




UNIMED CHAPECÓ

CONTROLES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE DE DADOS PESSOAIS

2ª Edição

Chapecó - SC
2021

	<p align="center">CONTROLES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE DE DADOS PESSOAIS</p>	<p align="right">MAN.GOV.0004/01 Implantação: 06/2021 1º Revisão: 10/2021 Classificação: INTERNO</p>
--	--	--

1. INTRODUÇÃO

Para assegurar que as informações tratadas estejam adequadamente protegidas, a Unimed Chapecó adota medidas de controles para segurança das informações e dos dados pessoais tratados.

Esse Manual contém as medidas técnicas e administrativas para proteção da integridade, segurança e fidedignidade dos dados tratados, abrangendo os controles para os processos de captura, produção, armazenamento, uso e compartilhamento de dados, com vistas a garantir a qualidade dos dados e informações tratadas pela Unimed Chapecó.

Os controles versam sobre medidas de segurança do ambiente de tecnologia, controles para a extração de dados, controles para acesso às informações, medidas de segurança para o acesso físico, descarte seguro de ativos e segurança móvel.

Este Manual absorve a antiga Política de Utilização de Rede de Informática (PLI.TI.0001).

2. APLICAÇÃO

As diretrizes estabelecidas neste manual foram elaboradas de acordo com a Política de Segurança da Informação e Privacidade de Dados Pessoais e aplicam-se a todos os setores organizacionais e unidades de negócio da Unimed Chapecó, devendo ser observadas em todas as operações e atividades realizadas pela Cooperativa, no que diz respeito aos controles de segurança da informação e de privacidade de dados pessoais.

3. CONFIDENCIALIDADE

Classificação do documento: **INTERNO**.


Este documento pertence à Unimed Chapecó, para fins de utilização, única e exclusiva, de seus colaboradores e administradores.

É proibida a reprodução no todo ou em parte, bem como a divulgação e/ou disponibilização a terceiros, sob qualquer motivo, salvo nos casos analisados e aprovados, formalmente, pela Diretoria Executiva; ou pelo Comitê de GRC; ou pelo Conselho de Administração da Unimed Chapecó.

4. SEGURANÇA DO AMBIENTE DE TECNOLOGIA DA INFORMAÇÃO

Neste tópico são definidas medidas de segurança do ambiente de tecnologia.

Elaborado: Segurança da Informação Núcleo de Governança Corporativa	Revisado: Comissão de Segurança da Informação e Privacidade de Dados Pessoais	Aprovado: Comitê de GRC Unimed Chapecó
--	--	---

	<p align="center">CONTROLES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE DE DADOS PESSOAIS</p>	<p align="right">MAN.GOV.0004/01 Implantação: 06/2021 1º Revisão: 10/2021 Classificação: INTERNO</p>
--	--	--

4.1 Proteção de estações de trabalho

As estações de trabalho devem possuir antivírus instalado e atualizado e ser bloqueadas para uso de drives externos, assim como para instalação de softwares pelos usuários, sendo possível apenas a instalação de softwares homologados, sendo este procedimento realizado pelo setor de Tecnologia da Informação (TI). Em caso de extrema necessidade a TI deverá avaliar a liberação, mediante aprovação da Gerência, mantendo relação de máquinas liberadas. Não deve ser permitida a conexão física ou lógica à rede da Cooperativa, por equipamentos particulares e/ou não gerenciados ou não homologados pelo setor de TI.

4.2 Armazenamento de dados em diretórios de rede

O diretório de rede de acesso interno público (fileserver\gerais) não deverá ser realizado para armazenamento de arquivos que contenham informações confidenciais, restritas e dados pessoais de natureza sensível. Tais informações devem ser armazenadas em diretórios de rede específicos (fileserver\nome do setor), com acesso controlado e restrito aos usuários que necessitam utilizar tais informações.

Caso algum arquivo precise ser mantido no diretório de rede de acesso interno público (fileserver\gerais), para uso compartilhado entre setores, deverá possuir senhas de acesso de responsabilidade do usuário.

