipulado pela MADRID SAÚDE.



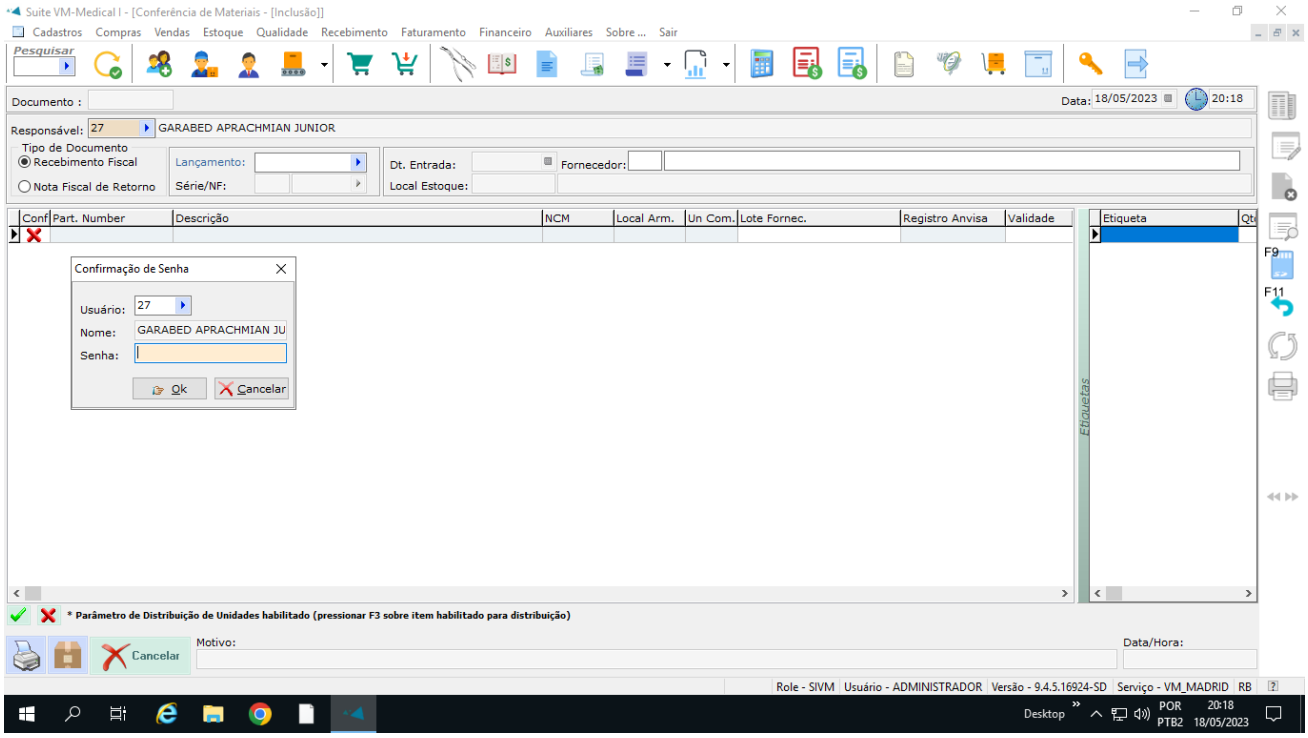


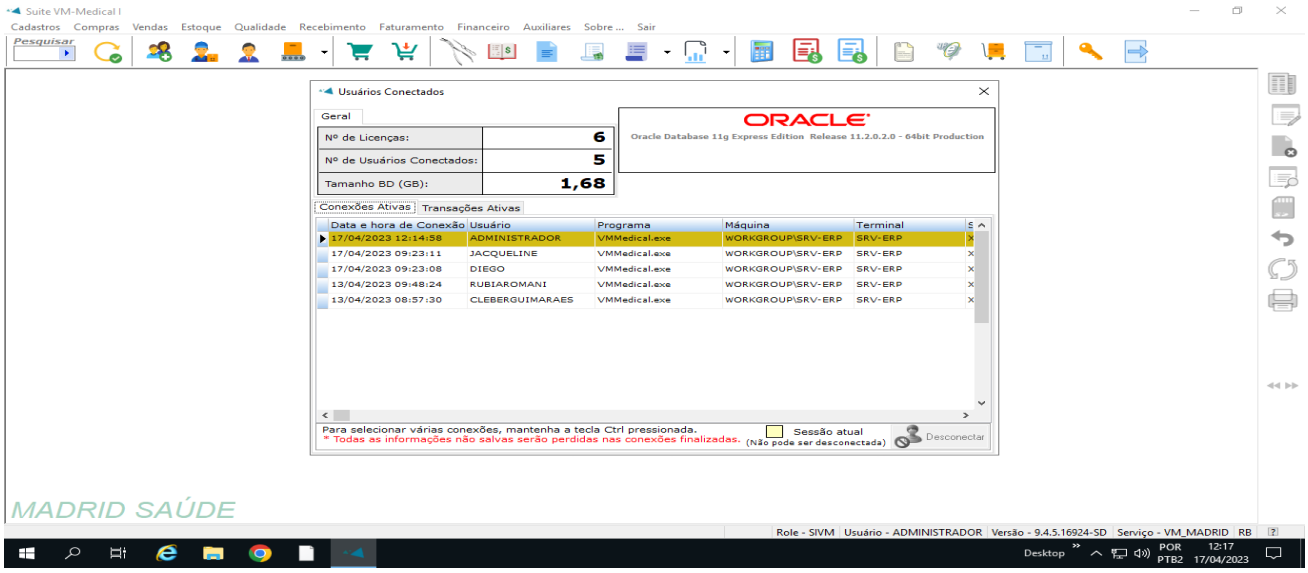
7.11.2 - PLATAFORMA VM MEDICAL – START EDITION:

A tela apresentada abaixo é a de inicialização do sistema. O Menu Principal só pode ser acessado após a inserção do nome do usuário e senha. Através do Login com usuário e senha, os usuários têm acesso controlado, conforme permissões concedidas pelo Administrador do Sistema.



Para qualquer alteração, impressão, ou criação de arquivos PDF é necessário o registro do usuário e sua senha para registro de data e hora da modificação e alteração realizada, conforme evidência abaixo.



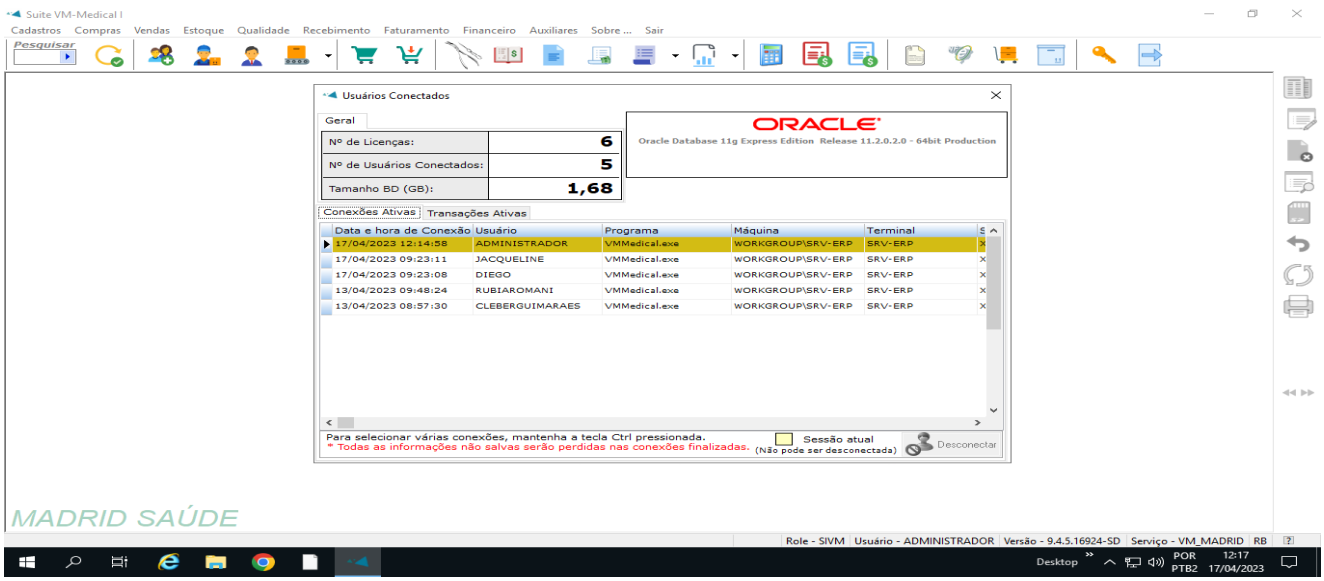


7.12 - Utilização dos Equipamentos de Informática e Comunicação

Os equipamentos de informática e de comunicação são utilizados pelos colaboradores da MADRID SAÚDE para a realização das atividades profissionais. Excepcionalmente, o uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

A MADRID SAÚDE, por meio de sua área de TI, poderá registrar todo e qualquer uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das Informações e Dados Pessoais. A responsabilidade em relação à Segurança da Informação será comunicada na fase de contratação dos colaboradores, os quais deverão assinar um termo de responsabilidade.

As estações de trabalho possuem códigos internos (IP), que permitem a rastreabilidade de todas as atividades executadas, assim como, é possível à área de TI monitorar todo acesso realizado por meio de sua rede, sendo de responsabilidade de cada colaborador zelar pelos seus respectivos acessos.



