1. OBJETIVO

Esta Política visa estabelecer as diretrizes de segurança da informação, observando os princípios da confidencialidade, integridade e disponibilidade das informações da Unimed Erechim.

2. ABRANGÊNCIA

Cooperados, colaboradores, prestadores de serviços, fornecedores e/ou quaisquer outros que se relacionam com a Unimed Erechim e que, no âmbito dessa relação, possam vir a ter acesso a informações, equipamentos, arquivos, sistemas, ou outros ativos de propriedade da Unimed Erechim.

3. GLOSSÁRIO

- **AD (Active Directory)** – Software da Microsoft projetado para ambientes Windows que utiliza o protocolo LDAP. É responsável pelo armazenamento de informações sobre os objetos de uma rede de computadores;
- **Appliance** - Hardware dedicado com software específico para executar ações exclusivas e específicas em caráter autônomo com alta capacidade;
- **Backup** - Cópia de dados, configurações de servidores, máquina virtuais e informações dos ambientes de tecnologia;
- **Banco de Dados** - Tecnologia focada no armazenamento e gerenciamento de dados geralmente associado ao uso de um ERP;
- **BI** - Business Intelligence (Inteligência de Negócios), é um conjunto de tecnologias, processos e ferramentas que auxiliam as organizações a coletar, analisar e transformar dados brutos em informações significativas para tomar decisões estratégicas e operacionais;
- **Chamado** - Manifesto de necessidade de apoio de qualquer forma feito por algum dos stakeholders;
- **Cloud ou Cloud Computing** - Disponibilidade de computação em nuvem (fora da Unimed) para armazenamento ou para processamento de informações;
- **CQVU** – Centro de Qualidade de Vida da Unimed Erechim;
- **Credencial** - No contexto deste documento termo para designar o usuário e senha utilizados para identificar algum steakholder;
- **Datacenter** - Central de processamento de dados com alta capacidade e disponibilidade. Utilizado para hospedar ambientes de tecnologia;
- **Delay** – Entende-se nos contextos aqui aplicados como sendo uma espécie de atraso em alguma etapa do processo citado/envolvido;
- **DHCP** - Numa tradução livre, protocolo de configuração dinâmica para endereços de rede – protocolo utilizado para entregar endereços IP à todas os objetos de uma rede de informação;
- **Diretório Compartilhado** - Pastas com conteúdo armazenado em alguma instância da rede;
- **ERP** - Sistema Integrado de Gestão;
- **Estações** – Computadores ou notebooks da UERE utilizados pelos stakeholders;
- **File Server** – Servidor utilizado com propósito único de armazenar e gerir documentos, arquivos e informações da instituição com política de permissões personalizável de acordo com as necessidades;
- **Firewall** - Dispositivo utilizado numa rede de computadores que tem por objetivo aplicar políticas de segurança;
- **GLPI** – Ferramenta de gestão e controle de demandas de TI institucionalizada como a centralizadora dos chamados abertos pelos stakeholders;
- **GNU** - Gestão de Negócios Unimed – software utilizado para gestão de documentos, processos, fluxos, documentação de ações estratégicas e controle de algumas ações operacionais;

- **GPO** – Diretivas de grupo com políticas de controle utilizados na rede;
- **Hardware -** Equipamento utilizado nos ambientes de tecnologia como servidores e computadores;
- **High Availability -** HA – alta disponibilidade – termo utilizado para representar um sistema resistente a falhas de software, hardware e energia, visando entregar o máximo dos serviços pelo maior tempo possível;
- **Hospedar -** Armazenar;
- **IP -** Endereço de protocolo de internet – termo utilizado para representar o identificador de cada objeto numa rede de informação;
- **LAN TO LAN -** Rede local para rede local – serviço fornecido pela operadora visando interligar duas redes de forma transparente, mantendo as mesmas premissas de eficiência e segurança aplicadas em uma rede local;
- **LGPD** – Lei Geral de Proteção de Dados Pessoais;
- **Log:**
  - **on**: entende-se por "logar em" – ação relacionada ao fato de usar uma credencial para acessar um sistema ou uma rede;
  - **in**: entende-se por "logar no", processo de autenticação relacionado ao fato de usar uma credencial para acessar um sistema;
  - **out**: entende-se como "sair de" – ação relacionada ao fato de sair com segurança, finalizando a respectiva sessão de um programa, sistema ou rede de computadores.
- **MDM -** Ferramenta para gerenciamento de dispositivos móveis;
- **Mídias Removíveis -** Dispositivo de armazenamento de conteúdo que pode ser removido da energia e manter as informações salvas possibilitando uso posterior. Alguns exemplos: pen drives, cartões de memória, CDs e DVDs;
- **Nobreak -** Fonte de energia ininterrupta com foco na sustentação das operações em caso de falha no fornecimento de energia pela concessionária;
- **OPS** – Operadora de Planos de Saúde;
- **P2P** - Peer-to-peer é uma arquitetura de redes de computadores onde cada um dos pontos da rede funciona tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central;
- **PDTI** – Plano Diretor de Tecnologia da Informação;
- **Print** - Captura eletrônica no estilo de imagem do conteúdo que está em exibição num determinado momento na tela do computador;
- **Ransomware** - É um tipo de malware que impede os usuários de acessarem seu sistema ou arquivos e exige o pagamento de resgate para recuperar o acesso;
- **Restore** – Processo de restauração de dados, configurações de servidores, máquina virtuais e informações dos ambientes de tecnologia;
- **Snapshot -** Cópia instantânea do conteúdo total de uma máquina virtual com seus dados, sistema operacional e configurações;
- **Software** – Programa de computador criado para desempenhar uma ou várias funções determinadas;
- **Stakeholders -** Termo destinado à representação de todas as partes interessadas;
- **Storage -** Unidade de armazenamento de dados com alta capacidade;
- **TI -** Tecnologia da informação;
- **TS -** Terminal de Serviço do Windows, comumente entendido como sendo uma área de trabalho remota;

INTERNO
As informações contidas neste documento são de uso interno e de propriedade da Unimed Erechim.

Classificação da Informação	☐ **PÚBLICA**	☒ **INTERNA**	☐ **RESTRITA**	☐ **CONFIDENCIAL**

- **UERE –** Unimed Erechim;
- **Usuário –** Parte interessada que utiliza qualquer recurso tecnológico da UERE;
- Virtualização – processo de conversão tecnológica com a redução de servidores físicos que busca otimizar o recurso do hardware com softwares específicos;
- **VM –** Máquina virtual, geralmente utilizada como servidor em ambientes virtualizados;
- **VOIP –** Voz sobre IP – representa a possibilidade de realizar ligações telefônicas utilizando o protocolo IP;
- **VPN** – Rede privada virtual, conhecida comumente como túnel. Estabelece uma conexão criptografada utilizando a internet entre dois ou mais pontos;
- **WAF** – Firewall de aplicações web – termo utilizado para representar um firewall de aplicações projetado para filtrar e distinguir transações legítimas de ataques em endereços e portas da publicadas;
- **Web Filter –** Filtro de conteúdo para sítios da internet.