4.3 Proteção de perímetro

Para proteção da informação contra ataques externos ou o acesso por pessoas não autorizadas, o setor de TI deve implementar ferramentas e medidas de controle preventivas instaladas em dispositivos móveis, estações de trabalho, no serviço de correio eletrônico, no serviço de navegação WEB e no serviço de impressão, tais como: firewall, criptografia, segmentação da rede interna e externa.


5. CONTROLE PARA EXTRAÇÃO DE DADOS

Para limitar a extração de dados, utiliza-se de mecanismos de proteção, bem como, orientações aos colaboradores.

5.1 Drives externos

A liberação de acesso USB só é concedida mediante autorização da Gerência/Diretoria. É realizado configuração no Domínio para bloqueio de todas as portas USB de cada estação de

Elaborado: Segurança da Informação Núcleo de Governança Corporativa	Revisado: Comissão de Segurança da Informação e Privacidade de Dados Pessoais	Aprovado: Comitê de GRC Unimed Chapecó
--	--	---

	<p align="center">CONTROLES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE DE DADOS PESSOAIS</p>	<p align="right">MAN.GOV.0004/01 Implantação: 06/2021 1º Revisão: 10/2021 Classificação: INTERNO</p>
--	--	--

trabalho. O setor de Tecnologia da Informação deverá manter registro atualizado de acessos concedidos, bem como, a justificativa para tal liberação.

5.2 Restrições

Não é permitido a qualquer usuário, fazer fotos com celulares particulares da tela dos sistemas de gestão, principalmente do Prontuário Eletrônico do Paciente (PEP).

Nos computadores assistenciais, a função Print Screen deverá estar desabilitada, visto não ser permitido a extração de dados do PEP.

Não é recomendado o uso do E-mail, WhatsApp, Telegram, ou qualquer outro aplicativo particular de troca de mensagens ou arquivos, para o compartilhamento de informações sigilosas ou dados pessoais sensíveis (sujeitos ao sigilo médico) tratados pela Cooperativa.

6. CONTROLE DE ACESSO ÀS INFORMAÇÕES


Controles para acesso às informações armazenadas no ambiente de tecnologia da informação (banco de dados, sistemas, diretórios de rede e ferramentas de disponibilização e apresentação de painel, indicador e dashboard a clientes), incluindo os dados pessoais tratados pela Unimed Chapecó.

6.1 Termo de confidencialidade e uso das informações

Os colaboradores da Unimed Chapecó devem aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de segurança da informação e privacidade de dados pessoais. O termo de confidencialidade, dando ciência à Política de Segurança da Informação e Privacidade de Dados Pessoais, bem como aos seus Manuais, deve ser assinado por toda a força de trabalho, devendo constar, inclusive, como documento do processo de admissão, arquivado pelo setor de Gestão de Pessoas (GP) na pasta do funcionário.

Os contratos firmados pela Unimed Chapecó com clientes, funcionários, fornecedores, prestadores de serviço, assistencial ou não, administradores e cooperados, devem possuir cláusulas de ciência e comprometimento e responsabilização em relação à confidencialidade e ao uso adequado das informações, incluindo dados confidenciais e pessoais. Os contratos firmados com terceiros devem conter cláusula de confidencialidade e de concordância com os termos da Política de Segurança da Informação e Privacidade de Dados Pessoais.

Elaborado: Segurança da Informação Núcleo de Governança Corporativa	Revisado: Comissão de Segurança da Informação e Privacidade de Dados Pessoais	Aprovado: Comitê de GRC Unimed Chapecó
--	--	---

	<p align="center">CONTROLES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE DE DADOS PESSOAIS</p>	<p align="right">MAN.GOV.0004/01 Implantação: 06/2021 1º Revisão: 10/2021 Classificação: INTERNO</p>
--	--	--

6.2 Criação de usuários

Os usuários do ambiente de TI têm um único ID de acesso em cada ambiente que seja necessário o credenciamento. Este ID de acesso será válido pelo período do vínculo ativo de trabalho com a Unimed Chapecó e não deve ser reaproveitado para outros usuários, mesmo após o término das necessidades de uso inicial.

