POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Unimed Marília

Sumário

1. INTRODUÇÃO

Esta Política de Segurança da Informação (PSI) é mantida e divulgada pela UNIMED MARÍLIA para orientar seus colaboradores e prestadores de serviços sobre como proteger adequadamente as informações manipuladas no exercício de suas funções. Todas as informações da UNIMED MARÍLIA, de seus clientes, colaboradores, prestadores de serviços, cooperados e demais partes interessadas devem ser obtidas, manipuladas, armazenadas e, eventualmente, destruídas conforme as determinações desta política.

2. TERMOS E DEFINIÇÕES

Área de TI: Compreende o setor, tecnologias e pessoas, de Tecnologia e Inovação da UNIMED MARÍLIA.

PSI: Política de Segurança da Informação.

Ativo: Qualquer recurso de processamento da informação digital ou físico que tenha valor para a UNIMED MARÍLIA.

Colaborador: Pessoa que esteja trabalhando em nome da UNIMED MARÍLIA, como empregado efetivo, empregado temporário, estagiário ou menor aprendiz.

Confidencialidade: Propriedade que garante que apenas pessoas autorizadas possuem acesso a informações sensíveis.

Login: Processo de identificação e autenticação de um usuário para permitir o seu acesso a um sistema.

Negócio, Empresa ou Unimed: Referem-se a UNIMED MARÍLIA e respectivas Unidades de Negócios.

Prestador de Serviço: Pessoa que esteja trabalhando em nome, para ou na UNIMED MARÍLIA, ou que de outra forma possa ter acesso a informações confidenciais, como, consultor, fornecedor, terceiro e parceiro de negócio.

Recursos de TI ou Recursos de Informática: Recursos eletrônicos físicos e lógicos, periféricos e softwares relacionados com a informática ou Tecnologia da Informação.

SGSI: Sistema de Gerenciamento da Segurança da Informação – é a parte do sistema de gestão global da Empresa, baseado numa abordagem sobre o risco do negócio, para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação.

> **Nota:** O sistema de gestão inclui a estrutura organizacional, políticas, atividades de planejamento, responsabilidades, práticas, procedimentos, processos e recursos.

Usuário: Qualquer pessoa que utiliza recursos de TI.

Wireless: Sistema de comunicação que não requer fios para transportar sinais.

3. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

As diretrizes da Política de Segurança da Informação (PSI) é garantir a continuidade do negócio através da mitigação dos riscos de segurança da informação, minimizando os impactos tangíveis e intangíveis, garantindo que os recursos de informática e informações sejam usados de maneira adequada. A segurança de nossas informações e de nossos sistemas de informação é fundamental para atingirmos nossos objetivos de negócio.

A PSI tem por objetivo garantir a Confidencialidade, Integridade e Disponibilidade das informações da UNIMED MARÍLIA e que estão sob sua custódia, tais como informações de clientes, acionistas, colaboradores e prestadores de serviços, durante todo o ciclo de vida das informações, em um esforço conjunto entre todos os colaboradores e prestadores de serviço.

A UNIMED MARÍLIA entende ser vital para seu negócio a adequada proteção das informações assim como a contínua conscientização de seus colaboradores, prestadores de serviços e conselheiros para minimizar riscos.

Qualquer dado e/ou informação deve ser tratado com base no princípio da confidencialidade, de modo que não sejam compartilhadas e se houver necessidade de armazenamento, que seja em ambiente seguro e acessados apenas por pessoas autorizadas.

A UNIMED MARÍLIA deve estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a PSI dentro do contexto das suas atividades de negócios gerais e os riscos que ela enfrenta.

4. EQUIPE DE SEGURANÇA DA INFORMAÇÃO

A UNIMED MARÍLIA criará a Equipe de Segurança da Informação como a maior autoridade para avaliação de políticas, padrões e procedimentos com relação à Segurança da Informação.

4.1 REPRESENTAÇÃO DO EQUIPE DE SEGURANÇA DA INFORMAÇÃO

A Equipe de Segurança da Informação é multidisciplinar e renovado a cada dois anos em pelo menos um terço, sendo composto por no mínimo, representantes dos seguintes departamentos:

- Atenção Plena a Saúde - APS
- Atendimento
- Auditoria em Saúde
- Central de Relacionamento
- Centro de Especialidades Médicas - CEM
- Centro de Reabilitação - CER
- Centro de Reabilitação Infantil Especializado - CRIE
- Comercial
- Compras
- Contabilidade
- Contas Médicas
- Departamento Pessoal - DP
- Departamento Saúde Ocupacional - DSO
- Espaço Viver Bem - EVB
- Farmácia Comercial
- Farmácia Oncológica

- Faturamento
- Financeiro
- Gestão de Rede
- Gestão de Serviços
- Marketing
- Órteses Próteses e Materiais Especiais - OPME
- Ouvidoria
- Pós-Venda
- Projetos e Qualidade
- Pronto Atendimento
- Recursos Humanos - RH
- Regulação ANS
- Relacionamento ao Cooperado
- Segurança e Saúde do Trabalhador - SST
- Serviço de Atenção Domiciliar - SAD
- Serviço Social
- Tecnologia da Informação – TI

Havendo a necessidade, representantes de outras áreas podem ser convidados a participar de reuniões da Equipe de Segurança da Informação.

4.2 ATIVIDADES DA EQUIPE DE SEGURANÇA DA INFORMAÇÃO

1. Avaliar a Política de Segurança da Informação, para posterior aprovação da Presidência.

2. Identificar e atribuir responsabilidades com relação à segurança da informação;

3. Avaliar e monitorar o nível de segurança da UNIMED MARÍLIA e auditar os processos descritos nesta política;

4. Monitorar alterações que possam afetar a segurança e, caso necessário, aprovar as iniciativas de melhoria do nível de segurança;

5. ABRANGÊNCIA E RESPONSABILIDADES

Todos os envolvidos que utilizam ou possuem acesso à informação ou aos recursos de Tecnologia da Informação (TI) da UNIMED MARÍLIA ou sob sua custódia, sejam colaboradores, estagiários, conselheiros ou prestadores de serviços, devem garantir que as práticas definidas na PSI sejam aplicadas e seguidas continuamente. Para isto, todos os colaboradores, conselheiros e prestadores de serviço assistencial da sede administrativa e serviços próprios **devem assinar o termo F-RH-062 - TERMO DE RESPONSABILIDADE.**

O acordo de confidencialidade da UNIMED MARÍLIA está contemplado no termo **F-RH-062** citado acima.

Aqueles que, uma vez cientes, violem as regras de segurança, estarão sujeitos a ação disciplinar interna, sem prejuízo das demais sanções e responsabilidades civis, criminais e trabalhistas aplicáveis.