4. DIRETRIZES

4.1. Uso das Informações

A Unimed Erechim considera todas as informações geradas como um ativo. Portanto, seu uso deve ser dimensionado objetivando estabelecer uma comunicação eficiente e esclarecedora com os diversos públicos.

Esta Política possui como base as diretrizes organizacionais (missão, visão e valores) da Unimed Erechim, alinhados à legislação vigente e melhores práticas relacionadas à segurança da informação, sempre observando os pilares:

- **Confidencialidade**: Garantia de que a informação é acessível somente a pessoas com acesso autorizado.
- **Integridade**: Salvaguarda da exatidão e completeza da informação e dos seus métodos de processamento.
- **Disponibilidade**: Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

Toda e qualquer informação produzida e ou adquirida pela Unimed Erechim é de sua exclusiva propriedade, independentemente da sua forma - eletrônica, escrita ou falada. Todos os usuários envolvidos são responsáveis pela guarda, sigilo e proteção destas informações.

A Unimed Erechim monitora todas as informações corporativas, desde o recebimento, envio, armazenamento, utilização e manuseio, sem prévia notificação aos usuários, visando a garantir e a assegurar o sigilo e a segurança das partes interessadas.

Todos os usuários que tenham acesso às informações da Unimed Erechim ou sob a guarda desta – privilegiadas, pessoais, sensíveis ou não - não poderão utilizá-las para fins pessoais ou divulgá-las a pessoas não autorizadas, sem aprovação da Diretoria Executiva e/ou Conselho de Administração.

Toda e qualquer informação que não tenha sido tornada pública, oficialmente, é considerada confidencial. É expressamente proibida, aos usuários, a divulgação, cópia e/ou reprodução de informações confidenciais sem o prévio consentimento da Unimed Erechim, tanto no âmbito interno quanto externo, mesmo que em regime de informalidade.

Não é permitido aos cooperados, colaboradores, prestadores de serviços, fornecedores, clientes e demais partes interessadas, tirar fotos, filmar, gravar, publicar ou compartilhar imagens dos

ambientes internos da Unimed Erechim sem prévio consentimento da Diretoria Executiva e/ou Conselho de Administração.

Cooperados e colaboradores, quando no exercício de suas funções nas dependências da Unimed Erechim, devem observar, além desta política, as normas e diretrizes constantes no PDTI - Plano Diretor de Tecnologia da Informação e na PL-GRC.05 - Política de Privacidade e Proteção de Dados Pessoais, disponíveis no GNU.

4.1.1. Propriedade Intelectual

Os arquivos, documentos e informações criados pelos colaboradores enquanto estiverem desempenhando as atividades laborais para as quais foram contratados, pertencem, intelectualmente, de maneira exclusiva, à Unimed Erechim e não podem ser enviados como anexos de e-mail, removidos da rede, cedidos a terceiros, utilizados para finalidades alheias à sua criação ou replicados de qualquer outra maneira sem o prévio consentimento da CEO responsável e Diretoria Executiva.

4.1.2. Geração de Relatórios e Exportação de Dados

A extração de dados através de scripts ou modelagem de relatórios nos sistemas de informação ou BI da Unimed Erechim ocorre:

- Quando um colaborador solicitar um relatório ou alterações nas lógicas de uma modelagem já existente. Neste caso, a demanda obrigatoriamente deverá estar registrada em GLPI com as devidas justificativas e seu atendimento estará condicionado diretamente, a validação da liderança imediata;
- Quando a liderança solicitar um relatório ou alterações nas lógicas já existentes. Neste caso a demanda obrigatoriamente deverá estar registrada num GLPI;
- Quando qualquer colaborador, independente do nível hierárquico, solicitar uma exportação de dados que contenha informações pessoais ou pessoais sensíveis e nunca antes tenha sido solicitada ou avaliada. Neste caso soma-se aos processos acima descritos a necessidade de validação via GLPI do DPO da Unimed Erechim e CEO responsável pelo processo solicitante.

4.2. Acordos de Confidencialidade

A disponibilização de informações confidenciais pela Unimed Erechim para execução de atividades relativas à função ou cargo deverá ser precedida da assinatura do FOR-GP.1.7M - Termo de Responsabilidade e Compromisso, no momento da admissão do colaborador e na posse dos membros eleitos do Conselho de Administração, Diretoria Executiva e Conselho Fiscal.

Todos os contratos com prestadores de serviços ou demais entidades que se relacionarem com a Unimed Erechim e que venham a ter acesso a informações privilegiadas deverão conter, obrigatoriamente, cláusulas de confidencialidade, da Lei Geral de Proteção de Dados Pessoais, de responsabilidade e consequências, caso as exigências previstas sejam violadas.

4.3. Práticas e Normas

4.3.1. Gerais e de Gestão de Pessoas

É vedado o tratamento de demandas particulares ou que violem os princípios éticos descritos no código de conduta da UERE ou nas legislações vigentes, por meio de qualquer recurso. As ferramentas de trabalho disponibilizadas pela Unimed Erechim aos seus colaboradores ou partes interessadas, devem ser utilizadas apenas para este fim.

No exercício de suas funções, conselheiros, diretoria executiva e colaboradores deverão utilizar, exclusivamente, os recursos digitais como, mas não se limitando, contas de e-mail corporativo e agendas eletrônicas fornecidos em seu ingresso na Unimed Erechim. É vedada a utilização de contas

particulares e provedores comuns como, mas não se limitando, Gmail, Outlook, Yahoo e Terra. Ao término do vínculo com a Unimed Erechim, os recursos serão bloqueados e permanecerão como parte do histórico institucional, podendo ser consultados em caso de necessidade institucional comprovada, a qualquer tempo.

No ingresso de um novo colaborador a área de Gestão de Pessoas deverá:

- Solicitar formalmente, via abertura de chamado, a criação das credencias e concessão dos acessos básicos (Computador, E-mail Corporativo, Chat interno, GLPI's, Portal RH e GNU) fornecidos ao colaborador através do FOR-TI.2.1 – Carta de Acessos para Novos Colaboradores (**a liderança do novo colaborador é responsável por solicitar acessos personalizados ao cargo exercido, tais como acessos a sistemas e unidades. Não é permitido a prática de usuários espelho na criação ou concessão de acessos. Em caso de haver alteração de função/transferência de colaborador, a antiga liderança deverá solicitar revogação dos acessos restritos ao cargo anterior, e a nova liderança deverá solicitar os novos acessos necessários**);
- Orientar a leitura desta Política de Segurança para ciência das informações aqui contidas;
- Colher assinatura no FOR-GP 1.7M - Termo de Responsabilidade e Compromisso;
- Inserir na socialização de novos colaboradores as práticas e normativas de segurança desta Política;
- No desligamento de um colaborador, deverá sinalizar via abertura de chamado à área de tecnologia o fim do vínculo deste com a Unimed Erechim. A partir do chamado, dever-se-á executar os bloqueios, inativações e cancelamentos das credencias que este colaborador possuía de acordo com o checklist de desligamento automatizado do GLPI (**em se tratando do desligamento de um colaborador da área de TI que possuía acesso ao cofre de senhas, todas as credenciais que este colaborador tinha acesso, deverão ser substituídas/atualizadas imediatamente após o desligamento do colaborador**).