É proibido aos usuários o compartilhamento de login e senha, bem como realizar qualquer ação utilizando ID de acesso individual para que não tenha sido autorizado. As atividades realizadas por um determinado ID de acesso serão de responsabilidade do respectivo usuário.

O setor de Gestão de Pessoas deve comunicar ao setor de Tecnologia da Informação, por meio do Intratarefas, os novos colaboradores, para que seja criado usuário para acesso ao ambiente de Tecnologia.

Os coordenadores dos setores da Cooperativa devem solicitar ao setor de Tecnologia da Informação a criação de usuários para terceiros, tais como consultores, auditores e clientes, quando necessário, limitando o acesso aos dados, com posterior revogação de acesso imediatamente após a utilização destas credenciais

6.3 Senhas de acesso


O setor de Tecnologia da Informação, no momento da criação dos usuários para acesso ao ambiente de tecnologia, deve estabelecer processo de criação e envio de senhas aos novos usuários. Para a criação de novas contas é necessário somente o nome completo. O nome do perfil do usuário é definido com base no nome do mesmo e uma senha padrão é repassada para o colaborador.

A senha de acesso de cada usuário é pessoal e intransferível, tendo este a responsabilidade de garantir o sigilo, não sendo permitido o compartilhamento das senhas entre usuários.

As senhas de acesso ao ambiente de TI deverão seguir o seguinte padrão:

- a) mínimo de 8 caracteres;
- b) conter letras minúsculas e maiúsculas;
- c) conter caracteres especiais, como: @, !, #, \$, %, *, etc.;
- d) conter números;
- e) expirar, no máximo, após 180 dias, sendo obrigatória sua substituição, por nova senha, diferente das últimas 2 senhas utilizadas.

Elaborado: Segurança da Informação Núcleo de Governança Corporativa	Revisado: Comissão de Segurança da Informação e Privacidade de Dados Pessoais	Aprovado: Comitê de GRC Unimed Chapecó
--	--	---

	CONTROLES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE DE DADOS PESSOAIS	MAN.GOV.0004/01 Implantação: 06/2021 1º Revisão: 10/2021 Classificação: INTERNO
--	--	--

O que não se deve utilizar:

- a) datas pessoais, tais como número de CPF, RG, CRM, data de nascimento, nascimento do filho, data de casamento, dentre outras;
- b) nomes próprios e/ou de parentes;
- c) numeração sequencial (ex: 12345678);
- d) senhas utilizadas externamente de uso pessoal.

A senha de acesso ao ambiente de TI de cada usuário, será bloqueada automaticamente após 05 tentativas incorretas, necessitando contatar o setor de TI para liberação.

6.4 Alteração das senhas de acesso

Caso o usuário esqueça a senha de acesso ao sistema, é necessário entrar em contato com a equipe de TI, onde a equipe técnica redefinirá a senha.

A mesma senha do AD (Active Directory) é vinculada para acesso aos computadores, comunicadores, sistema MV e e-mail.

6.5 Concessão de acesso aos sistemas, bancos de dados e diretórios de rede

A concessão de acesso ao ambiente de TI deve ser efetuada pelo setor de Tecnologia mediante as seguintes aprovações prévias e formais:


- Coordenador ou gerente do setor do colaborador que necessita do acesso ao sistema;
- Gestor da informação, responsável por conceder acesso a um determinado sistema, módulo do sistema, banco de dados ou diretório de rede.

Exemplo 1: Para concessão de acesso ao sistema Contábil para um colaborador do setor de autorizações, deve ser obtida a aprovação do coordenador do setor de autorizações (gestor do colaborador), assim como do coordenador do setor de contabilidade (gestor da informação);

Exemplo 2: Para concessão de acesso ao diretório de rede do setor de Gestão de Pessoas, para um colaborador do setor Financeiro, deve ser obtida a aprovação do coordenador do setor Financeiro (gestor do colaborador), assim como do coordenador do setor de Gestão de Pessoas (gestor da informação).