Medidas disciplinares para prestadores de serviços que violem as regras da PSI serão tratadas conforme acordado em contrato e lei aplicável.

5.1 CATEGORIAS DE RESPONSABILIDADES

Para operacionalizar o controle dos direitos e deveres relativos à segurança, a UNIMED MARÍLIA deve adotar o sistema de categorias de responsabilidades.

5.1.1 Responsável

Os Responsáveis pelas Informações são os Responsáveis pelas Áreas, Diretores ou seus Representantes. São, em suma, as pessoas com a responsabilidade pela aquisição, criação, manutenção e descarte das informações da cooperativa.

Os Responsáveis avaliam o risco, definem a classificação da informação, definem os controles de segurança e também quais pessoas podem ter acesso à informação. É também atribuição do Responsável aprovar a forma com que as informações serão utilizadas e zelar por ela.

Toda a aplicação, sistema ou informação crítica, obrigatoriamente deve ter um Responsável designado. Os Responsáveis devem definir a classificação de sensibilidade e a quais usuários o acesso será concedido.

5.1.2 Usuário

Os Usuários devem se familiarizar e seguir todos os itens da PSI. Dúvidas sobre a manipulação apropriada de um tipo específico de informação devem ser dirigidas ao Responsável pelo Ativo.

Dúvidas sobre a manipulação apropriada de um tipo específico de informação devem ser dirigidas ao Responsável.

Casos duvidosos ou omissos devem ser decididos pela Equipe de Segurança da Informação.

6. MANUTENÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

É aconselhável a revisão da PSI a cada 24 meses. A Equipe de Segurança da Informação pode, no entanto, iniciar o processo de revisão a qualquer momento. A decisão de revisar a PSI pode ser tomada com base em critérios próprios ou a partir de um dos seguintes acontecimentos:

1. Incidentes de segurança considerados significativos;
2. Novas vulnerabilidades identificadas;
3. Alteração ou publicação de legislação aplicável à segurança de dados;
4. Mudanças na estrutura técnica ou organizacional da UNIMED MARÍLIA.

Toda revisão deve ser analisada pela Equipe de Segurança da Informação e formalmente registrada. As modificações, bem como o controle de versão da PSI devem ser cuidadosamente observadas.

6.1 Auditoria interna da Política da Segurança da Informação

A cooperativa deve conduzir auditorias internas do PSI em intervalos planejados para determinar se os objetivos, controles, processos e procedimentos de sua PSI:

a) atende aos requisitos de segurança da informação identificados;

b) são efetivamente implementados e mantidos; e

c) são executados como esperado.

Um programa de auditoria deve ser planejado, levando em consideração o status e a importância dos processos e quais áreas a serem auditadas, bem como os resultados de auditorias anteriores. Os critérios de auditoria, escopo, frequência e métodos devem ser definidos.

A seleção de auditores e a realização de auditorias devem assegurar objetividade e a imparcialidade do processo de auditoria. Os auditores não devem auditar seu próprio trabalho.

7. POLÍTICAS ESPECÍFICAS

A PSI é composta pelas Diretrizes e as seguintes políticas específicas:

1. Política de Controle de Acesso e Autenticação;
2. Política de Uso de Equipamentos e Recursos de TI;
3. Política de Uso de Portáteis e Acesso Remoto;
4. Política de Acesso à Internet;
5. Política de Uso de Correio Eletrônico;
6. Política de Segurança em Recursos Humanos;
7. Política de Segurança Física e do Ambiente;
8. Política de Operações e Gerências de Sistemas;
9. Política de Armazenamento de Arquivos;
10. Política Relacionada à LGPD (Lei Geral de Proteção de Dados).

7.1 POLÍTICA DE CONTROLE DE ACESSO E AUTENTICAÇÃO

7.1.1 Registro do Usuário

Todo usuário que acessa o ambiente de Tecnologia da UNIMED MARÍLIA deve ser identificado lógica e unicamente através de sua conta (“login” e senha) de uso exclusivo. As senhas de acesso são confidenciais e individuais e sua revelação a outros ou permitir o seu uso por outros é proibida.

7.1.2 Cadastro, Alteração e Exclusão de Cargos ou Funções

É de responsabilidade da área de TI criar, bloquear e excluir os usuários nos sistemas. Quando tecnicamente viável, as informações dos colaboradores, contidas na base de dados da área de Recursos Humanos, devem ser utilizadas como fonte para o cadastro do colaborador nos demais sistemas.

Sempre que o Departamento de Recursos Humanos, Gestor da Pessoa ou Segurança Empresarial, registrarem e informarem a alteração do cargo/função de um colaborador ou prestador de serviço interno, os seus direitos de acesso às informações devem ser revisados pelos responsáveis de perfis de acesso concedidos ao colaborador ou prestador de serviço interno.

Os colaboradores ou prestadores de serviços que forem afastados, desligados, ou tiverem encerramento de contrato, devem ter sua conta bloqueada em todos os sistemas.

7.1.3 Controle de Privilégios

É de responsabilidade da área de TI controlar os direitos de acesso de contas de sistemas corporativos, como “Super Usuário”, administrador ou quaisquer outras denominações que signifiquem poderes adicionais para instalar, alterar ou apagar informações. Os controles devem observar, pelo menos:

1. Utilização de um usuário diferente do normal, quando este estiver executando tarefas de “Super Usuário”;

2. Clara identificação de quais usuários tem acessos às “contas privilegiadas”;

3. Registro de uso das contas, com verificação periódica.

7.1.4 Troca de Senha de Acesso Privilegiado

As senhas administrativas devem ser trocadas periodicamente respeitando requisitos de complexidade mínimos e o tempo máximo de 90 dias.

7.1.5 Privilégios em Equipamentos Específicos

É de responsabilidade da área de TI configurar os direitos dos usuários de forma que estes possuam direitos mínimos de acesso na estação de trabalho, mas suficientes para a execução de suas tarefas.

Para casos específicos, onde os requisitos de negócio ou dificuldade técnica tornem obrigatória a concessão de direitos adicionais, no mínimo os seguintes controles compensatórios devem ser implementados:

1. Registro do identificador do usuário com poderes adicionais;

2. Registro do identificador do equipamento, ou equipamentos, onde os direitos foram concedidos;

3. Justificativa da concessão de tal acesso.

7.1.6 Acesso de Administradores aos Sistemas

Os administradores de sistema devem efetuar acesso somente a informações para uso de suas atividades. É terminantemente proibido aos administradores acessar dados privados de quaisquer outras pessoas, sejam colaboradores, clientes ou prestadores de serviços, sem justificativa.

Os dados acessados pelos administradores de sistemas não devem ser compartilhados com pessoas não autorizadas.