4.3.2. Acesso Físico de Colaboradores e Visitantes

Todos os colaboradores devem estar devidamente identificados com a utilização de crachá corporativo, em local visível, quando estiverem dentro das dependências da Unimed Erechim e suas filiais, retirando-o apenas ao final do expediente de trabalho.

O acesso de visitantes é de responsabilidade de cada área, cabendo zelar pela aprovação, programação e comunicação à recepção geral para que esta faça a entrega de crachás de visitação aos mesmos. Quando em visitação, devem ser observadas as medidas de segurança necessárias quanto ao registro de imagens e ao acesso a informações por qualquer meio.

Em nenhuma circunstância uma pessoa poderá adentrar ou permanecer sozinha nas dependências da Unimed Erechim, em horário distinto daquele contratualmente acordado, mesmo que seja para trabalho urgente ou inadiável, independentemente do seu cargo ou função. Exceções a essa regra deverão ser aprovadas pela gerência responsável.

O acesso físico a áreas sensíveis como andar administrativo, diretoria, sala de máquinas, internações, bloco cirúrgico, farmácia hospitalar, entre outros, se dá por controle biométrico, assegurando que apenas pessoas autorizadas tenham acesso a estes ambientes. No que diz respeito ao acesso físico a sala dos servidores, este somente pode ser feito por colaboradores da área de TI (Supervisor de TI, Analistas de Infraestrutura ou de Suporte) ou com o acompanhamento destes, também mediante a autenticação digital biométrica.

4.3.3. Segurança no Ambiente de Trabalho

Não é permitida a divulgação de imagens da Unimed Erechim, de suas instalações e de seus colaboradores, bem como o compartilhamento de informações restritas, pessoais ou sensíveis em *sites*, redes sociais, aplicativos ou qualquer meio de comunicação sem aprovação das gerências da Unimed Erechim.

Os colaboradores têm o dever de assegurar que informações utilizadas na execução de suas atividades, tanto em formato físico, quando digital, não serão deixadas desprotegidas em seus postos de trabalho. Quando não utilizadas ou ao final do expediente de trabalho, as mesmas devem ser armazenadas em locais apropriados e protegidos de acessos não autorizados.

O descarte de informações restritas ou confidenciais deve ser feito obrigatoriamente mediante fragmentação do documento ou descarte acompanhado, de acordo com o MAN-GRSA.13 – PGRSS – Sede.

4.3.3.1 Mesa Limpa e Tela Limpa

A prática de mesa limpa e tela limpa reduz o risco de acessos não autorizados a informações, tanto em formato digital quanto físico. Abaixo listamos algumas práticas que devem ser adotadas:

- Não deixar documentos desprotegidos sobre a mesa ou postos de trabalho;
- Manter postos de trabalho limpos e organizados, utilizando apenas os documentos necessários às atividades em execução;
- Na área de trabalho ou unidade de armazenamento local de cada computador, não deverão existir arquivos, apenas atalhos e ou ícones padrão do sistema operacional;
- A tela do computador sempre deverá ser bloqueada na ausência do colaborador do seu posto de trabalho.

4.3.3.2 Trabalho Remoto com Computador Pessoal

O acesso originado por dispositivos não pertencentes à UERE é disponibilizado através de VPN exclusiva e restrita, limitando a conexão somente ao TS destinado para esta função, não concedendo de imediato acessos privilegiados a rede institucional. Para isso, segue-se o protocolo abaixo:

- Mediante a solicitação do RH através de um chamado, com aprovação da CEO, procede-se com a configuração de um acesso nominal para o colaborador;
- Encaminha-se para o usuário os procedimentos de instalação e configuração que devem ser realizados no computador pessoal;
- Ao final do período de home office, estes acessos são bloqueados.

4.3.3.3 Trabalho Remoto com Computador Institucional

Ao utilizar dispositivos que aplicam as políticas de segurança da instituição, o acesso segue o protocolo abaixo:

- Mediante a solicitação do RH através de um chamado, com aprovação da CEO, procede-se com a liberação de um acesso nominal de VPN ao colaborador;
- Instala-se no computador da Unimed Erechim que o colaborador estiver utilizando o software responsável por criar o túnel com a rede da Unimed;
- Após a conexão VPN, os serviços ficam disponíveis mantendo a mesma estrutura de comunicação e protocolos de segurança que praticados presencialmente na Unimed;
- Ao final do período de home office, estes acessos são bloqueados.

4.3.3.4 Trabalho Remoto com Computador Institucional

Os acessos são realizados somente ao TS destinado/necessário para atendimento da demanda contratada, utilizando VPN nominal emitida para o consultor ou analista. As credenciais são revisadas periodicamente e bloqueadas após o término dos atendimentos.

4.3.4. Estações de Trabalho

É vedada a instalação de qualquer programa pelos usuários, nas estações de trabalho da Unimed Erechim, ficando esta atividade sob responsabilidade do técnico de apoio ao usuário de informática e analistas de infraestrutura. A funcionalidade é liberada apenas com credenciais administrativas. Destaca-se que a demanda deve ser solicitada à área de TI, mediante chamado dada a natureza sensível da solicitação sendo necessário avaliar se:

- O programa não ocasionará dano à rede ou aos ativos de tecnologia em uso pela cooperativa;
- O programa trará benefícios reais ao processo que o está solicitando;
- Existe a necessidade de adquirir uma licença para o uso da referida tecnologia no ambiente coorporativo;
- O computador tem condições de executar o programa com performance adequada.

É vedado o uso de mídias removíveis nas estações de trabalho da Unimed Erechim, salvo sob necessidade comprovada após análise entre liderança imediata do processo e TI.

É praticado o bloqueio automático da tela dos computadores, após 5 (cinco) minutos de inatividade, preconizando garantir a segurança dos dados caso o usuário saia da frente da estação.

É praticado o desligamento automático dos computadores da rede, em horário agendado, visando ampliar sua vida útil e reduzir o consumo de energia. Esta prática está habilitada em processos que não tem jornada de trabalho de vinte e quatro horas.

4.3.5. Ambiente Lógico

O acesso às informações e sistemas da Unimed Erechim é concedido de acordo com as atividades atribuídas ao cargo ou função exercida. É atribuição da liderança imediata a solicitação de acessos personalizados através de GLPI, bem como a revisão periódica dos mesmos. Não é permitida a manipulação ou utilização de informações de contas de acesso das quais a pessoa não tem necessidade de uso.