- Os registros das atividades com a respectiva identificação dos responsáveis pela requisição, aprovação, concessão, comprovação e revogação dos acessos, devem ser realizados através do intratrefas preservando o controle do processo.

Elaborado: Segurança da Informação Núcleo de Governança Corporativa	Revisado: Comissão de Segurança da Informação e Privacidade de Dados Pessoais	Aprovado: Comitê de GRC Unimed Chapecó
--	--	---

	CONTROLES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE DE DADOS PESSOAIS	MAN.GOV.0004/01 Implantação: 06/2021 1º Revisão: 10/2021 Classificação: INTERNO
--	--	--

6.6 Revisão periódica de acesso aos sistemas, bancos de dados e diretórios de rede

O Núcleo de Governança Corporativa (NGC) deve conduzir processo, pelo menos uma vez ao ano, de revisão dos usuários com acesso ativo ao ambiente de tecnologia da informação, com apoio dos coordenadores e gerentes dos setores, visando identificar:

- Usuários com acesso indevido;
- Acessos que não atendem aos requisitos de segregação de funções, ou seja, situações em que um único usuário possa executar e controlar o processo durante todo seu ciclo de vida, do início ao fim de uma transação no sistema, como por exemplo: i) cadastrar fornecedores; ii) cadastrar pagamentos; e iii) liberar /aprovar pagamentos.

O NGC deve solicitar ao setor de TI a adequação e/ou revogação dos acessos considerados indevidos e/ou conflitantes, após validar com os coordenadores e/ou gerentes dos setores, podendo o caso, quando necessário, ser submetido para análise e deliberação da Comissão de Segurança da Informação e Privacidade de Dados Pessoais e ao Comitê de GRC.

6.7 Bloqueio e exclusão de acesso aos sistemas, bancos de dados e diretórios de rede

O setor de Gestão de Pessoas deve comunicar, diariamente, ao setor de Tecnologia da Informação, os colaboradores transferidos, promovidos e desligados.

Nos casos de transferência e/ou promoção, o setor de TI deve solicitar a aprovação do novo gestor do colaborador, assim como do gestor da informação, para que o colaborador permaneça com os acessos vigentes e/ou receba novos acessos requeridos para exercer suas novas funções.


Nos casos de colaborador desligado, o setor de TI deverá bloquear, imediatamente (dentro de 24h do desligamento), o acesso do respectivo usuário ao ambiente de tecnologia da informação.

6.8 Gravação de Logs

É obrigatória a gravação de logs ou trilhas de auditoria do ambiente computacional, para todos os dados sensíveis tratados, de forma a permitir identificar: quem fez o acesso, quando o acesso foi feito, o que foi acessado e como foi acessado.

Essas informações devem ser protegidas contra modificações e acessos não autorizados.

Elaborado: Segurança da Informação Núcleo de Governança Corporativa	Revisado: Comissão de Segurança da Informação e Privacidade de Dados Pessoais	Aprovado: Comitê de GRC Unimed Chapecó
--	--	---

	<p align="center">CONTROLES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE DE DADOS PESSOAIS</p>	<p align="right">MAN.GOV.0004/01 Implantação: 06/2021 1º Revisão: 10/2021 Classificação: INTERNO</p>
--	--	--

7. SEGURANÇA FÍSICA PARA ACESSO ÀS DEPENDÊNCIAS DA UNIMED CHAPECÓ

Medidas de segurança para o acesso físico também são importantes e devem ser observadas.

7.1 Mecanismos de segurança e monitoramento de acesso

A Unimed Chapecó se reserva o direito de instalar câmeras e gravar imagens de todos os ambientes que compõem suas instalações administrativas e ambulatoriais, desde que não violem a privacidade e a intimidade das pessoas.