Em casos específicos, os Administradores de Sistema devem trabalhar em conjunto com a área de Segurança Empresarial, única autorizada a efetuar investigações e solicitar registros e acessos a informações.

7.1.7 Regras para Criação de Contas

Na composição dos nomes de contas na rede “logins”, deverão ser atendidos os seguintes critérios básicos:

1. Toda conta de acesso é criada utilizando o seguinte padrão:

   a. Nome Inicial, ponto, ultimo nome (para colaboradores, prestadores de serviço, estagiários e temporários); ou

   b. Nome Inicial, ponto, penúltimo nome (para colaboradores, prestadores de serviço, estagiários e temporários);

7.1.8 Configuração de Senhas de Acesso

É de responsabilidade da área de TI, sempre que tecnicamente possível, parametrizar os sistemas com, no mínimo, as seguintes regras:

- Exigir a troca a cada 90 dias;
- Exigir a troca da senha padrão no primeiro acesso do usuário;

A área de TI, para casos específicos e visando proteger os ativos da UNIMED MARÍLIA pode definir requisitos mais restritivos dos que foram definidos acima.

7.1.9 Armazenamento de Senha

As senhas não podem ser guardadas de forma legível em arquivos, bases de dados, macros de software, chaves de função, terminais, anotadas em papel, ou em outros locais, nos quais, pessoas sem autorização possam ter acesso.

7.1.10 Senhas Padrão

É de responsabilidade da área de TI alterar a senha de equipamentos ou sistemas que utilizem uma senha padrão, no momento de sua instalação ou recebimento, antes de sua entrada em atividade.

7.1.11 Acesso Administrativo Padrão

Contas de acesso padrão com privilégios especiais, como por exemplo, usuários “root” e “administrador”, não devem ser utilizados nas atividades do dia-a-dia. Para atividades do dia-a-dia uma conta diferente da conta administrativa padrão deve ser utilizada, devendo ser criada uma conta nominal com os privilégios necessários, permitindo a rastreabilidade das ações executadas.

7.1.12 Mínimo Privilégio

Os usuários devem receber apenas os direitos necessários para a execução de suas atividades.

7.1.13 Perfis de Uso e Direitos

Devem ser criados perfis, acessos e grupos de usuários com a finalidade de se reduzirem riscos relacionados ao gerenciamento de acessos. Como grupo ou perfis entendem-se vários usuários que estão sob as mesmas regras e podem ser gerenciados em conjunto.

Para as aplicações que não permitem níveis de segregação, as atividades dos usuários devem ser registradas pela aplicação e posteriormente devem ser verificadas pelo gestor do usuário.

7.1.14 Direitos

Os direitos de acesso devem ser cadastrados nos grupos ou perfis de acordo com as necessidades de negócio da UNIMED MARÍLIA. Em ambos os casos os direitos devem ser aprovados pelo gestor da pessoa e posteriormente pelo responsável do perfil e ou ativo, o qual deve ser um colaborador ou prestador de serviço da UNIMED MARÍLIA. O gestor da pessoa e o responsável pelo perfil ou ativo devem efetuar uma análise se a pessoa realmente necessita do acesso, autorizando somente o necessário.

7.1.15 Bloqueio de Usuários Inativos

É de responsabilidade da área de TI implementar, sempre que houver a possibilidade, um procedimento de bloqueio dos usuários que não acessam os sistemas há mais de 90 dias. Uma avaliação posterior por parte do Responsável pelo ativo definirá se os usuários bloqueados devem ser definitivamente excluídos.

7.1.16 Acesso de Fornecedores

O acesso de fornecedores a sistemas e informações da UNIMED MARÍLIA deve ser devidamente controlado, os requisitos de segurança estabelecidos na Política de Controle de Acesso e Autenticação devem ser verificados antes que a concessão seja efetuada.

Os fornecedores que tiverem acesso a sistemas e informações da UNIMED MARÍLIA devem declarar estar cientes e aderir formalmente a esta política, bem como realizar a assinatura do documento de confidencialidade.

7.2 POLÍTICA DE USO DE EQUIPAMENTOS E RECURSOS DE TI

7.2.1 Uso Autorizado

Os equipamentos e sistemas de propriedade da UNIMED MARÍLIA devem ser usados para atividades profissionais. Os usuários não devem utilizar-se dos equipamentos ou sistemas de informação de maneira que a sua produtividade ou de outros usuários seja prejudicada.

O uso pessoal ocasional é permissível desde que:

1. Seja formalmente autorizado pelo gestor da área;
2. Não interfira com a produtividade do usuário.

Todos os acessos aos recursos da UNIMED MARÍLIA devem ser formalmente autorizados.

7.2.2 Uso particular ou de terceiros

A conexão de dispositivos pessoais ou de terceiros, tais como computadores, notebooks, tablets, hubs, switches, entre outros, aos equipamentos ou à rede da UNIMED MARÍLIA é estritamente proibida sem a expressa autorização do departamento de Tecnologia e Inovação. Ressalta-se, ainda, que o uso de equipamentos pessoais no ambiente de trabalho através da ancoragem de Wi-Fi de celulares também requer a devida autorização e não é permitido sem a devida permissão.

7.2.3 Mudanças de Configuração

A UNIMED MARÍLIA fornece equipamentos pré-configurados com os padrões da cooperativa para os usuários.

O usuário não tem permissão para mudar a configuração do sistema operacional, nem de instalar novos programas. Da mesma forma, é proibido realizar alterações na configuração de hardware nem conectar periféricos ou outros equipamentos que não tenham sido fornecidos pela cooperativa.

Também não é permitido o compartilhamento de pastas locais em estações de trabalho e notebooks, devendo ser utilizados os compartilhamentos de rede disponibilizados pela cooperativa.

Quaisquer mudanças de configuração que sejam necessárias devem ser solicitadas a área de TI.

7.2.4 Sistema Antivírus

Todos os computadores devem ter sistema de antivírus instalado e ativo conforme os procedimentos da cooperativa. É proibido desativar/desinstalar o sistema de antivírus.

7.2.5 Erradicação de Vírus

Os vírus podem ser complexos e sofisticados, assim os usuários não devem tentar erradicá-los sem ajuda de um especialista. Se os usuários suspeitarem da infecção por um vírus, eles têm que deixar de usar o computador, desconectá-lo de todas as redes e buscar ajuda com área de TI.

7.2.6 Proteção do Equipamento

Todos os PCs, servidores, notebooks e estações de trabalho devem estar seguros por protetor de tela com senha ativada automaticamente para 10 minutos ou menos. Os computadores e terminais deverão ser desligados ou protegidos com mecanismo de travamento de tela (para usuários Windows, tecla “Windows + L”) e controlados por senha, quando não estiverem em uso.