Apenas a supervisão da TI e os analistas de infraestrutura da UERE detêm as permissões para gerenciamento de acessos e concessão de permissões à outras pessoas, sendo responsáveis pelo zelo, cuidado e administração destas permissões. Para controle e gerenciamento de acessos a cada diretório, a Unimed Erechim utiliza grupos de permissão específicos. A inclusão dos usuários nos grupos de segurança sempre deverá respeitar os níveis hierárquicos como exposto abaixo:

- Presidente, diretor administrativo e CEOs: possuem liberdade e autonomia para solicitar acesso e liberação de qualquer conteúdo hospedado pelo file server para consulta própria. Podem solicitar liberações de acessos à alguma pessoa específica. A necessidade deverá ser registrada com um chamado e executada;
- Supervisores/Coordenadores: podem solicitar a concessão de permissões aos arquivos que detêm, inclusive a pessoas externas ao processo que gerenciam. São responsáveis também por controlar o nível de permissão que desejam atribuir ou não aos seus colaboradores;
- Responsáveis por Processos Compartilhados: podem solicitar a concessão de permissões dos arquivos que detêm. São responsáveis também por controlar o nível de permissão que desejam atribuir ou não aos demais membros do processo correlato;

- Colaboradores ou Pessoas Chave: não podem solicitar nem conceder acessos a arquivos sem a qualificação da liderança imediata ou CEO responsável pelo processo. Em caso destas últimas atribuírem este poder temporariamente ao colaborador, deve haver um registro via e-mail estipulando o período de vigência da exceção.

A disponibilização de notebook para o colaborador como ferramenta de trabalho para uso contínuo pressupõe que o colaborador não estará utilizando seu desktop, valendo-se de uma única máquina. O uso concomitante de desktop e notebook deve ser autorizado pelo Gestor da área, mediante análise prévia pela área de TI.

A Unimed Erechim adota medidas técnicas apropriadas para prevenir que seus ativos possam ser acessados ilegalmente, modificados sem autorização, falsificados, destruídos ou sofram interferências que afetem a confidencialidade, a integridade ou a disponibilidade das informações.

A Unimed Erechim reserva a si o direito de monitorar, auditar e intervir nos acessos de dados que trafegam na Internet, de modo a salvaguardar seus interesses de acordo com o Marco Civil da Internet (Lei nº 12.965/2014), consonantes com os objetivos desta Política.

4.3.5.1 Protocolo de Comunicação Entre Filiais

Visando reduzir problemas de latência, otimização de rotinas operacionais internas como backups e elevar o nível de segurança na troca dos pacotes de dados entre as filiais da Unimed Erechim, adota-se como protocolo de comunicação o uso de links dedicados LAN to LAN.

4.3.5.2 Firewalls

No Centro de Qualidade de Vida Unimed, opera-se com dois firewalls em alta disponibilidade. Complementar a estes, utiliza-se também uma estrutura de firewall para aplicações Web, com foco no site institucional e endereços web publicados abaixo do domínio da Unimed Erechim. Nas filiais da Unimed Erechim, opera-se com um firewall dedicado para cada estabelecimento.

4.3.5.3 Gestão de acessos

As credenciais de acesso de cada usuário são pessoais e intransferíveis, sendo vedado seus empréstimos e compartilhamento, associados a qualquer tipo de acesso a informações, sistemas e equipamentos, estando sujeito às sanções previstas no Código de Conduta. Cada usuário é responsável por manter suas credenciais em sigilo.

A senha de acesso à rede compreende acesso aos sistemas vinculados ao AD, sendo: computador, e-mail corporativo, chat interno, GLPIs, GNU, Portal RH e áreas de trabalho remotas, quando necessário. Deverá ser redefinida com a frequência de 60 (sessenta) dias, não podendo ser igual as últimas duas senhas utilizadas, além de não poder conter a completude do nome ou sobrenome do usuário e deve respeitar os protocolos de complexidade abaixo:

- Ser composta por no mínimo dez dígitos;
- Atender no mínimo a **três** dos seguintes critérios:
  - Conter ao menos uma letra minúscula;
  - Conter ao menos uma letra maiúscula;
  - Conter números;
  - Conter caracteres especiais como (!@#$%¨&*).

Senhas de acesso privilegiado (administradores), devem conter no mínimo doze dígitos e atender no mínimo a **três** dos seguintes critérios:

- Conter ao menos uma letra minúscula;
- Conter ao menos uma letra maiúscula;
- Conter números;
- Conter caracteres especiais como (!@#$%¨&*).

Recomenda-se como boa prática a adoção dos padrões descritos acima também nos sistemas que não são de domínio e/ou não são administrados pela Unimed Erechim, como, mas não se limitando, a redes sociais, serviços de terceiros, entre outros.

De forma automática, as credenciais são bloqueadas após cinco tentativas de login malsucedidas, permanecendo assim por dois minutos. Após esse intervalo, são novamente permitidas, todavia continuam sujeitas à validação prévia.

As senhas de administração deverão ser trocadas em caso do desligamento de algum colaborador da área de tecnologia. Sob nenhuma circunstância, as senhas devem ser armazenadas de maneira legível ou em formato físico, visando evitar qualquer divulgação ou uso indevido das mesmas. O uso de mecanismos e softwares para o armazenamento automático de senhas de acesso a sistemas e sites na internet deverá estar enquadrado no padrão estabelecido pela área de tecnologia da Unimed Erechim.

As senhas corporativas da Unimed Erechim são armazenadas no cofre de senhas corporativo, uma solução com banco de dados criptografado. Além disso, o sistema registra logs detalhados de acesso, leitura e alteração das senhas, garantindo uma trilha de auditoria completa. Para reforçar a segurança, a autenticação de dois fatores é obrigatória. Este cofre de senhas está hospedado na nuvem, proporcionando acesso conveniente e seguro de qualquer lugar. Conta também com versão desktop e em situações de contingência, pode trabalhar offline. Possui backup recorrente e ativo, permite, para administradores, a transferência de propriedade dos registros armazenados, bem como a execução de rotinas de backup manual. Além disso, há suporte dedicado, buscando garantir o funcionamento contínuo e a integridade dos dados.

A utilização dos computadores da Unimed Erechim apenas será admitida mediante o uso de credenciais individuais, fornecidas a cada parte interessada, não sendo admitido o uso compartilhado destas, salvo quando, por questões operacionais, faz-se necessário entregar maior dinamismo e fluidez no dia a dia. Estes casos são avaliados com rigor pela área de TI e documentados a seguir.