Todas as gravações estão de posse do setor de Tecnologia da Informação, podendo ser requisitadas por solicitação à equipe responsável desde que dentro do prazo de 30 dias, que é o tempo em que as mesmas ficam disponíveis. Os pedidos de acesso às imagens deverão ser autorizados pela gerência.

7.2 Controles para acesso físico às áreas administrativas

É de responsabilidade do setor de Gestão de Pessoas o fornecimento de crachás de acesso às instalações da Unimed Chapecó. Os cartões de acesso devem ser mantidos com seus respectivos proprietários e não devem ser emprestados em hipótese alguma. O extravio ou roubo dos crachás de acesso deve ser informado imediatamente ao GP para realização do bloqueio do mesmo.


Para acessar o setor Administrativo, existe portão com controle de acesso com crachá. A liberação do portão sem crachá é realizada pelo setor de telefonia, que deverá anotar o nome da pessoa e o destino da entrada. Os demais colaboradores não deverão permitir a entrada de pessoas estranhas sem a devida identificação.

Para o acesso dos cooperados, o setor Univocê é quem fica responsável pela liberação dos crachás, mediante apresentação das documentações pertinentes, isso ocorre no ingresso do cooperado na Unimed Chapecó e é válido por um ano. Ao vencer este prazo, os cooperados precisam retornar com as mesmas documentações ao Univocê para a renovação do acesso.

7.3 Controles para acesso físico às áreas assistenciais / ambulatoriais

Para acesso à internação deverá ocorrer controle de acesso na portaria. Os visitantes devem receber etiquetas de identificação, os terceiros (doula, fotógrafos) precisam termo para atuação no hospital (mediante cadastro, informam normas do hospital, fazem orientação, exigem documentos de identificação e certificação) e apresentar termo de consentimento do paciente. Os fotógrafos precisam apresentar autorização dos médicos para atuar. Quando este

Elaborado: Segurança da Informação Núcleo de Governança Corporativa	Revisado: Comissão de Segurança da Informação e Privacidade de Dados Pessoais	Aprovado: Comitê de GRC Unimed Chapecó
--	--	---

	<p align="center">CONTROLES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE DE DADOS PESSOAIS</p>	<p align="right">MAN.GOV.0004/01 Implantação: 06/2021 1º Revisão: 10/2021 Classificação: INTERNO</p>
--	--	--

acompanhante ou terceiro sair, deve-se recolher a etiqueta e registra a saída. Para acesso ao PA (novo hospital), os acompanhantes que tem direito, deverão ser identificados com etiqueta.

7.4 Controles para acesso físico ao Datacenter

O acesso ao Datacenter da Unimed Chapecó é restrito à equipe de Tecnologia da Informação. É de responsabilidade da equipe de TI monitorar, manter e controlar os serviços residentes no Datacenter. Somente a equipe de TI é autorizada a liberar o acesso físico às instalações do Datacenter. É vedado ao setor de Gestão de Pessoas a liberação de acesso ao Datacenter a quaisquer colaboradores, médicos ou terceiros, sem autorização expressa da Coordenação da TI ou Gerência Corporativa.

7.5 Controles para acesso físico ao arquivo morto

O acesso ao arquivo morto é restrito somente a pessoas do setor e pessoas previamente autorizadas pela coordenação do setor, devendo manter controle de acesso formalizado.

7.6 Controles para acesso físico aos estacionamentos e carga/descarga

O estacionamento é restrito aos colaboradores e médicos portadores de crachá específico, caso contrário, a liberação deverá ser controlada pela Telefonia. No acesso de carga e descarga, o controle é pelo setor de Compras quando se trata de representante ou vendedor, pelo Almoxarifado quando se refere a entrega de materiais e medicamentos, pela Nutrição quando entrega de alimentos, pela Manutenção quando entrega de materiais de manutenção e equipamentos. Além destes, a Telefonia também tem acesso para liberações.