7.2.7 Sistemas Homologados

A UNIMED MARÍLIA possui sistemas homologados para todas as atividades previstas em seus processos. É proibido instalar sistemas que não tenham sido fornecidos pela cooperativa, mesmo que freeware.

No caso de necessidade de uso de um sistema que não tenha sido homologado, os usuários devem solicitar o sistema ao seu gestor ou a área de TI. O sistema deve passar pela homologação antes de ser colocado em produção.

A homologação de novos produtos deve ocorrer em ambiente de rede controlado, que não concorra com o ambiente produtivo.

7.2.8 Cópias de Segurança

Os usuários devem manter todos os documentos eletrônicos importantes e de conteúdo corporativo nos servidores de arquivos, os quais possuem processos automáticos e periódicos de cópias de segurança.

7.2.9 Descarte e Reutilização de Equipamentos

Quando do descarte ou reutilização de um equipamento, seus discos rígidos e eventuais outras mídias devem ter seus dados totalmente sobrescritos de tal maneira que o acesso ao conteúdo seja impossibilitado, antes de serem reutilizados ou descartados. A IT-TI-050 - Descarte de equipamentos descreve o processo.

7.2.10 Mídias Removíveis

Entende-se como mídias removíveis, para efeito desta Política de Segurança, se entende disquete, CD-ROM, CD-R, CD-RW, disco ZIP, drive virtual, pendrives e similares.

As mídias removíveis devem ser destruídas antes do descarte, de tal maneira que o acesso ao conteúdo seja impossibilitado conforme as políticas de Segurança da Informação. Em caso de dúvidas consulte a área de TI para mais detalhes.

O uso de mídias removíveis deve ser controlado. Em especial a gravação de CD/DVDs deve ser feita apenas pelas pessoas autorizadas conforme procedimento da cooperativa.

Os dispositivos USB como pendrive, HD removível ou outro tipo de armazenamento de dados deve ser autorizado pelo Gestor da pessoa e posterior análise e autorização da área de TI.

Não é permitido o uso de mídias removíveis particulares no ambiente da UNIMED MARÍLIA. O uso deve ser considerado um caso especial e necessita de autorização formal conforme os procedimentos da cooperativa.

7.2.11 Guarda do Equipamento

O usuário que utiliza sempre ou na maior parte do tempo o mesmo computador para executar suas tarefas é considerado como responsável pelo equipamento. Se o equipamento foi danificado, perdido ou roubado deve informar prontamente área de TI. A definição de responsabilidade será definida de acordo com a análise do ocorrido e aplicada em conjunto pelas áreas de Segurança Empresarial, Recursos Humanos e Jurídico.

7.2.12 Drives de Rede

Responsabilidades do colaborador ou prestador de serviço interno nos acessos aos drives de rede:

1. Todo acesso a qualquer drive da rede deve seguir as definições de segurança de cada usuário e características de seu agrupamento de trabalho.

2. O acesso ao Drive de Rede (U:\"SETOR\COLABORADOR") é restrito/confidencial apenas ao próprio colaborador, devendo ser armazenado nele apenas arquivos relacionados ao negócio da UNIMED MARÍLIA.

3. O acesso ao Drive de Rede (U:\"SETOR\") é restrito/confidencial aos colaboradores pertencentes ao setor, devendo ser armazenado nele apenas arquivos relacionados ao negócio da UNIMED MARÍLIA.

As seguintes atividades são estritamente proibidas, sem exceções:

1. Gravar qualquer informação CONFIDENCIAL e/ou SECRETA no diretório U:\ Pasta Temporária

2. Gravar qualquer informação com conteúdo impróprio nos drives de rede, como arquivos de músicas, vídeos, fotos e programas que não estejam relacionados ao ambiente de trabalho e/ou as atividades da pessoa.

3. Os usuários devem apagar informações obsoletas dos drives de rede para impedir o acúmulo desnecessário de informações.

7.2.13 Cuidado com Informações Impressas

Informações não devem permanecer em equipamentos de fax e impressoras. Os usuários devem retirar os documentos imediatamente após a impressão.

Da mesma maneira documentos com informações sensíveis devem ser guardados adequadamente (cofres, gavetas e armários com chave) conforme a criticidade das informações neles contidos.

7.2.14 Mensageiro Instantâneo

O Mensageiro Instantâneo (Skype, Teams, WhatsApp ou outros) são programas que permitem a troca de mensagens rápidas entre Colaboradores, Cooperados, Prestadores de Serviços ou outros. As mensagens trocadas são armazenadas e podem ser verificadas pela Segurança. O mensageiro não deve ser utilizado para a troca de qualquer informação pessoal. Cada colaborador ou prestador de serviço será responsável pela troca de informações de maneira adequada a fim de minimizar o risco de expor dados pessoais devido LGPD (Lei Geral de Proteção de Dados). Sempre analisar se de fato aquela informação deve ser compartilhada através desses recursos.

7.2.15 Desligar os Equipamentos

É dever de todos os colaboradores e prestadores de serviço, desligar o computador, monitor, notebook, impressora e todo equipamento eletrônico ao final do expediente, ou quando se ausentar da estação de trabalho por um longo período de tempo. Essa prática é necessária para que as atualizações pendentes sejam realizadas e também para contribuir com a segurança, vida útil do equipamento e economia de energia.

7.3 POLÍTICA DE USO DE PORTÁTEIS E ACESSO REMOTO

7.3.1 Pré-requisito

Antes de ser concedido o acesso remoto ou o uso de um computador portátil, o usuário deve estar ciente do que prega, no mínimo, a política de segurança da informação vigente.

7.3.2 Acesso Remoto

A UNIMED MARÍLIA permite que em determinadas situações os colaboradores possam trabalhar remotamente (Home Office), porém o colaborador deverá:

- Solicitar à TI, através de S3, o cadastro de uso de VPN;
- Possuir equipamentos necessários para realização do trabalho (computador, internet, etc);
- Se o colaborador precisar de algum equipamento emprestado, por um curto período de tempo e a Unimed Marília tiver disponível, o mesmo poderá ser emprestado desde que o colaborador e o gestor preencham o documento DI-TI-004- TERMO DE RESPONSABILIDADE e entreguem assinado para TI.

7.3.3 Uso de Equipamentos Corporativos

Colaboradores que recebem equipamentos corporativos, como notebook, tablets, dentro outros (exceto smartphone) deverão assinar o documento F-CONT-004. O termo de responsabilidade para que usa celular corporativo (smartphone) é o F-COMP-045.

7.3.4 Uso Autorizado

O computador portátil disponibilizado pela UNIMED MARÍLIA, deve ser utilizado exclusivamente pela pessoa autorizada. O uso do equipamento por terceiros, sejam eles sócios, familiares, amigos ou qualquer outro é expressamente proibido.