7.13 - Utilização da Internet

Sob o aspecto de proteção e integridade dos sistemas de informação, a Internet é classificada como conexão de alto risco. Os usuários devem estar cientes, portanto, das peculiaridades da navegação na Internet, antes de acessá-la e de utilizar os seus recursos.

A internet, via cabo ou Wi-Fi, deverá ser utilizada para fins profissionais, como ferramenta de busca de informações, que contribuam para o desenvolvimento das atividades da MADRID SAÚDE

O colaborador é responsável pelas atividades realizadas por intermédio de sua conta de usuário e senhas de acesso. Em particular, o usuário deverá observar os termos de licença de uso do material obtida através da internet.

Os colaboradores da MADRID SAÚDE não deverão em hipótese nenhuma:

a) Utilizar a Internet com objetivos ou meios para a prática de atos ilícitos, proibidos pela lei ou pela presente Política, lesivos aos direitos e interesses da empresa ou de terceiros;
b) Utilizar a Internet com objetivo de danificar, inutilizar, sobrecarregar ou deteriorar os recursos de tecnologia da informação e dados de qualquer tipo, de uso corporativo, pessoal ou de terceiros;
c) Acessar a sites de proxy com o objetivo de burlar os mecanismos de segurança existentes;
d) Acessar sites de pornografia, pedofilia e outros contrários à lei. O acesso a esses sites é terminantemente proibido, ainda que eles não estejam bloqueados no sistema de segurança da Instituição.

Os equipamentos fornecidos para o acesso à internet são de propriedade da MADRID SAÚDE, que poderá analisar e, se necessário, bloquear qualquer arquivo, site, e-mail, domínio ou aplicação armazenados na rede ou internet, estejam eles em disco local ou na rede. Assim, a MADRID SAÚDE, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos.

7.14 - Utilização de e-mail (Correio Eletrônico)

Os serviços de correio eletrônico são oferecidos como um recurso profissional pela MADRID SAÚDE, através de contrato com a empresa DB TECH TECNOLOGIA, que tem por objeto a prestação de serviço de hospedagem site do Cliente, composto do domínio madridsaude.com.br, domínios “parqueados”, da página corporativa atual da empresa e das suas respectivas contas de correio eletrônico, na infraestrutura da DBTECH e/ou de parceiro comercial. A lista de recursos disponibilizados, e de seus respectivos preços, estão presentes na proposta PTC-SV-2016-02001, anexa a este contrato para seus colaboradores no cumprimento de seus objetivos nas áreas de atuação.
O uso pessoal é permitido como exceção para casos em que se faça necessário, mas não priorizado e desde que não provoque efeitos negativos para qualquer outro usuário, não viole o sistema de mensagens, não interfira nas suas atividades, não interfira direta ou indiretamente nas operações dos recursos computacionais e serviços de correio eletrônico da MADRID SAÚDE, não incorra em gastos adicionais para a empresa, ou viole qualquer outra lei ou norma vigente.

Portanto, cada usuário é responsável por utilizar os serviços de correio eletrônico de maneira profissional, ética e legal. Deve ser considerado que o correio eletrônico é inerentemente uma forma insegura de comunicação, não garantindo sigilo ou entrega.

A MADRID SAÚDE poderá fornecer recursos adequados para melhorar o nível de segurança no uso do correio eletrônico, como, por exemplo, chaves de criptografia e assinatura digital e o acesso às mensagens nos servidores de correio eletrônico deve ser feito usando protocolos seguros – Outlook ou Webmail. Os colaboradores e parceiros com acesso, aos serviços de mensagem eletrônica disponibilizados pela MADRID SAÚDE devem observar o seguinte:

a) Todos os usuários dos ativos de Informações de propriedade da MADRID SAÚDE, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse da empresa, mantendo uma conduta ética e profissional;
b) Todas as contas de e-mail terão uma titularidade, sendo o usuário titular o responsável direto pelas mensagens enviadas por intermédio do seu endereço de e-mail;
c) Os usuários poderão ser titulares de uma única caixa postal individual no servidor de e-mail, com direitos de envio/recebimento de mensagens, via Intranet e Internet;
d) Contas com inatividade por um período igual ou superior a 60 (sessenta) dias serão bloqueadas, a fim de evitar o recebimento de novas mensagens;
e) O usuário deve utilizar o e-mail de forma adequada e diligente;
f) É vedado o envio, armazenamento ou manuseio de material que caracterize a divulgação, incentivo ou prática de atos que:
    I. Contrariem o disposto na legislação vigente, ética, moral e de ordem pública;
    II. Sejam proibidos pela presente Política, lesivos aos direitos e interesses da MADRID SAÚDE ou de terceiros;