8. DESCARTE SEGURO


O descarte seguro de informações é uma preocupação da Unimed Chapecó e as regras deverão ser observadas sempre que existir, seja um descarte de um documento físico, eletrônico ou de um equipamento.

8.1 Descarte de documentos físicos

O descarte de informações impressas deve ser adequado, sendo que não devem utilizar para rascunho impressões que contenham dados pessoais de qualquer natureza ou ainda informações sigilosas da Unimed Chapecó. Os impressos devem ser triturados antes de serem jogados no lixo.

O descarte de prontuários físicos ou quaisquer documentos que contenham dados pessoais e informações sigilosas, armazenados no arquivo morto, finalizado o prazo legal de guarda,

Elaborado: Segurança da Informação Núcleo de Governança Corporativa	Revisado: Comissão de Segurança da Informação e Privacidade de Dados Pessoais	Aprovado: Comitê de GRC Unimed Chapecó
--	--	---

	<p align="center">CONTROLES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE DE DADOS PESSOAIS</p>	<p align="right">MAN.GOV.0004/01 Implantação: 06/2021 1º Revisão: 10/2021 Classificação: INTERNO</p>
--	--	--

deverão ser descartados de forma segura, de modo que não possibilite acesso indevido aos dados.

8.2 Descarte de documentos eletrônicos

É de responsabilidade de cada usuário/setor eliminar os documentos e informações que estão em desuso, armazenados no diretório de rede de acesso interno público (fileserver\gerais). Como forma de monitoramento, periodicamente o NGC poderá realizar auditorias para verificação.

É dever também de cada usuário/setor eliminar periodicamente os arquivos armazenados no dispositivo (computador). Como forma de monitoramento, a TI poderá fazer limpeza periódica nos computadores de uso da assistência, eliminando arquivos salvos no dispositivo.

8.3 Descarte de equipamentos

Em caso de descarte de equipamentos, o setor de Tecnologia da Informação deverá efetuar a eliminação de qualquer dado que esteja armazenado nos dispositivos descartados, por meio de formatação física.


9. SEGURANÇA MÓVEL

A Unimed Chapecó mantém a separação entre as redes de internet, sendo o acesso à rede corporativa permitido somente para equipamentos da Cooperativa e a rede de visitantes fica liberada para todos os públicos. A fim de manter a segurança e proteção dos dados e informações tratadas, é proibida a utilização de equipamentos particulares em rede corporativa, seja de terceiros, dos colaboradores ou médicos, conforme descrito no parágrafo anterior.

O acesso à rede da Unimed externamente é liberado via VPN, sendo que a autorização para liberação deve ser realizada pela gerência e/ou coordenação quando se referir a colaboradores, e do diretor hospitalar em caso de médicos cooperados. Essa autorização pode ser enviada por escrito, e-mail ou mensagem específica, informando o nome da pessoa e motivo da liberação. Quando findada a finalidade do acesso remoto, o mesmo é revogado pela área de Tecnologia da Informação.

A VPN serve para determinar uma comunicação segura através da criptografia dos dados transmitidos entre a Unimed e o dispositivo móvel do colaborador. Os acessos em que o colaborador possui conectado a VPN são os mesmos enquanto dentro da empresa. Em caso de concessão de acessos via VPN, faz-se necessário assinatura de Termo específico sobre a confidencialidade requerida. A TI deverá manter registro atualizado de acessos concedidos via VPN.

Elaborado: Segurança da Informação Núcleo de Governança Corporativa	Revisado: Comissão de Segurança da Informação e Privacidade de Dados Pessoais	Aprovado: Comitê de GRC Unimed Chapecó
--	--	---

	<p align="center">CONTROLES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE DE DADOS PESSOAIS</p>	<p align="right">MAN.GOV.0004/01 Implantação: 06/2021 1º Revisão: 10/2021 Classificação: INTERNO</p>
--	--	--

10. RESPONSABILIDADE E CONSCIENTIZAÇÃO

É de responsabilidade de cada usuário, manter as medidas e controles necessários para segurança e salvaguarda das informações.