7.3.5 Cópia de Segurança

Os usuários de computadores portáteis são responsáveis pelas informações neles armazenadas.
É de responsabilidade do usuário manter os dados considerados sensíveis na rede, para que as devidas cópias de segurança sejam realizadas.

7.3.6 Exposição Pública

Material sensível não deve ser lida, manuseado ou discutido em: elevadores, sala de café, refeitório, restaurantes, aviões, ônibus, metrô, trens ou em outros lugares de acesso público.

7.3.7 Bagagem Em Caso De Deslocamento e Viagem

Os equipamentos portáteis, como notebook, smartphone, laptop, palmtop, e outros computadores transportáveis que contenham informação sensível não podem ser despachados como bagagem. Para evitar danos e roubo, esses equipamentos têm que permanecer na posse do viajante como bagagem de mão.

7.3.8 Uso de Celular Corporativo

7.3.8.1. Uso Apropriado

- O aparelho deverá ser utilizado única e exclusivamente a serviço da cooperativa, tendo em vista a atividade a ser desenvolvida;
- Fica proibido o uso do aparelho, em caráter pessoal e particular, para ligações, envio de mensagens de texto, navegação na internet e uso de rede sociais;
- Zelar pelo uso correto e manutenção do aparelho;

7.3.8.2. Segurança e Privacidade

- Mantenha o celular protegido por senha, PIN ou outro método de autenticação seguro.
- Não compartilhe sua senha ou dispositivo com terceiros.
- Utilize apenas aplicativos aprovados pela cooperativa e baixe-os de fontes confiáveis, como a loja oficial de aplicativos.
- Ative recursos de segurança, como o bloqueio automático da tela após um período de inatividade e a criptografia de dados.

7.3.8.3. Proteção de Dados

- Não armazenar informações confidenciais ou sensíveis diretamente no celular. Utilize soluções de armazenamento seguro recomendadas pela cooperativa.
- Qualquer conteúdo trocado através de ferramentas de comunicação usada no celular coorporativo, após cumprir a finalidade, devem ser imediatamente eliminadas ou se necessário a guarda, armazenadas conforme a política descrita no item **7.9 Política de Armazenamento de Arquivos.**
- Realize backups regulares dos dados corporativos.

- Relatar imediatamente qualquer perda, roubo ou incidente de segurança ao departamento de TI.

- Mapear um processo no sistema DPOnet, seguindo as etapas referente ao processo da LGPD e tratar a RMC, se gerada. Cada departamento que utilizar um celular coorporativo, obrigatoriamente, tem que mapear esse processo.

7.3.8.4. Comunicação

- Utilize ferramentas de comunicação aprovadas para troca de informações sensíveis, como o e-mail corporativo.

- Não discutir assuntos confidenciais em ambientes públicos ou não seguros, evitando que pessoas próximas escutem qualquer assunto coorporativo.

7.3.8.5. Comportamento Online

- Não acesse sites não confiáveis ou de conteúdo inadequado usando o celular corporativo.

- Evite clicar em links suspeitos ou abrir anexos de e-mails de remetentes desconhecidos.

7.3.8.6. Manutenção e Suporte

- Mantenha o sistema operacional e os aplicativos do celular sempre atualizados.

- Solicite suporte técnico ao departamento de TI para qualquer problema técnico ou necessidade de atualização.

- Caso o aparelho seja danificado, negligenciado ou extraviado, o valor do equipamento deverá ser ressarcido a cooperativa, conforme (F-COMP-046)**.**

7.3.8.7. Devolução do Dispositivo

- O celular corporativo deve ser devolvido à cooperativa ao término do contrato de trabalho ou quando solicitado.

- Antes de devolver o dispositivo, certifique-se de que todos os dados corporativos foram removidos.

7.3.8.8. Conta Google

- O celular corporativo deve ser utilizado somente com a conta Google fornecida pelo departamento Gestão de Compras, em hipótese alguma, essa conta padrão pode ser substituída pelo colaborador, sem conhecimento do departamento Gestão de Compras.

7.3.8.9. Termo de responsabilidade de uso de telefone celular

- O colaborador ao receber o aparelho, precisa dar ciência no Termo de responsabilidade de uso de telefone celular (F-COMP-046), que fica sob responsabilidade do departamento Gestão de Compras.

7.4 POLÍTICA DE ACESSO À INTERNET

7.4.1 Confiabilidade da Informação

Toda a informação vinda da Internet deve ser considerada suspeita até que se confirme o contrário. Não há nenhum processo do controle de qualidade na Internet, e uma quantidade considerável de informação é ultrapassada, imprecisa ou falsa. Em muitos casos, a informação falsa tem por objetivo fraudar o usuário.

Antes de usar uma informação recebida via Internet para finalidades de tomada de decisão, os usuários devem validar essa informação em pelo menos mais uma fonte confiável.

7.4.2 Verificação de Vírus

Todos os arquivos recebidos através da Internet devem ser verificados através das ferramentas adequadas fornecidas pela UNIMED MARÍLIA. Esta verificação visa evitar a infecção dos computadores por vírus ou outros programas maliciosos.

7.4.3 Divulgação de Informações

Os usuários não devem divulgar informações internas através da Internet, por exemplo em mídias sociais ou blogs. Informações que de algum modo possam afetar a UNIMED MARÍLIA nas suas relações com os clientes, fornecedores ou imagem pública são expressamente proibidas.

A divulgação de informações ao público deve ser efetuada através da área de Comunicação da Unimed Marília.

7.4.4 Uso Pessoal

Os usuários não devem utilizar-se da Internet ou outros sistemas de informação interna de maneira que a sua produtividade ou de outros usuários seja prejudicada.

A navegação ou acesso a locais com conteúdo abaixo relacionados é expressamente proibida, a menos que faça parte das suas atividades diárias de trabalho:

1. Vírus, jogos, pornografia;
2. Sons, vídeos, imagens não relacionados com o trabalho;
3. Conteúdos de orientação sobre partidos políticos, religiosa, racial, sexual ou tratando de qualquer atividade ilegal.

7.4.5 Registros

A UNIMED MARÍLIA se reserva o direito de registrar os sites visitados, os "downloads" efetuados, o tempo de acesso e a informação consultada.

A solicitação dos registros para eventuais análises deve ser efetuada à área de Tecnologia e Inovação.

7.5 POLÍTICA DE USO DE CORREIO ELETRÔNICO

7.5.1 Propriedade da Companhia

Como uma ferramenta de produtividade, a UNIMED MARÍLIA encoraja o uso do correio eletrônico.

O seu uso implica o reconhecimento de que os sistemas de comunicações eletrônicas e todas as mensagens geradas ou transmitidas através dos mencionados sistemas são de propriedade da UNIMED MARÍLIA, podendo ser monitoradas.