É importante enaltecer que o uso de credencias genéricas em sistemas da informação não é aceita, tampouco praticada. Quanto as credenciais para autenticação no domínio, utilizam-se credencias compartilhadas e com acesso limitado, nas situações abaixo, permitindo apenas o desbloqueio dos computadores, acesso à internet e impressão. A saber:

SITUAÇÃO	CENÁRIO
Bloco cirúrgico - Estar Médico	Utilizados para pesquisa, impressões e acesso ao sistema de prescrições
Prescrição Médica Hospital, Consultórios Hospital e Consultórios Saúde Ocupacional	Utilizados pelo corpo clínico (médicos) para prescrição e evolução de pacientes internados
Eventos, Anfiteatro e Salas de Reuniões	Notebooks de uso comum para realização de eventos na Unimed ou fora dela, com foco na reprodução de conteúdos
Farmácias	Utilizados no atendimento para evitar necessidade de logins novos em cada troca de vendedor

Notebooks Saúde Ocupacional – Atendimento Externo	Utilizados para realização de atendimentos externos (impressões, coletas de dados, geração de documentos e atividades correlatas)
Ilha na Fisioterapia	Utilizados pelos fisioterapeutas de forma compartilhada visando otimizar o atendimento dada a quantidade de profissionais

Tabela 01 – Credenciais genéricas para ingresso no domínio

Entende-se como prática necessária a revisão periódica dos acessos de forma proativa, além do praticado no dia a dia, com o intuito de mantê-los atualizados e assegurar o controle das permissões, uma vez que colaboradores e membros do corpo diretivo são realocados de função ou, até mesmo, têm seus contratos e vínculos com a Unimed Erechim rescindidos.

Adota-se como estratégia a abertura automática e recorrente de chamados pela área de Tecnologia da Informação, solicitando o processo de revisão. Os chamados apenas poderão ser finalizados com as evidências de que o processo de revisão ocorreu realmente, documentando as alterações realizadas com, mas não se limitando, *prints* de tela, relatórios ou descrições dos ajustes realizados e dos acessos afetados, ou caso não sendo necessário qualquer ajuste, que houve a análise necessária. Os processos de revisão estipulados seguem:

PROCESSO/SISTEMA	PERIODICIDADE	VALIDAR	MECANISMOS DE SUPORTE
AD, TS e VPN	QUADRIMESTRE	Existência de usuários ativos indevidamente (possíveis demissões ou realocação de área) e herança de permissões	Relatório de colabores ativos, situação do contrato e área alocada - RH
TOTVS (TS e ERP)	SEMESTRE	Existência de usuários ativos indevidamente (possíveis demissões ou realocação de área), herança de permissões e grupos de acesso	Relatório de colabores ativos e área alocada – RH + Relatório de colaboradores ativos do serviço de 24 X 7 da Federação
VSM	TRIMESTRE	Existência de usuários ativos indevidamente (possíveis demissões ou realocação de área) e herança de permissões	Relatório de colabores ativos e área alocada - RH
Wisedoc	TRIMESTRE	Existência de usuários ativos indevidamente (possíveis demissões ou realocação de área) e herança de permissões	Relatório de colabores ativos e área alocada - RH
UniLab	TRIMESTRE	Existência de usuários ativos indevidamente (possíveis demissões ou realocação de área) e herança de permissões	Relatório de colabores ativos e área alocada - RH
SAF	TRIMESTRE	Existência de usuários ativos indevidamente (possíveis demissões ou realocação de área) e herança de permissões	Relatório de colabores ativos e área alocada - RH
Agile Work	TRIMESTRE	Existência de usuários ativos indevidamente (possíveis demissões ou realocação de área) e herança de permissões	Relatório de colabores ativos e área alocada - RH
Metadados	TRIMESTRE	Existência de usuários ativos indevidamente (possíveis demissões ou realocação de área) e herança de permissões	Relatório de colabores ativos e área alocada - RH

Autorizador	TRIMESTRE	Existência de usuários ativos indevidamente (possíveis demissões ou realocação de área) e herança de permissões	Relatório de colabores ativos e área alocada - RH
E-mail	TRIMESTRE	Existência de usuários ativos indevidamente (possíveis demissões ou realocação de área) e herança de permissões	Relatório de colabores ativos e área alocada - RH
GLPI's	TRIMESTRE	Existência de usuários ativos indevidamente (possíveis demissões ou realocação de área) e herança de permissões	Relatório de colabores ativos e área alocada - RH
Painel Administrativo	TRIMESTRE	Existência de usuários ativos indevidamente (possíveis demissões ou realocação de área) e herança de permissões	Relatório de colabores ativos e área alocada - RH
GoodData	TRIMESTRE	Existência de usuários ativos indevidamente (possíveis demissões ou realocação de área) e herança de permissões	Relatório de colabores ativos e área alocada - RH
GES	TRIMESTRE	Existência de usuários ativos indevidamente (possíveis demissões ou realocação de área) e herança de permissões	Relatório de colabores ativos e área alocada - RH
OnZap	TRIMESTRE	Existência de usuários ativos indevidamente (possíveis demissões ou realocação de área) e herança de permissões	Relatório de colabores ativos e área alocada - RH
Biometrias – Control ID	BIMESTRE	Existência de vínculo legítimo e comprovado com a Unimed	Relatórios de Cooperados e Colaboradores Ativos

Tabela 02 – Revisão periódica de acessos

4.3.6. E-mail Corporativo

As mensagens de correio eletrônico são instrumento de comunicação, interna e externa, para a realização do negócio da Unimed Erechim. Estas mensagens devem ser escritas em linguagem profissional e não devem comprometer a imagem da Unimed Erechim e/ou outras entidades, mantendo em cópia apenas pessoas necessárias.

Fica desprovida de eficácia e validade a mensagem que contiver opiniões particulares e vínculos obrigacionais, expedida por quem não detenha poderes de representação por parte da Unimed Erechim.

É vedada a utilização de figuras, desenhos, frases de efeito, citações e mensagens.

Os anexos inseridos em mensagens eletrônicas, somente devem ser enviados quando necessário, sempre verificando se o destinatário está correto.

E-mails e arquivos anexados de remetentes desconhecidos ou duvidosos devem ser removidos ou encaminhados para avaliação da área de Tecnologia da Informação.

Cada usuário deve eliminar, da sua caixa de correio eletrônico, quaisquer mensagens desnecessárias, visando a otimizar espaço no servidor, reduzindo, assim, também, o risco de vazamentos e exposições.

A Unimed Erechim reserva a si o direito de, a qualquer momento, auditar o conteúdo das caixas de e-mail e mecanismos corporativos de comunicação interna, de seus usuários.

4.3.7. Internet

A Internet é disponibilizada como ferramenta para o desenvolvimento de atividades, processos, pesquisas, tecnologias e competências relacionados ao negócio da Unimed Erechim, a qual mantém regras de utilização e bloqueio de acessos a determinados sites, conteúdo, anexos, armazenamentos e conteúdos correlatos.

Acessos inapropriados, não relacionados com o negócio da Unimed Erechim, devem ser evitados. Conteúdos inapropriados ou que infrinjam alguma legislação serão bloqueados internamente.