10.1 Conscientização em segurança da informação e privacidade de dados pessoais

A Unimed Chapecó promove a disseminação dos princípios e diretrizes de segurança da informação e de privacidade de dados pessoais, por meio de programas de conscientização e de capacitação promovidos pelo setor de Gestão de Pessoas (GP) e pelo Núcleo de Governança Corporativa (NGC), tais como: palestras, treinamentos e campanhas veiculadas através de e-mails, News e portal corporativo.

10.2 Uso do e-mail corporativo

O e-mail corporativo é uma ferramenta de trabalho, comunicação e apoio para os processos de negócios da cooperativa, não podendo ser utilizado para fins pessoais, sendo assim, todo o tráfego (entrada e saída), poderá ser monitorado.


A seguir, alguns tópicos que devem ser respeitados.

- É proibido o cadastramento do e-mail corporativo (@unimedchapeco.coop.br) em sites que não tenham a finalidade de trabalho.
- É proibido utilizar práticas que visem ocultar sua verdadeira identidade no envio de e-mail.
- Não é permitida a abertura de anexos de e-mail com as seguintes extensões: exe, com, bat, src, pif, dat, ini, sys, key e src, por se tratarem, na maioria dos casos, de vírus ou programas maliciosos.

10.3 Uso do WhatsApp Corporativo

A ferramenta BLIP é utilizada como WhatsApp Corporativo. Em alguns setores ainda utilizam o emulador de Android (Bluestack ou NOX), estes em processo de migração para a plataforma Blip dentro da rede corporativa, com o número corporativo hospedado na plataforma WhatsApp Business. O WhatsApp Corporativo deve ser utilizado pelos colaboradores autorizados para finalidade específica relacionada as atividades do setor, respeitando as demais políticas e diretrizes internas de proteção de dados.

Elaborado: Segurança da Informação Núcleo de Governança Corporativa	Revisado: Comissão de Segurança da Informação e Privacidade de Dados Pessoais	Aprovado: Comitê de GRC Unimed Chapecó
--	--	---

	CONTROLES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE DE DADOS PESSOAIS	MAN.GOV.0004/01 Implantação: 06/2021 1º Revisão: 10/2021 Classificação: INTERNO
--	--	--

10.4 Uso da internet

A internet é ferramenta de trabalho para desenvolvimento de atividades, processos e pesquisas, tecnologias e competências, sendo assim, todo o tráfego da internet é passível de monitoramento. A Unimed Chapecó mantém regras de utilização e bloqueio de acesso a determinados sites, caixa de e-mail, conteúdos, etc.

A Unimed Chapecó não autoriza a utilização dos meios de comunicação da cooperativa para divulgar mensagens com conteúdo ilegal, pornográfico ou qualquer sentido discriminatório, de cunho religioso, político-partidário, ideológico ou em desacordo com os seus princípios éticos.

A seguir, alguns pontos que normatizam a utilização da internet:

- Somente páginas de interesse das atividades de trabalho serão liberadas;
- Caso se faça necessário para o trabalho, o acesso a algum site não liberado deverá ser solicitado pelo colaborador, ao setor de TI, via chamado na ferramenta Intratarefas, com a marcação de seu coordenador no sistema para ciência e acompanhamento. O setor de TI deverá avaliar os riscos relacionados para liberar ou não o acesso;
- Haverá geração de relatórios dos sites acessados por usuário e se necessário, a publicação deste relatório;
- Não será permitida a utilização de serviços de streaming, tais como Rádios online, vídeos, etc.

10.5 Comunicador interno

O uso do comunicador interno deve ser restrito a comunicação da empresa, não devendo ser utilizado para fins pessoais. Todas as conversas pelo comunicador são passíveis de serem monitoradas e armazenadas em repositório que permitam auditoria, se necessário.


Abaixo, algumas normas de utilização do comunicador interno:

- É obrigatório a utilização do comunicador sempre que o colaborador estiver no seu posto de trabalho;
- A linguagem utilizada no comunicador deve ser linguagem formal.