7.5.2 Uso Autorizado

Os sistemas de comunicações eletrônicas da UNIMED MARÍLIA devem ser usados unicamente para atividades do trabalho. Para o uso do correio eletrônico é obrigatória a utilização de senha e Login pessoal e intransferível.

O uso pessoal ocasional é permissível desde que:

1. Não interfira com a produtividade;
2. Não tenha prioridade sobre nenhuma atividade da UNIMED MARÍLIA;

7.5.3 Regras para Criação de Contas de E-mail

Na composição dos nomes de contas de e-mail, deverá ser seguido um dos seguintes modelos de criação:

a. <nome>.<sobrenome>@unimedmarilia.com.br;

   OBS: Se necessária alteração de login, comunicar a T.I.

7.5.4 Proibições

As seguintes atividades são estritamente proibidas, sem exceções:

1. Enviar mensagens não solicitadas, incluindo o envio de "*junk mail*" ou outros materiais de propaganda a indivíduos que não tenham requisitado especificamente estes materiais (e-mail spam);
2. Qualquer forma de assédio via e-mail, quer através da linguagem, frequência, tamanho ou conteúdo das mensagens;
3. Postar e-mails ou mensagens não relacionadas ao negócio da UNIMED MARÍLIA em listas ou newsgroups;
4. Utilizar o e-mail da UNIMED MARÍLIA para fins não relativos ao negócio da UNIMED MARÍLIA;

7.5.5 Armazenamento da Senha

Embora os clientes de correio eletrônico ofereçam essa opção, os usuários não devem salvar sua senha de acesso para evitar acessos não autorizados.

7.5.6 Privacidade

A UNIMED MARÍLIA não pode garantir que as comunicações eletrônicas serão privadas. Os usuários devem estar atentos ao fato que comunicações eletrônicas podem, enquanto dependendo da tecnologia, ser interceptadas, impressas ou armazenadas por terceiros.

7.5.7 Proteção

Todos devem estar cientes que os sistemas de comunicações eletrônicas não são protegidos automaticamente.

Todos devem ter extrema cautela ao abrir e-mails com anexos recebidos de fontes desconhecidas, pois os mesmos podem conter vírus, bombas de e-mail, ou códigos de cavalos-de-tróia. Anexos e mensagens devem ser verificadas com antivírus.

7.5.8 Conteúdos de Mensagens

Os usuários não devem utilizar termos obscenos ou observações pejorativas em mensagens de correio eletrônico.

É proibido utilizar os recursos de correio eletrônico para:

1. Arquivos contendo vírus, jogos, música, pornografia, vídeo ou imagens não relacionadas com o trabalho.
2. Mensagens de propaganda ou venda de produtos com fins particulares.
3. Cartas de corrente ou “spam”.
4. Mensagens de orientação política, religiosa, racial, sexual ou que configurem atividade ilegal.

7.5.9 Mensagens Suspeitas

Os usuários devem remeter para a área de TI as mensagens suspeitas que receberem, quando julgarem que isso é necessário para prevenir outros usuários. Em especial, mensagens com o objetivo de fraudar o usuário ou a cooperativa devem ser enviadas para a área de TI ti@unimedmarilia.com.br, com o assunto “Fraude”.

7.5.10 Respostas Automáticas e Encaminhamento de E-mail

Os usuários devem cadastrar respostas automáticas no período que estiverem ausentes da cooperativa, quando o período de ausência for superior a 5 dias.
Não é recomendado habilitar o encaminhamento de e-mail para que outros usuários recebam essas mensagens.
A decisão de habilitar o encaminhamento ficará sob responsabilidade do gestor.

7.6 POLÍTICA DE SEGURANÇA EM RECURSOS HUMANOS

7.6.1 Segurança na Seleção de Pessoal

Durante os processos de recrutamento e seleção, devem ser atendidas as condições definidas na Política de Gestão de Pessoas contidas no documento W:\Gestão da Qualidade\DOCUMENTOS SGQ\Processo de Recursos Humanos\DOCUMENTOS VIGENTES\DI - IT - Regulamento Interno e Instrução de Trabalho\DI-RH-009 -Política de gestão de pessoas.doc.

7.6.2 Responsabilidades

7.6.2.1 Contratação de Colaboradores, Estagiários e Temporários

O processo de seleção, treinamento, transferência e demissão de colaboradores e estagiários e temporários é de responsabilidade da área de Recursos Humanos juntamente com o Gestor da área onde a pessoa exerce suas atividades.

7.6.2.2 Contratação de Terceiros e Prestadores

O processo de seleção, treinamento, transferência e demissão de terceiros é de responsabilidade do gestor da área contratante.

Cada gestor é responsável pelas ações dos seus terceiros. Deve solicitar o login (para os casos desta necessidade) a área de TI, solicitar renovação no caso desta necessidade e obrigatoriamente cancelar este login em casos de demissão, afastamento ou término do contrato.

7.6.3 Segurança na Integração

Os novos colaboradores devem passar por um processo de integração que inclua um treinamento em segurança da informação. Esse treinamento tem por objetivo deixar clara a importância da segurança da informação para o negócio da UNIMED MARÍLIA e estimular o cumprimento voluntário da política.

Na integração, os colaboradores devem ser claramente informados das funções de segurança em que estarão inseridos, bem como das responsabilidades a eles atribuídas.

Durante este processo, os colaboradores deverão assinar um documento indicando que leram a Política de Segurança da Informação e se comprometem a segui-la.

7.6.4 Desligamento

Quando do desligamento de pessoal, a área de Recursos Humanos em conjunto com o gestor da pessoa deve analisar a necessidade de realizar uma entrevista de desligamento. Caso seja realizada, na entrevista devem ser relembradas as responsabilidades com relação ao sigilo das informações manipuladas quando trabalhando na UNIMED MARÍLIA, destacando que os compromissos de confidencialidade permanecem em vigor, mesmo depois de encerrado o contrato de trabalho.

As devidas providências devem ser tomadas para que sejam revogados todos os acessos lógicos e físicos da pessoa que está sendo desligada bem como a devolução de todos os ativos físicos pertencentes à UNIMED

MARÍLIA como notebooks, desktops, celular/smartphone, assim como mídia ou cópia de alguma informação da cooperativa que esteja sob a custódia da pessoa.

Após comunicado de desligamento, será destacado um colaborador do RH para acompanhar o demitido a sua posição de trabalho para apanhar seus pertences, se despedir de seus colegas de setor, se desejar, porém não lhe será permitido acesso a computadores ou qualquer documento, por fim, será conduzido até a recepção, este processo não deverá durar mais que trinta minutos.

