A Política de Segurança da Informação (PSI) tem por objetivo orientar as ações de segurança a serem implantadas e seguidas pela Unimed Alto da Serra visando garantir os princípios de integridade, confidencialidade, disponibilidade, autenticidade e legalidade das informações.

A Política de Segurança da Informação é um regulamento formal da cooperativa acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todas as pessoas que direta ou indiretamente utilizarem estas informações, estando alinhada com os requisitos do negócio. Seu propósito é estabelecer as diretrizes a serem seguidas pela Cooperativa no que diz respeito à adoção de normas, regulamentações, procedimentos e mecanismos relacionados à segurança da informação. Adotar procedimentos e mecanismos integrados a segurança da informação de forma a servir de referência para auditorias na apuração e avaliação de responsabilidades.

RESOLUÇÕES

Esta política define as práticas de segurança e privacidade da informação da Cooperativa construída em conformidade com as resoluções da ANS (Agência Nacional de Saúde Suplementar), do CFM (Conselho Federal de Medicina) e apoiada nas normatizações abaixo descritas:

ANS – Padrão TISS e suas versões – Padrão para registro e intercâmbio de dados entre operadoras de assistência à saúde e prestadores de serviços médico-hospitalares da ANS.

Resolução Normativa n° 21 da ANS e suas correlações - Dispõe sobre a proteção das informações relativas à condição de saúde dos consumidores de planos privados de assistência à saúde.
Resolução Normativa n° 501 da ANS - Estabelece o Padrão obrigatório para Troca de Informações na Saúde Suplementar - Padrão TISS dos dados de atenção à saúde dos beneficiários de Plano Privado de Assistência à Saúde.

Lei Federal nº 9.279/1996 - Regula direitos e obrigações relativos à propriedade industrial.

Lei Federal nº 9.610/1998 - Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.

Resolução n.º 1821/2007 do CFM - Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde.

Lei nº 12.888/2010 – Lei da Igualdade.

Lei Federal n° 12.853/2013 - Altera os arts. 5º, 68, 97, 98, 99 e 100, acrescenta arts. 98-A, 98-B, 98-C, 99-A, 99-B, 100-A, 100-B e 109-A e revoga o art. 94 da Lei nº 9.610, de 19 de fevereiro de 1998, para dispor sobre a gestão coletiva de direitos autorais, e dá outras providências.

ISO/IEC 27001 - fornece as diretrizes e melhores práticas recomendadas sobre gestão de segurança da informação da organização para ser usada pelos responsáveis por iniciar, implementar ou manter e melhorar sistemas de gestão de segurança da informação.

Lei Federal n.º 13.787/2018 - Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.

Lei Geral de Proteção de Dados Pessoais (LGPD) nº 13.709/2018 – É a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.

IDENTIFICAÇÃO DA EMPRESA

1. Nome da Cooperativa: Unimed Alto da Serra – Sociedade Cooperativa de Serviço Médico Ltda.
2. CNPJ: 88.732.318/0001-08
3. Endereço: Rua XV de Novembro, n.º 556, Centro, Vacaria/RS
4. Responsáveis pelo sistema de segurança: Daniel Freitas de Andrade e Rafael Borille

ASSINATURAS DE APROVAÇÃO	Diretor Presidente Dr. George Silvestre	george.silvestre@unimed-as.com.br Assinado George A.M. Silvestre D4Sign carlos.almeida@unimed-as.com.br
	Gerência Carlos José Borges de Almeida	Assinado Carlos José Borges de Almeida D4Sign
	Analista de T.I e Coordenador do Comitê de Privacidade Rafael Borille	rafael.borille@unimed-as.com.br Assinado Rafael Borille da Fonseca D4Sign daniel.freitas@unimed-as.com.br
	Analista de T.I Daniel Freitas Andrade	Assinado D4Sign
	Unimed Alto da Serra – Sociedade Cooperativa de Serviço Médico Ltda.	

DEFINIÇÕES

ANS: Agência Nacional de Saúde Suplementar.
CFM: Conselho Federal de Medicina.
IEC: Comissão Eletrotécnica Internacional.
ISO: Organização Internacional para Padronização.
LOGIN: Credenciais de acesso a software, constituído por um usuário e uma senha, utilizadas em conjunto.
LOGOFF: Comando utilizado para dar saída de um software.
PSI: Política de Segurança da Informação.
PSI: Política de Segurança da Informação.
TISS: Troca de Informação em Saúde Suplementar.
CGP: Comitê de Gestão de Privacidade.
CREDENCIAL: O mesmo que Login, é o conjunto com o nome do usuário com sua senha.
SOFTWARE: Qualquer programa ou sistema de computador.
HARDWARE: Qualquer peça ou parte física do computador.
CHAT: Programa de troca de mensagens instantâneas entre usuários.
BACKUP: Cópia de arquivos de computador, para garantir a segurança para que estes não sejam perdidos.
RESTORE: Processo inverso ao backup, recuperação dos arquivos copiados(Backup).