10.6 Mesa e tela limpa

Para evitar exposição desnecessária, documentos ou arquivos contendo informações confidenciais e sigilosas não devem ser deixados sobre a mesa de trabalho ou expostos na tela do computador.

Elaborado: Segurança da Informação Núcleo de Governança Corporativa	Revisado: Comissão de Segurança da Informação e Privacidade de Dados Pessoais	Aprovado: Comitê de GRC Unimed Chapecó
--	--	---

	<p align="center">CONTROLES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE DE DADOS PESSOAIS</p>	<p align="right">MAN.GOV.0004/01 Implantação: 06/2021 1º Revisão: 10/2021 Classificação: INTERNO</p>
--	--	--

Os usuários devem tomar cuidado com a exposição das informações na tela de computadores em ambientes de circulação ou públicos. As informações impressas devem ser descartadas adequadamente, sendo que não devem utilizar para rascunho impressões que contenham dados pessoais e sensíveis (triturados antes de serem jogados no lixo).

Os colaboradores têm o dever de assegurar que as informações sensíveis, tanto em formato digital quanto físico, e ativos não devem ser deixados desprotegidos em locais de trabalho, quando não estão em uso, mesmo que seja por um curto período de tempo.

Os colaboradores devem zelar pela guarda e integridade das informações nos ambientes onde atuam, protegendo locais onde existam armazenamento de informações, sejam físicos ou eletrônicos, por meio de guarda ou proteção por senha, além da racionalização de recursos que realizam cópias de documentos.

10.7 Criptografia de Arquivos

A criptografia é um conjunto de técnicas pensadas para proteger uma informação de modo que apenas emissor e receptor consigam compreendê-la. Em geral são usados programas para realizar a codificação e para decodificação é necessário ter acesso à chave utilizada no primeiro processo, contudo, é possível utilizar a criptografia de arquivos por meio da inserção de senhas.


É imprescindível evitar exposição desnecessária de qualquer documento ou arquivos compartilhados externamente que contenham dados pessoais sensíveis e/ou informações confidenciais e sigilosas, os mesmos devem ser criptografados antes do envio para qualquer contato. A senha deve ser compartilhada apenas com o receptor, não devendo esta ser encaminhada junto com o arquivo.

As orientações para senhas seguras no processo de criptografia estão descritas neste manual, no Item 6.3, os exemplos apresentados podem ser utilizados em qualquer arquivo. Adicionalmente, foi elaborada instrução técnica de trabalho (ITT.NGC.0001-00) para auxílio no processo de criptografia com senha.

11. REVISÕES E ALTERAÇÕES

Anualmente este manual deverá ser revisado pela Comissão de Segurança da Informação e Privacidade de Dados. Eventuais alterações deste Manual poderão ser realizadas por proposta da própria Comissão revisora, do Núcleo de Governança Corporativa, da Diretoria Executiva, do Conselho de Administração ou do Comitê de GRC, cabendo a este último a sua apreciação e aprovação em reunião.

Elaborado: Segurança da Informação Núcleo de Governança Corporativa	Revisado: Comissão de Segurança da Informação e Privacidade de Dados Pessoais	Aprovado: Comitê de GRC Unimed Chapecó
--	--	---

	CONTROLES DE SEGURANÇA DA INFORMAÇÃO E DE PRIVACIDADE DE DADOS PESSOAIS	MAN.GOV.0004/01 Implantação: 06/2021 1º Revisão: 10/2021 Classificação: INTERNO
--	--	--

12. VIGÊNCIA

Este Manual foi apreciado e aprovado em reunião do Comitê de GRC realizada no dia 10/06/2021, entrando em vigor nesta mesma data e por prazo de vigência indeterminado.

Elaborado: Segurança da Informação Núcleo de Governança Corporativa	Revisado: Comissão de Segurança da Informação e Privacidade de Dados Pessoais	Aprovado: Comitê de GRC Unimed Chapecó
--	--	---