Adicionalmente, não é permitida a gravação ou impressão de dados utilizados pelo colaborador ou prestador de serviço, durante o exercício de suas funções, independente da mídia utilizada ou dos sistemas onde os dados estão armazenados no momento do seu desligamento. Estas informações, uma vez armazenadas nos sistemas da cooperativa, são consideradas de propriedade da UNIMED MARÍLIA e após o desligamento os dados serão eliminados.

Poderá ser utilizado o documento “perfil de rede” F-RH-004 para a T.I. realizar a desativação dos acessos aos sistemas.

7.6.5 Conscientização Periódica

Os colaboradores ou prestadores de serviços devem participar de reforços periódicos de conscientização em segurança da informação conforme o agendamento feito pela cooperativa. O conteúdo deste treinamento deve permitir que as pessoas reconheçam os problemas e incidentes de segurança da informação e respondam de acordo com as necessidades do negócio.

7.7 POLÍTICA DE SEGURANÇA FÍSICA E DO AMBIENTE

7.7.1 Perímetros de Segurança

Para evitar acesso não autorizado, dano ou interferência aos sistemas de informação considerados sensíveis, perímetros de segurança devem ser claramente definidos. Salas de Servidores, Equipamentos de Rede e No-breaks, devem possuir as devidas proteções utilizadas em perímetros de segurança.

Barreiras físicas e sistemas de controle de acesso devem ser implementados para garantir o acesso apenas por pessoas autorizadas.

Um perímetro de segurança deve ter, no mínimo, as seguintes características:

1. Paredes, portas e teto com solidez adequada;

2. Um sistema de portaria, recepção e identificação eletrônica para controle e registro dos acessos.

Todo acesso ao ambiente da UNIMED MARÍLIA, exceto ao setor de atendimento presencial, deve ser precedido de uma identificação na recepção. A recepção deve, obrigatoriamente, solicitar um documento de identificação oficial (Carteira de Identidade ou CNH e passaporte, no caso de estrangeiros), para garantir a identidade do visitante. A recepção só liberará o acesso da pessoa com o crachá de identificação quando o colaborador responsável for recebe-la para acompanha-la no prédio da Unimed Marília.

Os colaboradores ou prestadores de serviços devem sempre questionar a presença de pessoas não conhecidas ou não identificadas nos ambientes de trabalho interno da UNIMED MARÍLIA.

Todas as atividades dentro de um perímetro de segurança devem ser previamente autorizadas e monitoradas conforme o nível de criticidade do perímetro.

As portas de acesso a um perímetro de segurança devem sempre ser mantidas fechadas e todos os trabalhos de prestadores de serviços externo devem ser acompanhados.

Todas as atividades executadas por terceiros dentro do datacenter devem ser acompanhadas durante todo o tempo por um colaborador da UNIMED MARÍLIA.

7.7.2 Colaboradores

Colaboradores devem sempre realizar a entrada pelo local indicado, acesso liberado apenas por leitura biométrica, previamente cadastrada para controle e segurança do ambiente.

7.7.3 Visitantes

Visitantes devem ser sempre acompanhados e a visita deve ser previamente agendada e autorizada.

7.7.4 Área de Carga e Recebimento

O recebimento de cargas ou equipamentos deve ser efetuado somente pelas pessoas autorizadas.

7.7.5 Equipamentos e Instalações

Os servidores ou outros equipamentos considerados críticos devem ser protegidos contra ameaças físicas como: roubo, fogo, poeira, água, temperatura e outras relevantes.

As seguintes atividades não são permitidas em áreas com equipamentos críticos:

1. Guarda de Materiais inflamáveis.
2. Comer e beber.
3. Fumar.

7.7.6 Transporte de Material para Fora da Cooperativa

Equipamentos, mídias, licenças de software, informações ou qualquer outro ativo de propriedade da UNIMED MARÍLIA não podem ser retirados da cooperativa sem autorização prévia.

7.7.7 Uso de Crachá

Toda e qualquer pessoa que adentrar as Unidades da UNIMED MARÍLIA deverá estar portando obrigatoriamente o seu próprio crachá, em local visível, que liberará seu acesso às áreas preestabelecidas.

7.7.8 Mesa Limpa

Todo e qualquer documento ou mídia de armazenamento eletrônico deve ser guardado em local seguro (idealmente em armários ou outras formas de mobília de segurança), quando não estiver em uso, especialmente ao final do expediente quando o local estiver desocupado. Cabe ao gestor informar aos

colaboradores e prestadores de serviço sobre esta prática de guarda e designar quem pode ter posse da chave, que deverá estar descrito na Instrução de Trabalho.

7.7.9 Ambiente monitorado

Toda a cooperativa dispõe de câmeras de segurança para controle de acesso, as gravações ficam armazenadas por um determinado período e caso seja necessário, poderá ser acionado para resolver algum incidente.

7.8 POLÍTICA DE OPERAÇÕES E GERÊNCIA DE SISTEMAS

7.8.1 Segurança na Documentação dos Recursos de TI

A documentação dos recursos de TI deve ser armazenada em local seguro e o acesso deve ser restrito apenas às pessoas que necessitem das informações.

7.8.2 Inventário dos Recursos

A área de TI é responsável por manter um inventário de softwares e hardwares de propriedade da UNIMED MARÍLIA ou sob sua guarda, identificando os proprietários.

7.8.3 Cópias de Segurança

É de responsabilidade da área de TI implementar um processo para realização de cópias de segurança dos dados armazenados e processados, exclusivamente, nos servidores corporativos; equipamentos como desktops e notebook não fazem parte do escopo. O processo deve contemplar as ações necessárias para a que as informações sejam recuperadas, em casos de emergências, no menor tempo possível.

7.8.3.1 Periodicidade

É de responsabilidade da área de TI em comum acordo com a área solicitante e também com legislações aplicáveis definir a frequência de execução do backup, tempo de retenção e testes de recuperação para as cópias de segurança realizadas.

7.8.4 Licenças de Software

As licenças de softwares adquiridos pela UNIMED MARÍLIA devem ser registradas e armazenadas em local seguro.

É vedado o uso de uma licença pessoal por duas ou mais pessoas, bem como o uso de qualquer software sem a devida licença ou de forma contrária à autorizada pelo licenciante.

7.9 POLÍTICA DE ARMAZENAMENTO DE ARQUIVOS

7.9.1 Objetivo

Esta política estabelece diretrizes claras para o armazenamento de arquivos da cooperativa, com o intuito de proteger dados sensíveis, garantir a integridade das informações e assegurar que todos os dados críticos sejam devidamente respaldados. A proteção adequada e o gerenciamento eficaz dos dados são fundamentais para a segurança e a continuidade dos processos.