III. De qualquer forma, possam danificar, inutilizar, invadir, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, do usuário ou de terceiros;
IV. Promovam ameaças, difamação ou assédio a outras pessoas;
V. Contenham conteúdo considerado impróprio, obsceno ou ilegal;
VI. Sejam de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
VII. Contenham a prática de qualquer tipo de discriminação relativa à raça, sexo, credo religioso, incapacidade física ou mental ou outras situações protegidas;

g) É vedada ainda a utilização do e-mail, nas situações abaixo:
I. Acesso não autorizado à caixa postal de outro usuário;
II. Uso para atividades com fins comerciais ou políticos e o uso extensivo para assuntos pessoais ou privados;
III. Envio de mensagens do tipo “corrente” e “spam”;
IV. Envio intencional de mensagens que contenham vírus eletrônico ou qualquer forma de rotinas de programação de computador, prejudiciais ou danosas;
V. Utilização de listas e/ou caderno de endereços da MADRID SAÚDE para a distribuição de mensagens que não sejam de estrito interesse funcional e sem a devida permissão do responsável pelas listas e/ou caderno de endereços em questão;
VI. Divulgação de informações em não conformidade com a diretriz de Classificação de Informações prevista nesta política;
VII. Envio de qualquer mensagem que torne a empresa vulnerável a ações civis ou criminais;
VIII. Exclusão de mensagens relacionadas às atividades profissionais, quando a MADRID SAÚDE ou pessoas a ele relacionadas estiverem.

A MADRID SAÚDE possui instrumentos para o bloqueio ou cópia de mensagens de maneira a subsidiar processos internos de sindicância ou para atendimento de ordem judicial. O bloqueio poderá ser aplicado a recepção de mensagens provenientes de alguns locais, comerciais ou não, em caso de inconveniência e/ou possível ameaça contida em mensagens indesejáveis. Os usuários devem utilizar em sua assinatura padrão texto que identifica os requisitos de Segurança da Informação relacionados a confidencialidade da troca de informações, servindo como instrução a terceiros que recebam mensagens provenientes da MADRID SAÚDE.

“AVISO: A informação contida neste e-mail, bem como em qualquer de seus anexos, é CONFIDENCIAL e destinada ao uso exclusivo do (s) destinatário (s) acima referido (s), podendo conter informações sigilosas e/ou legalmente protegidas. Caso você não seja o destinatário desta mensagem, informamos que qualquer divulgação, distribuição ou cópia deste e-mail e/ou de qualquer de seus anexos é absolutamente proibida. Solicitamos que o remetente seja comunicado imediatamente, respondendo esta mensagem, e que o original desta mensagem e de seus anexos, bem como toda e qualquer cópia e/ou impressão realizada a partir destes, sejam permanentemente apagados e/ou destruídos.”

“NOTICE: The information contained in this e-mail and any attachments there to is CONFIDENTIAL and is intended only for use by the recipient named herein and may contain legally privileged and/ or secret information. If you are not the e-mail´s intended recipient, you are hereby notified that any dissemination, distribution or copy of this e-mail, and/or any attachments thereto, is prohibited. Please immediately notify the sender replying to the above-mentioned e-mail address, and permanently delete and/or destroy the original and any copy of this e-mail and/or its attachments, as well as any printout thereof.”

7.15 - Utilização de software de Mensagens Instantâneas/Redes Sociais

Os serviços de comunicação instantânea instalados nos equipamentos serão inicialmente disponibilizados aos colaboradores que necessitem dessa ferramenta e poderão ser bloqueados, caso o gestor requisite formalmente à área de TI da MADRID SAÚDE.

O uso de aplicativos de comunicação pelos colaboradores, a partir de recursos da MADRID SAÚDE, para compartilhar informações profissionais, deverá ser feito de forma responsável para evitar riscos desnecessários, que possam comprometer as atividades, os projetos ou a própria empresa.

O colaborador deve, ainda, preservar o sigilo e a confidencialidade das Informações e Dados Pessoais, atender aos requisitos de segurança previstos nesta Política e respeitar a legislação vigente.

7.16 - Utilização de Dispositivos Móveis Corporativos

Dispositivos móveis corporativos são equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: notebooks, notebooks, smartphones, tablets, pen drives, USB drives, HD externos e cartões de memória.

É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações de uso interno, restritas ou confidenciais por meio de dispositivos móveis corporativos.

O usuário deve utilizar os dispositivos móveis corporativos de forma adequada e diligente, de forma a prevenir ações que possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos (hardware e software), bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros.

O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de dispositivos móveis corporativo, tanto por sua guarda quanto pelos conteúdos neles instalados.

Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel corporativo em nuvem contratada pela MADRID SAÚDE – WINOV SOLUÇÕES. Não é permitida a alteração da configuração dos sistemas operacionais dos equipamentos, em especial, os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um colaborador da área de TI.

O colaborador deverá responsabilizar-se em não utilizar quaisquer programas e/ou aplicativos, inclusive gratuitos, que não tenham sido instalados ou autorizados por um colaborador da área de TI.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela MADRID SAÚDE, notificar imediatamente seu gestor e a área de TI. Também deverá, assim que possível, registrar um Boletim de Ocorrência na Delegacia de Furtos de Roubos (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à MADRID SAÚDE e/ou a terceiros.