Para garantir a segurança do ambiente e dos ativos da Unimed Erechim, as regras abaixo devem ser observadas:

- É vedado o acesso a todo conteúdo que possa infringir qualquer princípio da Constituição vigente, como discursos de ódio; de preconceito, discriminação, violência, seja qual for a natureza; de pornografia e/ou de conteúdos similares;
- É vedado o acesso a sítios da internet com conteúdo de entretenimento na rede corporativa como Netflix, Facebook, Instagram, YouTube e similares;
- É vedado utilizar os recursos para fazer downloads (mp3, vídeos, programas diversos), distribuição de *software* ou dados não legalizados, bem como a distribuição destes.
- É vedado divulgar informações confidenciais da Unimed Erechim em grupos de discussão, listas ou bate-papo;
- É vedado efetuar *upload* para nuvens particulares ou públicas de quaisquer dados ou *softwares* de propriedade da Unimed Erechim, sem expressa autorização;
- É vedado o uso de mensageiros instantâneos não homologados e/ou não autorizados pela área de Tecnologia da Informação;
- É vedada a utilização de sistemas de bate-papo e demais aplicativos não homologados e/ou não autorizados pela área de Tecnologia da Informação;
- É vedado o acesso a *sites* de apostas e execução de jogos;
- É vedado o uso de tecnologias para *download* de conteúdo ilegal da Internet ou que utilizem tecnologia P2P, tais como uTorrent, Ares e similares;
- É vedado o uso de qualquer *software* de troca de arquivos na Internet;
- É vedada qualquer transferência de arquivos que violem as Leis de Direitos Autorais.

Caso a área de Tecnologia da Informação encontre não conformidades, poderá efetuar bloqueios de acessos que possam comprometer a segurança da rede corporativa e o bom desempenho dos trabalhos.

4.3.8. Servidor de Arquivos em Rede

Informações relacionadas aos negócios da Unimed Erechim não devem ser armazenadas em estações de trabalho e equipamentos móveis, tais como *laptops*, celulares, *tablets* e similares. Devem ser armazenadas em diretórios de rede, respeitando as diretrizes definidas no MAN-QUA-1 - Sistema 5X + Vida, para que o processo de *backup* MAN-TI.6 – Sistema de Backup, seja assegurado.

É disponibilizado à cada processo individualmente e a toda Unimed um diretório de uso compartilhado denominado “Temp” no servidor de arquivos, com limpeza automática configurada. Neste não é permitido o uso para troca de arquivos que contenham dados pessoais e/ou pessoais sensíveis neste ambiente.

4.3.9. Uso de Dispositivos Móveis

4.3.9.1 Dispositivos Corporativos

Quando se descreve “dispositivo móvel”, entende-se: tablets, celulares e smartphones.

Os dispositivos móveis disponibilizados pela Unimed Erechim se destinam exclusivamente ao uso profissional.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Unimed Erechim, comunicar imediatamente seu gestor direto, a área de TI, bem como a área Administrativa. O colaborador também deverá procurar a ajuda das autoridades policiais registrando, imediatamente, um boletim de ocorrência (BO) relativo ao evento.

O colaborador toma ciência, de que o uso indevido do Dispositivo Móvel fornecido pela Unimed Erechim, caracterizará a assunção de todos os riscos da sua má utilização, sendo este o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros.

O uso de celular e tablets deverão estar em total conformidade com as disposições estabelecidas nesta política. A Unimed Erechim, na qualidade de proprietária dos equipamentos fornecidos, reserva-se no direito de monitorar e inspecioná-los, a qualquer tempo.

É expressamente proibido o uso dos dispositivos móveis da Unimed Erechim para fins ilícitos e não condizentes com o trabalho e a missão da empresa ou ainda, que violem o código de ética e conduta, incluindo, mas não se limitando, a criação de perfil ou e-mail falso; publicação em redes sociais ou envio de e-mail para fins de difamação e ofensas; pirataria; pornografia; pedofilia; concorrência desleal; entre outros.

Os dispositivos corporativos deverão operar com sistema operacional Android, compatíveis e homologados com a versão Enterprise. Mais detalhes e especificação dos modelos aceitos, podem ser consultadas em: https://androidenterprisepartners.withgoogle.com/devices/#!?device_categories=knowledge_worker. Deverão também, obrigatoriamente, contar com a instalação do MDM e antivírus corporativos, homologados pela Unimed Erechim.

Nesta esfera, por exemplo, são aplicadas políticas para controle de instalação de aplicativos, rotinas de escaneamento recorrentes em busca de softwares maliciosos, criptografia e políticas de navegação.

4.3.9.2 Dispositivos Particulares

A Unimed Erechim não veda a utilização de dispositivos móveis particulares nas suas dependências, porém sua utilização não deverá interferir na qualidade e eficiência esperada do colaborador.

Na esfera profissional, quando utilizado, deve seguir as regras abaixo:

- É vedado realizar fotos e vídeos das dependências da empresa que identifiquem pessoas sem o respectivo consentimento destas;
- É vedado realizar fotos e vídeos das dependências da empresa que exponham situações não públicas ou criem e permitam explorar brechas de segurança;
- Na rede corporativa comum, seu uso é permitido, apenas com recursos de acesso pertencentes ao próprio colaborador – sendo vedada a cópia, transferência, upload e download de documentos institucionais privados ou que contenham dados pessoais de qualquer pessoa física;
- Não devem ser conectados à rede corporativa privada.

A Unimed Erechim não se responsabiliza pela segurança e manutenção de qualquer recurso pessoal, sendo de inteira responsabilidade do colaborador, sua guarda e manuseio.

4.3.9.3 Visitantes

São estabelecidos procedimentos de controle de acesso a visitantes que durante sua permanência na instituição necessitem conectar seus dispositivos móveis à rede. Neste caso é entregue uma rede Wi-Fi exclusiva, isolada do ambiente corporativo da Unimed Erechim logicamente, apenas com acesso à Internet. Não se admite a utilização de dispositivos terceiros na rede de dados privada.

4.4 Lei Geral de Proteção de Dados Pessoais – LGPD

Durante o curso de suas atividades, a Unimed Erechim realiza o tratamento de dados pessoais, tanto de pessoas relacionadas à sua estrutura interna, quanto de terceiros.

Para garantir a segurança dos dados pessoais tratados no exercício de suas atividades e evitar a ocorrência de acessos indevidos ou não autorizados, perda, destruição ou qualquer outra ação que comprometa a integridade, a disponibilidade ou a confidencialidade dessas informações, a Unimed Erechim manterá procedimentos e ferramentas implementadas que seguem os mais altos padrões de segurança da informação.

O Comitê de Privacidade, o Encarregado pelo Tratamento de Dados Pessoais e a área de Segurança da Informação da Unimed Erechim trabalham em conjunto para manter seguros todos os dados pessoais tratados, maximizando a prevenção a exposições, vazamentos e acessos indevidos. É obrigação de cada usuário do ambiente de TI da Unimed Erechim ou que conheça esta política, caso identifique qualquer infração ao regido pela LGPD, que notifique imediatamente o público citado acima.

Todas as partes interessadas devem atuar em conformidade com a PL-GRC.05 - Política de Privacidade e Proteção de Dados Pessoais.