7.9.2 Armazenamento local não autorizado

Todos os colaboradores e prestadores de serviço estão estritamente proibidos de salvar arquivos diretamente nos discos rígidos locais (e.g., C:\ drive) de seus computadores corporativos ou de qualquer outro equipamento móvel utilizado. O armazenamento local é vulnerável a falhas de hardware, perda de dados e não oferece suporte adequado para backup.

7.9.3 Locais de Armazenamento Autorizados

Os arquivos devem ser salvos exclusivamente em locais designados que possuem backup regular e são monitorados pela equipe de TI. Esses locais incluem, mas não se limitam a:

- Servidores de arquivos corporativos (Driver U);
- Serviços de armazenamento em nuvem corporativos (Microsoft 365, SharePoint, OneDrive);
- Prontuário Eletrônico do Paciente (PEP);
- GEDPRIME – Ferramenta responsável pelo gerenciamento eletrônico de documentos.

7.9.4 Justificativa

A centralização do armazenamento de dados em locais autorizados e com backup garante:

Segurança: Proteção contra perda de dados por falhas de hardware ou ataque cibernético.

Integridade: Manutenção da consistência e precisão dos dados.

Recuperação de Dados: Capacidade de restaurar dados a partir de backups em caso de exclusão acidental ou corrupção de dados.

Conformidade: Adesão às normas e regulamentações de proteção de dados.

7.9.5 Monitoramento e Conformidade

A equipe de TI realizará auditorias regulares para garantir a conformidade com esta política. O não cumprimento poderá resultar em medidas disciplinares, conforme estipulado nos regulamentos internos da empresa.

A adesão a esta política é essencial para a proteção de nossos ativos digitais e a continuidade de nossas operações.

7.9.6 Responsabilidades da TI

A TI não se responsabiliza pela perca de arquivos diretamente salvos nos discos rígidos locais, em desacordo com as orientações contidas nessa Política.

Em caso de formatação do computador, a TI se limita a salvar somente arquivos locais, quando relacionados a algum software específico utilizado no computador corporativo, desde que solicitado e registrado pelo solicitante em chamado S3.

7.10 POLÍTICA RELACIONADA A LGPD (LEI GERAL DE PROTEÇÃO DE DADOS)

7.10.1 Comitê da LGPD e Segurança da Informação

Existe um comitê interno formado com no mínimo um representante de cada setor para acompanhamento de ações relacionadas à LGPD e multiplicação do conhecimento com os demais colaboradores e prestadores de serviço. É fundamental que os membros, juntamente com os gestores avaliem periodicamente o tratamento dos dados e os impactos em novas operações, ou mudanças.

7.10.2 Canais de Atendimento ao Titular de Dados

A LGPD exige que as empresas disponibilizem um canal de comunicação oficial para que os titulares de dados possam fazer suas manifestações. É essencial que todos os colaboradores e prestadores de serviço conheçam essa informação para ajudar a disseminá-la e orientar os titulares de dados em caso de dúvidas.
Para acessar o formulário online, visite o site www.unimedmarilia.com.br. No menu LGPD, você será direcionado ao portal "Privacidade & Você", onde encontrará o Formulário de Atendimento ao Titular de Dados. Esse formulário permite que os titulares façam suas solicitações online, com acompanhamento em tempo real pelo nosso DPO.
Como medida de contingência, caso haja instabilidade no canal online, um formulário físico (F-ATEND-065) está disponível no EPA e pode ser preenchido manualmente.
Para dúvidas ou informações adicionais, entre em contato com nossa Central de Atendimento, disponível 24 horas por dia, sete dias por semana, pelo telefone 0800 201 2500.

7.10.3 Beneficiários / Prestadores / Terceiros

Todos os processos precisam se preocupar e garantir que haja uma confirmação de dados antes de fornecer informações aos beneficiários, prestadores ou terceiros para garantir que realmente o solicitante é ele mesmo. Dicas: Perguntar data de nascimento, CPF, criar formulários padrões, etc.

Periodicamente, é preciso revisar processos de modo a garantir que somente são solicitados dados pessoais que realmente são necessários para o andamento da operação, caso contrário, deixar de pedir informações desnecessárias, com o objetivo de reduzir riscos.

Existe um formulário disponível no site (formulário de atendimento ao titular de dados) e também um formulário físico (para atendimento presencial) F-ATEND-065 - Solicitação de Informação de titular – LGPD, onde o beneficiário pode solicitar revisão ou exclusão de dados.

Em todo contrato firmado entre a cooperativa e terceiros, deverá conter uma cláusula de proteção e uso de dados pessoais.

7.10.4 Qualidade

Os processos são revisados e tratados conforme o Sistema de Gestão da Qualidade, através do documento P-SGQ-001 - Controle de Documentos e Registros, onde cada setor é responsável por avaliar e revisar as informações de impacto de dados pessoais em seus novos processos ou apenas em processos revisados e registrar no sistema de tratamento de dados DPO.NET.

7.10.5 Descarte de Informações Físicas

Todos os processos que necessitam de trabalhar com informações impressas, deverão criar regras para definição de prazo de exclusão/descarte desses documentos. Documentos contento informações sensíveis e dados pessoais não poderão ser utilizados para fazer bloco de rascunho, deverão ser triturados através de equipamento próprio a fim de minimizar riscos de vazamento de dados.

7.10.6 Acervo ou Arquivo Morto

A responsabilidade do acerto e arquivo morto é da GEDPRIME, empresa terceira que foi contratada com a finalidade de coletar, cuidar, controlar acesso, armazenar e descartar documentos físicos. O descarte só acontece através de protocolo assinado dos envolvidos.

O setor de gestão de serviços tem o documento DI-GS-005 - GESTÃO DOCUMENTAL – ARQUIVO, onde descreve o processo.

7.10.7 Reutilização e Alienação Segura de Equipamentos

Todos os equipamentos que contenham mídias de armazenamento de dados são examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos (com exceção de OEM) com segurança, antes do descarte, reutilização ou alienação.

8. DESCUMPRIMENTO DAS NORMAS

É de responsabilidade de todo colaborador, conselheiro ou prestador de serviço interno, zelar pelo cumprimento da Política de Segurança da Informação da UNIMED MARÍLIA. Nos casos de descumprimento desta Política, o colaborador ou prestador de serviço interno deve relatar à Ouvidoria Interna através dos canais de comunicação por ela disponibilizados.

Em casos de incidentes de segurança a área de TI, se necessário, poderá notificar os colaboradores ou prestadores de serviço quanto ao descumprimento das normas de segurança da informação.

8.1 PENALIDADES

Qualquer colaborador ou prestador de serviço interno que violar esta política está sujeito às sanções aplicáveis por lei ou contrato, inclusive a demissão por justa causa e a resolução por inadimplemento.