Em caso de desligamento o colaborador deve realizar imediata devolução de seus dispositivos móveis à área de TI.

7.17 - Utilização de Mídias Removíveis

O uso de mídias removíveis deve ser tratado como exceção à regra, pois a porta USB é o principal ponto de vulnerabilidade de segurança, podendo ser usada para a fuga de Informações e Dados Pessoais. Para esta utilização é necessário solicitar ao DPO autorização justificando a utilização e, só depois de aprovada, poderá ser utilizada em caráter sempre excepcional.

Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que tais dispositivos possam vir a causar, uma vez que esse tipo de mídia pode conter vírus e softwares maliciosos, capazes de danificar e corromper dados.

7.18 - Acesso remoto à rede da MADRID SAÚDE

A interconexão entre redes privadas a distância permite ao usuário utilizar-se de redes e serviços de redes disponibilizados por terceiros. O acesso a redes remotas disponibilizados por redes privadas externas permitem ao usuário acessar, utilizar e executar aplicações e sistemas operacionais disponibilizados naquele ambiente, desde que tenham acesso autorizado para isto.

Por se tratar de um acesso entre redes privadas, a segurança e integridade da Informações trafegada dependem das configurações da rede. Logo, este tópico tem como objetivo estipular um conjunto de diretrizes e recomendações aos diferentes usuários da MADRID SAÚDE.

A boa utilização destes serviços é de responsabilidade de cada usuário, os que utilizam a rede da MADRID SAÚDE e/ou terceiros que utilizam serviços de acesso remoto. Cabe enfatizar que os serviços estão disponibilizados para o uso estritamente profissional e de interesse da MADRID SAÚDE.

a) O usuário somente pode realizar acesso interativo entre redes onde a permissão esteja autorizada. A autorização depende das atividades profissionais relacionadas a função exercida;

b) O usuário deve utilizar somente o local e o ambiente físico aprovado pela MADRID

c) O usuário externo deve configurar de forma adequada o firewall e a proteção antivírus na rede externa à rede da MADRID SAÚDE;

d) O usuário somente poderá realizar as atividades em período estipulado pela MADRID SAÚDE.

7.19 - Instalações de Software

O colaborador da MADRID SAÚDE **é proibido de instalar** todo e qualquer programa não autorizado em seu computador e em qualquer outro dispositivo computacional pertencente à empresa, salvo as instalações de programas que contenham prévia autorização do gestor ou da área de TI. Este comando também é aplicado a programas com conteúdo de atualização conhecidos como patches.

O usuário é proibido de remover toda e qualquer versão de software obsoleto, mesmo em casos em que exista uma versão atualizada da aplicação utilizada.

Caso o usuário necessite instalar ou remover qualquer software, deverá entrar em contato com o gestor responsável.

Não é permitida a instalação/uso de softwares ilegais (sem licenciamento), sendo que a área de TI poderá valer-se desta Política para desinstalar, sem aviso prévio, todo e qualquer software sem licença de uso, em atendimento à Lei 9.609/98 (Lei do Software).

É proibido executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da MADRID.

7.20. Comunicação Verbal dentro e fora da MADRID SAÚDE

Somente os colaboradores que estão devidamente autorizados a falar em nome da MADRID SAÚDE, para os meios de comunicação, podem fazê-lo em nome da empresa.

A fim de evitar exposição desnecessária da MADRID SAÚDE, os colaboradores não devem tratar de assuntos internos em locais públicos ou dentro das instalações físicas da empresa, quando próximos a visitantes ou terceiros.

7.21. Engenharia Social

É um termo utilizado coloquialmente que representa a habilidade de enganar pessoas com o objetivo de obter Informações sigilosas ou Dados Pessoais. Essa ação pode ocorrer de diversas formas, mas o comum é os engenheiros utilizarem a falta de conscientização dos colaboradores em relação à Segurança da Informação da empresa.

O ataque pode ser feito (i) de forma direta, quando há um contato entre o engenheiro social e a vítima, por meio de telefonemas ou pessoalmente, ou (ii) de forma indireta, quando há a utilização de softwares ou outras ferramentas, a fim de captar dados que facilitem o acesso às Informações e Dados Pessoais desejados. Podem ser, por exemplo, mensagens que contenham avisos de premiações, ofertas de sociedade em grandes somas de dinheiro, heranças e negócios em outros países etc.

Assim, se o colaborador suspeitar de um possível ataque, através dos meios tecnológicos, deverá comunicar imediatamente à área de TI. Caso a tentativa de ataque tenha ocorrido por outros meios (não tecnológicos), deverá ser comunicada ao gestor.