4.4.1 Determinações

- É vedada a reutilização de folhas impressas como rascunho;
- Todos os documentos que contenham dados pessoais e/ou dados pessoais sensíveis, uma vez que tenham chegado ao fim da sua vida útil, devem ser fragmentados e encaminhados para descarte;
- Documentos internos impressos tais como: e-mails, contratos, negociações, demandas de clientes, autorizações, contas hospitalares, resultados de exame, entre outros que contenham dados estratégicos, sensíveis e/ou pessoais sensíveis, independentemente de seu conteúdo, devem trafegar dentro de pastas e/ou envelopes. Para fins de identificação, devem ser utilizadas as etiquetas do correio interno, atentando-se ao risco e potencial impacto que os dados impressos nestes documentos possuem;
- A manutenção, guarda e tratamento de documentos impressos, dentro de cada processo, deve ocorrer respeitando obrigatoriamente a tabela de temporalidade definida, aprovada e praticada;
- Processos que possuem arquivos dentro de seus setores, é obrigatório que estes permaneçam trancados, sem a chave na porta e com controle de rastreabilidade dos documentos aí contidos, caso estes precisem ser retirados;
- Caso os colaboradores que trabalhem no setor estejam todos ausentes, a sala deve permanecer chaveada e os computadores bloqueados e/ou desligados;
- Áreas de atendimento e/ou administrativas que tratem dados pessoais e/ou dados pessoais sensíveis, caso seja necessário que os colaboradores deixem seus postos de trabalho durante o expediente ou tratamento, todos os documentos, informações e arquivos que estiverem sobre a mesa, obrigatoriamente devem ser guardados;
- Admite-se o uso de mensageiros como WhatsApp e Telegram SOMENTE para troca de comunicados, avisos e interações sociais. É expressamente proibida a troca de mensagens contendo dados

pessoais e/ou pessoais sensíveis de todo e qualquer parte interessada que por ventura tenha autorizado o tratamento de seus dados à Unimed Erechim, seus serviços próprios e/ou filiais;

- É vedado o acesso às ferramentas institucionais como e-mail e chat fora do horário de expediente contratado ou em períodos de afastamento – neste último pratica-se o bloqueio preventivo da conta, o redirecionamento desta para outro colaborador e o bloqueio do usuário no AD, impedindo todo e qualquer acesso no período;
- É vedado o compartilhamento dos dados pessoais e pessoais sensíveis de cada parte interessada sem o consentimento prévio do titular, expressamente autorizado e documentado, quando a atividade o exigir;
- Todos contratos com terceiros, incluindo clientes, fornecedores, prestadores de serviço, assistencial ou não, devem possuir cláusulas que assegurem a confidencialidade e o uso adequado das informações de acordo com a LGPD;
- Devem ser realizadas anualmente reciclagens de conhecimento sobre o tema "Proteção de Dados, Dados Pessoais e Dados Pessoais Sensíveis", com todos os colaboradores da Unimed Erechim;
- O tratamento de dados pessoais e/ou pessoais sensíveis, realizado pela Unimed Erechim, está documentado, na Política de Privacidade e Proteção de Dados Pessoais;
- Devem ser realizadas auditorias periódicas de conformidade quanto ao tratamento de dados pessoais nos processos e adequações as determinações de seguranças expressas na Política de Privacidade e Proteção de Dados Pessoais, desta Política de Segurança da Informação e do Plano Diretor de Tecnologia da Informação.

4.4.2 Classificação da Informação

As informações da Unimed Erechim ou de terceiros, utilizadas durante as atividades da própria Unimed, devem ser classificadas de acordo com a sensibilidade que representam para o negócio. Assim, poderão receber o nível de proteção adequado, a depender da sua classificação.

As pessoas somente devem ter acesso às informações que sejam necessárias, direta ou indiretamente, ao desenvolvimento de suas atividades de trabalho e demais responsabilidades associadas dentro da organização, precedidas da assinatura do FOR-GP.1.7M – Termo de Responsabilidade e Compromisso ou de cláusulas de sigilo, confidencialidade e proteção de dados, estabelecidas em contrato.

No processo de classificação da informação, deve-se avaliar o valor da informação para a Unimed Erechim, os requisitos legais, a sensibilidade, a criticidade do tratamento da informação, a necessidade de compartilhamento e os impactos que eventual incidente pode causar para o negócio.

O processo de classificação da informação está documentado na IT-GRC.09 – Classificação da Informação.

4.5 Aquisição e Desenvolvimento de Software

O processo de aquisição e/ou desenvolvimento de novos sistemas deve considerar as melhores práticas de segurança da informação disponíveis no mercado.

A aquisição e/ou desenvolvimento de novos sistemas devem considerar a verificação de requisitos mínimos de segurança da informação, seguindo procedimentos de segurança desde a sua concepção. A definição, verificação e uso adequado destes requisitos é de responsabilidade da área de Tecnologia da Informação, em atenção do disposto no Plano Diretor de Tecnologia da Informação.

4.6 Backups

Backups são parte fundamental da estrutura de tecnologia da informação da Unimed Erechim, uma vez que asseguram a perenidade dos seus dados, da sua história e de todo conhecimento adquirido ao longo do tempo, possibilitando recuperá-los em caso de algum sinistro ou necessidade específica.

Dada a magnitude do ambiente de TI da Unimed Erechim, adota-se mais de uma estratégia de *backup* visando a entregar a melhor e mais segura experiência a todos os usuários. A fim de validar a consistência destes *backups* e sua aplicabilidade real, realizam-se testes por amostragem, periódicos (mensais) e recorrentes, de recuperação, documentados por meio do GLPI.

O processo de restauração das informações armazenadas em cópias de segurança é responsabilidade exclusiva da área de TI. Quando houver necessidade de restauração, o demandante deverá solicitar formalmente através de GLPI, justificando a demanda.

As diretrizes relativas à geração, recuperação e retenção de cópias de arquivos, sistemas e banco de dados estão descritas no MAN-TI.6 – Sistema de Backup e na IT-TI.72 – Manutenção Preventiva dos Computadores e Infraestrutura.

4.7 Uso de Antivírus (Endpoints)

A função principal de um antivírus endpoint é detectar, prevenir e remover ameaças, mantendo os dispositivos protegidos contra atividades maliciosas que possam comprometer a integridade dos dados, a privacidade do usuário e a segurança geral da rede institucional. Para isso, o software de antivírus monitora a atividade nos endpoints (estações de trabalho dos usuários ou dispositivos finais de uso), verifica arquivos e aplicativos em busca de comportamentos suspeitos e utiliza uma base de dados de definições de ameaças conhecidas para identificar e neutralizar possíveis riscos. Caso identifique a partir de sua matriz de conhecimento algum comportamento perigoso, isola o dispositivo da rede e aciona a área de TI da Unimed Erechim.