8. RESPONSABILIDADES

A correta utilização dos recursos disponibilizados é dever de todos os colaboradores, sendo que o uso indevido, negligente ou imprudente será responsabilizado, conforme normativos internos e legais.

A MADRID SAÚDE reserva-se o direito de analisar dados e evidências, a fim de obter provas, que possam ser utilizadas nos processos investigatórios, bem como, de adotar as medidas legais cabíveis.

Quanto à presente Política de Segurança da Informação da MADRID SAÚDE, as responsabilidades ficam assim distribuídas:

8.1 - Gestores da MADRID SAÚDE

a) Aprovar a Política de Segurança da Informação;
b) Implementar a presente Política e fazer cumprir as normas aqui presentes;
c) Determinar a adoção de medidas necessárias para seu cumprimento;
d) Assegurar que os colaboradores possuam acesso e conhecimento desta Política;
e) Orientar e informar aos colaboradores as práticas necessárias à Segurança da Informação;
f) Receber o reporte de todo e qualquer Colaborador e/ou área para tratar de assuntos pertinentes à Segurança da Informação de que trata este instrumento;
g) Receber e tratar as notificações dos casos de violação das diretrizes de segurança expostas neste instrumento;
h) Promover juntamente com a área de TI a segregação de acessos necessários aos sistemas da MADRID SAÚDE, evitando conflitos de interesse e adotando perfis de acesso.

8.2 - Área de TI

a) Monitorar o ambiente de TI e a atividade de todos os usuários durante os acessos às redes internas e externas (internet), por exemplo: sites, e-mails, sistemas e outros;
b) Executar as ações necessárias para tratar violações de segurança no âmbito tecnológico;
c) Configurar os equipamentos, instalar softwares e implementar os controles necessários, bem como, definir regras para a instalação de software e hardware nos equipamentos da MADRID SAÚDE;
d) Coordenar as atividades de tratamento e resposta a incidentes de TI;
e) Promover a recuperação de sistemas, se necessário;
f) Administrar, proteger e testar cópias de segurança de sistemas e dados relacionados aos processos operacionais considerados críticos;
g) Planejar e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida e a disponibilidade da rede interna;
h) Assegurar-se de que não sejam introduzidas vulnerabilidades ou fragilidades na rede e nos equipamentos;
i) Promover juntamente com os gestores dos processos a segregação de acessos necessários aos sistemas da MADRID SAÚDE, evitando conflitos de interesse e adotando perfis de acesso;
j) Promover juntamente com os gestores dos processos a segregação de acessos necessários aos sistemas da MADRID SAÚDE, evitando conflitos de interesse e adotando perfis de acesso;
k) Receber o reporte de todo e qualquer Colaborador e/ou área para tratar de assuntos pertinentes à Segurança da Informação de que trata este instrumento;
l) Receber e tratar as notificações dos casos de violação das diretrizes de segurança expostas neste instrumento;
m) Realizar testes e atualizações nos diversos acessos aos recursos de TI.

8.3 - Área de Controles Internos

a) Avaliar os riscos do processo juntamente com os responsáveis;
b) Elaborar e executar planos de testes e realizar auditoria nos controles relacionados à Segurança da Informação;
c) Monitorar o resultado e sugerir novos controles no ambiente de Segurança da Informação, quando aplicável.

8.4 - Todos os colaboradores Madrid Saúde

a) Conhecer e cumprir a presente Política;
b) Assinar termo de Ciência e Responsabilidade sobre a Política declarando ter conhecimento de suas responsabilidades;

c) Buscar orientação em caso de dúvidas relacionadas à Segurança da Informação;
d) Fiscalizar e orientar os parceiros e clientes da MADRID SAÚDE quanto às diretrizes desta política;
e) Comunicar imediatamente quando do descumprimento ou violação desta política, conforme diretrizes do Item 7. Tratamento de Violações.

9 – ATUALIZAÇÕES, DIVULGAÇÃO, TREINAMENTO, TRATAMENTO DE VIOLAÇÕES E RESPONSABILIDADES.

O DPO da Madrid Saúde divulgará anualmente, buscando a conscientização, educação e treinamento em Segurança da Informação, esta política e suas atualizações, sempre no mês de janeiro ou quando julgar necessário, a fim de que todos os colaboradores estejam cientes das normas constantes nesta Política e suas alterações (caso haja).

Os colaboradores atuais e aqueles futuramente contratados deverão assinar Termo de Ciência e Responsabilidade sobre a Política e Termo de Confidencialidade, comprometendo-se a agir conforme as diretrizes aqui estipuladas.

Toda violação ou desvio de Informações e Dados Pessoais são investigados para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos. Situações que podem ocasionar sanções incluem, mas não se limitam, a:

a) Uso ilegal de software;
b) Introdução (intencional ou não) de vírus de informática;
c) Tentativas de acesso não autorizado a dados e sistemas;
d) Compartilhamento de Informações e Dados Pessoais e/ou Divulgação de informações dos clientes da MADRID SAÚDE.

Ainda, a fim de garantir a confidencialidade, integridade e disponibilidade das Informações e Dados Pessoais, ao tomar conhecimento de todo e qualquer incidente de segurança da informação que ocorrer em ambiente próprio ou de terceiros, de sua responsabilidade, e que possa comprometer as atividades da MADRID SAÚDE, especialmente acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma inadequada ou ilícita, o Colaborador deverá notificar o gestor e O responsável de TI. Caso devidamente comprovado, o usuário infrator estará passível das seguintes penalidades imediatas, sem prévio aviso:

a) Descredenciamento da senha de acesso à Internet;
b) Cancelamento da conta de e-mail;
c) Cancelamento do acesso aos sistemas corporativos;
d) Desativação do ponto de rede do usuário;
e) Aplicação das penalidades previstas na legislação vigente no Brasil.

Nas mesmas penas incorrem o Colaborador que, ciente do incidente com as Informações e Dados Pessoais, deixa de comunicar o gestor e/ou a equipe de TI.

Especificadamente quanto aos Dados Pessoais, caso devidamente constatado que o Colaborador agiu com dolo ou culpa em incidente de vazamento de Dados Pessoais, aos quais eventualmente teve acesso, o Colaborador também se responsabilizará pelo pagamento de valores, importâncias ou quantias que o incidente e/ou tratamento inadequado tenha causado à MADRID SAÚDE que incluem: (i) multas e penalidades que a MADRID SAÚDE seja obrigada a pagar; e (ii) custos de defesa que a MADRID SAÚDE seja obrigada incorrer.

10 - GESTÃO DE CONTINUIDADE DE NEGÓCIOS

A Gestão de Continuidade de Negócios define os procedimentos para prevenção de interrupções de atividades críticas ao negócio, viabilizando a ativação de processos alternativos na ocorrência de indisponibilidade dos serviços. Também visa orientar os colaboradores em relação aos procedimentos a serem realizados quando da ocorrência de algum incidente, informando as partes interessadas.

A gestão de continuidade de negócios é um processo permanente destinado a preparar a MADRID SAÚDE e seus Colaboradores a resistir aos efeitos de emergências ou interrupções e minimizar os danos operacionais, legais, financeiros e à imagem da empresa.

A gestão de continuidade de negócios é um processo permanente destinado a preparar a MADRID SAÚDE e seus Colaboradores a resistir aos efeitos de emergências ou interrupções e minimizar os danos operacionais, legais, financeiros e à imagem da empresa.

Desta forma, a gestão de continuidade de negócios prepara os passos a serem tomados após uma emergência ou interrupção para a retomada das atividades críticas e posterior retorno à normalidade.

A MADRID SAÚDE, para conseguir atingir tal objetivo implantará as seguintes etapas:

I. Conhecer a unidade: nessa etapa denominada “análise de impacto nos negócios”, os gestores e equipe de TI da MADRID SAÚDE, na unidade de trabalhar, irá identificar:

a) Suas atividades críticas;
b) O tempo máximo que tais atividades podem ficar paradas sem que acarretem um dano insuportável à MADRID SAÚDE;
c) Os danos decorrentes da paralização;
d) A identificação das pessoas responsáveis pelas atividades críticas, bem como as capacitadas a realizá-las;
e) Os sistemas utilizados na execução das atividades críticas;
f) Os dados vitais requeridos nas atividades críticas, bem como informações de cópia de segurança;
g) Os recursos mínimos necessários à execução das atividades críticas;
h) Os riscos de acontecer um cenário de indisponibilidade de acesso físico, de indisponibilidade de TI e de indisponibilidade de pessoas; e
i) Possíveis locais alternativos de trabalho.

Após identificação, será elaborado Relatório de Impacto aos Negócios, documento que servirá de base para as próximas etapas.

I. Definição de estratégias: nessa fase são utilizadas informações colhidas durante o conhecimento da unidade para identificar e escolher opções de estratégias de continuidade.

A estratégia de continuidade habilita a unidade a continuar suas atividades críticas dentro do período máximo em que ela pode ser interrompida, antes que danos insuportáveis advindos da interrupção ocorram.

São definidas estratégias para:

I. Local de trabalho: definição de local alternativo no caso de indisponibilidade de acesso, bem como procedimentos a serem adotados;
II. Pessoas: disseminação de conhecimentos, mapeamento de processos, alocação de trabalhos na indisponibilidade de pessoas;
III. Tecnologia da Informação: procedimentos a serem realizados no caso de indisponibilidade dos recursos de TI e métodos de mitigá-la.
IV. Elaboração e implementação um ou mais planos: após a seleção dos processos críticos e a definição das estratégias, serão elaborados um ou mais planos que possibilitem a implementação dessas estratégias.
V. Testes: a gestão de continuidade de negócio e seus planos serão testados e auditados e mantidos por meio de revisões e atualizações periódicas constantes pela MADRID SAÚDE.