Todas as estações de trabalho e servidores possuem antivírus instalado e atualizado, com atualizações e varredura para busca de ameaças, automatizadas (realizam-se buscas programadas semanais todas as sextas-feiras para as estações de trabalho e em dias personalizados para os servidores, geralmente no domingo); contam também com proteção em tempo real e análise de comportamento histórico tanto de usuários quanto de programas. É responsabilidade da área de TI assegurar o processo de controle de malwares. É responsabilidade do colaborador comunicar a área de TI comportamentos associados a malwares e ransomware em suas estações de trabalho.

4.8 Gestão de Incidentes de Segurança e Privacidade

Incidente de segurança é um evento adverso confirmado que pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perdas ou acessos não autorizados independente do meio em que estão armazenados.

O usuário da informação deverá comunicar imediatamente à sua liderança e à área de Tecnologia da Informação qualquer incidente que possa trazer impactos na segurança dos ativos organizacionais.

A notificação pode acontecer por canais não padronizados como telefone e é impreterível o registro em GLPI, utilizando a categoria 'Incidente de S&P'.

Nesta tangente, o canal padronizado para notificações é o formulário 'Direitos e Requisições do Titular' categoria 'Notificação de não conformidade', disponível no seguinte endereço, de forma pública: https://www.unimed.coop.br/site/web/erechim/direitos-e-requisi%C3%A7%C3%B5es-do-titular.

Ao receber uma notificação de incidente de segurança, a área de TI irá atuar conforme disposto no Plano Diretor de Tecnologia da Informação.

Quando o incidente de segurança compromete a confidencialidade, integridade ou a disponibilidade de dados pessoais e/ou pode acarretar riscos ou dano relevante ao titular, o DPO da instituição deverá ser acionado para tratativas.

4.9 Gerenciamento de Riscos

Os riscos à segurança da informação são continuamente avaliados e monitorados de acordo com a PL-GRC.1 – Política de Gestão do Risco, considerando-se as ameaças que possam causar danos ao negócio. Os sistemas de proteção quanto às ameaças oriundas de ambientes externos e internos, são continuamente aprimorados.

É de responsabilidade da área de Tecnologia da Informação manter e gerenciar um programa de gestão de vulnerabilidades, de acordo com as melhores práticas de mercado alinhadas à Gestão de Risco.

4.10 Auditoria e Monitoramento

Todas as informações produzidas, acessadas, armazenadas ou distribuídas por meio dos recursos disponibilizados pela Unimed Erechim poderão ser monitoradas e auditadas sem comunicação prévia.

O processo de auditoria e monitoramento tem como objetivo averiguar o cumprimento das diretrizes corporativas, identificar conteúdos e acessos indevidos, detectar fraudes ou coletar evidências para processos judiciais ou em atendimento às auditorias internas e externas e aos órgãos reguladores e fiscalizadores.

Acessos a informações com finalidade diversa das acimas citadas serão interpretados como uso impróprio, sujeito a Gestão de Consequências.

5. PAPÉIS E RESPONSABILIDADES

5.1 Conselho de Administração e Diretoria Executiva

Cabe ao Conselho de Administração e Diretoria Executiva:

- Homologar as diretrizes desta política.
- Zelar pela aplicação efetiva das melhores práticas em Segurança da Informação.
- Cumprir as diretrizes constantes nesta Política e demais diretrizes de Segurança da Informação.

5.2 Setor de Tecnologia da Informação

Cabe à equipe de TI:

- Implementar medidas e executar trabalhos, contidos nesta política, que aumentem a disponibilidade, integridade e confidencialidade dos dados tratados por meio de sistemas computadorizados de propriedade da Unimed Erechim.
- Fiscalizar, periodicamente, o cumprimento de regras de acesso aos recursos existentes nos sistemas computadorizados.
- Fornecer suporte e assessoria, em temas de segurança da informação e seus controles associados, à Unimed Erechim, mediante necessidade.
- Apoiar a difusão da cultura de segurança da informação na Cooperativa.
- Documentar como estão estruturados os equipamentos de infraestrutura, interligações das redes locais, interligações de servidores e *softwares* básicos e de apoio.
- Conhecer os procedimentos da Política de Segurança da Informação vigente.
- Assegurar que seus colaboradores estejam informados e cientes de suas responsabilidades em relação à Política de Segurança da Informação vigente.
- Implementar os procedimentos da Política de Segurança da Informação vigente.

- Iniciar ação corretiva quando ocorrerem não conformidades ou quando sejam identificadas vulnerabilidades.
- Notificar, às áreas interessadas, das não conformidades encontradas.

5.3 Usuários da Informação

Cabe aos usuários da informação:

- Zelar por todo acesso, ao ambiente computadorizado, executado e registrado com a sua identificação de acesso.
- Respeitar e preservar o grau de confidencialidade da informação, divulgando-a, exclusivamente, para as pessoas autorizadas a terem esse conhecimento.
- Utilizar os recursos tecnológicos (equipamentos, programas e sistemas) alinhados aos interesses e às atividades da Unimed Erechim.
- Notificar, de imediato, a área de Tecnologia da Informação, da Unimed Erechim, de possíveis não conformidades de segurança identificadas.

6. DISPOSIÇÕES GERAIS

Sem prejuízo das disposições contidas nesta Política, a Unimed Erechim reserva-se ao direito de revisá-la, na periodicidade que melhor entender, sempre respeitando o prazo máximo de 1 (um) ano.

7. GESTÃO DE CONSEQUÊCIAS

O descumprimento das diretrizes desta Política será tratado em conformidade com o Código de Conduta da Unimed Erechim. Situações excepcionais serão encaminhadas para a Diretoria Executiva e/ou demais órgãos de governança.

8. REFERÊNCIAS

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 03/08/2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 03/08/2023.

FOR-GP.1.7M - Termo de Responsabilidade e Compromisso.

IT-TI.72 – Manutenção Preventiva dos Computadores e Infraestrutura.

MAN-GRC.01 - Código de Conduta Unimed Erechim.

MAN-GRSA.13 – PGRSS – Sede.

MAN-QUA-1 - Sistema 5X + Vida.

MAN-TI.6 – Sistema de Backup.

PDTI - Plano Diretor de Tecnologia da Informação.

PL-GRC.05 – Política de Privacidade e Proteção de Dados Pessoais.

PL-GRC.1 – Política de Gestão do Risco.

9. SÍNTESE DAS REVISÕES

VERSÃO	DATA	MOTIVO/MELHORIAS INCREMENTAIS	ELABORADOR	APROVADOR
00	17/11/2021	Elaboração do documento	Alex Onyszko Marieli Rech	Conselho de Administração
01	24/10/2023	Revisão geral do documento	Alessandra Sonda Alex Onyszko Marieli Rech	Conselho de Administração

INTERNO
As informações contidas neste documento são de uso interno e de propriedade da Unimed Erechim.

Classificação da Informação	☐ **PÚBLICA**	☒ **INTERNA**	☐ **RESTRITA**	☐ **CONFIDENCIAL**