11 - VIGÊNCIA, VALIDADE E ATUALIZAÇÕES

A presente Política passa a vigorar a partir da data de sua aprovação/revisão pela diretoria, sendo válida por tempo indeterminado. Após a implantação desta Política, com o objetivo de mantê-la atualizada e condizente com as necessidades da MADRID SAÚDE, deverão ser realizadas, anualmente, ou sempre que houver incidentes, revisões com a implantação de novas ações e controles para sua melhoria contínua. Possuímos contratos vigentes de serviços que asseguram o informado anteriormente com:

Dbtech Tecnologia da Informação LTDA - Hospedagem do site do Cliente, composto do domínio madridsaude.com.br, domínios “parqueados”, da página corporativa atual da empresa e das suas respectivas contas de correio eletrônico, na infraestrutura da DBTECH e/ou de parceiro comercial.

WINOV SOLUÇÕES EM TECNOLOGIA S.A. - Locação de servidor CLOUD COMPUTING, denominado HOSTCLOUD (“Solução Winov”).

VISTO SISTEMAS LTDA - Sistema de Gerenciamento da PLATAFORMA VM MEDICAL – START EDITION.

TOCOMPLY SOLUÇÕES TECNOLÓGICAS LTDA - Gestão e implementação do programa de integridade

12 – REFERÊNCIAS

a) Lei 9.609/1998 - Lei do Software;
b) Lei 12.527/2011 - Lei de Acesso à Informação;
c) Lei 12.737/2012 - Lei Carolina Dieckmann;
d) ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Sistemas de gestão da segurança da informação — Requisitos;
e) ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Código de prática para controles de segurança da informação;
f) Constituição da República Federativa do Brasil de 1988
g) Lei 12.965/2014 - Marco Civil da Internet;
h) Lei 13.709/2018 - Lei Geral de Proteção de Dados.

13 – GLOSSÁRIO

a) Ambiente Tecnológico: Compreende todos os sistemas, computadores e redes da MADRID SAÚDE.
b) Antivírus: Programa de proteção do computador que detecta e elimina os vírus (programas danosos) nele existentes, assim como impede sua instalação e propagação.
c) Aplicativos de comunicação: Programas de computador, geralmente instalados em dispositivos móveis, usados para troca rápida de mensagens, conteúdos e informações multimídia, a exemplo de WhatsApp, Telegram, Skype etc.
d) Ativo: Qualquer coisa que tenha valor para o MADRID SAÚDE e precisa ser adequadamente protegida.
e) 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.
f) Clientes: Clientes da MADRID SAÚDE.
g) Colaboradores: Colaboradores da MADRID SAÚDE.
h) Dispositivos móveis: Equipamentos de pequena dimensão que têm como características a capacidade de registro, armazenamento ou processamento de informações, possibilidade de estabelecer conexões e interagir com outros sistemas ou redes. Exemplos: smartphone, notebook, tablet, equipamento reprodutor de MP3, câmeras de fotografia ou filmagem.
i) Firewall: Dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
j) Hardware: conjunto dos componentes físicos (material eletrônico, placas, monitor, equipamentos periféricos etc.) de um computador.
k) Log: Registro de eventos em um sistema de computadores.
l) Mídias Removíveis: Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Pen Drive, cartão de memória entre outros.
m) Patches: Programas criados para atualizar ou corrigir um software.
n) Parceiros: Pessoas Físicas ou Jurídicas que possuem relação de negócios com a MADRID SAÚDE.
o) Perfil de Acesso: Grupo de acessos a um recurso tecnológico estratificado por função dentro da MADRID SAÚDE.
p) Proxie: Em redes de computadores, um proxie é um servidor (um sistema de computador ou uma aplicação) que age como um intermediário para requisições de clientes solicitando recursos de outros servidores.
q) Sites de proxie: Sites utilizados para acessar outros sites da web. Em redes corporativas que tem monitoramento ou bloqueio de sites, sites de proxie permitem a navegação anônima a sites proibidos.
r) Servidor: é um software ou computador, com sistema de computação centralizada que fornece serviços a uma rede de computadores, chamada de cliente.
s) Software: É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores.
t) Spam: Mensagem de e-mail publicada em massa com fins publicitários.
u) TI: Tecnologia da Informação.
v) USB: É um tipo de conexão “ligar e usar” que permite a conexão de periféricos sem a necessidade de desligar o computador.
w) Wi-Fi: Abreviação de Wireless Fidelity - é uma tecnologia de comunicação que não faz uso de cabos e, geralmente, é transmitida através de frequências de rádio, infravermelhos etc.

Esta Política de Segurança da Informação poderá ser atualizada, razão pela qual a MADRID SAÚDE recomenda a consulta periódica.