SOBRE A INFORMAÇÃO

A Informação é o resultado do processamento, manipulação e organização de dados, de tal forma que represente no conhecimento do sistema que a recebe. A informação é um ativo que, como qualquer outro é importante para a organização e para os negócios dispostos por ela, tem valor, portanto necessita ser adequadamente protegida contra ameaças e riscos. A informação pode existir e ser manipulada por meio escrito, visual e verbal. A Informação deve ser utilizada em conformidade com esta Política.

SEGURANÇA DA INFORMAÇÃO

A Segurança da Informação visa proteger qualquer tipo de informação que tenha valor para a organização. As medidas de segurança da informação visam proteger a informação de diversos tipos de ameaça, para garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

A segurança da informação é aqui caracterizada pela preservação da:

Confidencialidade - a garantia de que a informação é acessível somente a pessoas com acesso autorizado;
Integridade - a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
Disponibilidade - a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.
Autenticidade – a garantia de que a informação é proveniente da fonte anunciada e que não foi alvo de mutações ao longo de um processo.
Legalidade: o uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos.

Para assegurar os itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças. Em geral, o sucesso da **Política de Segurança da Informação** adotada por uma instituição depende da combinação de diversos elementos, dentre eles: a estrutura organizacional da empresa, as normas, os procedimentos relacionados à segurança da informação e à maneira pela qual são implantados e monitorados os sistemas tecnológicos utilizados, os mecanismos de controle desenvolvidos, assim como o comportamento de todas as pessoas que direta ou indiretamente utilizarem estes mecanismos, também realizando auditorias para localizar possíveis riscos de segurança.

PROPRIEDADE DA INFORMAÇÃO

Toda e qualquer informação produzida e adquirida pela ***Unimed Alto da Serra*** é de sua exclusiva propriedade, independente da sua forma: escrita, verbal ou visual. A ***Unimed Alto da Serra*** reserva-se o direito de utilizar estas informações estabelecendo regras de manipulação das mesmas de acordo com esta política, portando com o direito de monitorar o fluxo de entrada e saída das informações transmitidas, sem prévia notificação aos seus usuários. A ***Unimed Alto da Serra*** não compactua com violações de direitos autorais conforme texto da Leis Federais n° 9.610 e 12.853.

RISCOS

Os riscos típicos em segurança da Informação que esta política procura evitar são:

1. Revelação de informações de responsabilidade da organização;
2. Vazamento de informações de responsabilidade da organização;
3. Modificações indevidas de dados e programas;
4. Perda de dados e programas;
5. Destruição ou perdas de recursos e instalações;
6. Interdições ou interrupções de serviços essenciais;
7. Roubo de propriedades.

Estes riscos ocorrem principalmente pelos motivos a seguir:

1. Negligência – atos não intencionais de colaboradores e demais pessoas que utilizem o ambiente organizacional;
2. Acidentes – ocorrências acidentais, por fatores alheios;
3. Desastres naturais – ocorrências motivadas por causas naturais;
4. Ataques furtivos – ataques inesperados praticados por qualquer pessoa em qualquer ambiente que afete a organização;
5. Ataques forçados – praticados por colaboradores ou estranhos em qualquer ambiente;

ÁREAS DE SEGURANÇA

As divisões das áreas de segurança estão assim determinadas:

Segurança física: Conjunto de medidas destinadas à proteção e integridade dos ativos da cooperativa e à continuidade do negócio, abrangendo:

Vulnerabilidades

1. Riscos naturais: Inundações, tempestades, etc.
2. Riscos acidentais: Incêndios, interrupções de abastecimentos, entradas não autorizadas, etc.
3. Riscos não acidentais: roubo, furto, incêndios, interrupções de abastecimentos, entradas não autorizadas, etc.

Áreas sensíveis

4. Instalações físicas, equipamentos de TI, patrimônio físico, recursos humanos, etc.

Segurança lógica: Conjunto de medidas destinadas à proteção de recursos tecnológicos contra utilização indevida ou desautorizada, intencional ou não, abrangendo:

Vulnerabilidades

5. Acidentes por falhas - hardware, software e procedimentos.

Áreas sensíveis

6. Sistemas operacionais, sistemas gerenciadores de banco de dados, sistemas aplicativos e ferramentas de apoio.

Segurança das comunicações: Conjunto de medidas destinadas à proteção das informações que trafegam por meios eletrônicos ou convencionais e dos recursos utilizados para esse tráfego, abrangendo:

Vulnerabilidades

7. Acessos não autorizados às redes, adulteração de dados em tráfego, utilização não autorizada de informações, extravio de formulários ou documentos classificados formais e informais e divulgação de informações confidenciais.

Áreas sensíveis

8. redes de comunicação de dados, voz e imagem, conexões com redes externas e ligações de usuários externos aos recursos de rede interna.

Plano de Contingência

Para garantir a robustez e a disponibilidade contínua dos serviços de tecnologia da Unimed Alto da Serra, está implementado em sua infraestrutura uma estratégia de Clusters em Alta Disponibilidade (HA) em nosso site principal.

Essa abordagem proativa é essencial para mitigar riscos, assegurar a continuidade operacional e manter a resiliência em face de possíveis interrupções ou falhas. Nossos Clusters em Alta Disponibilidade são projetados para proporcionar uma infraestrutura resiliente, na qual múltiplos servidores ou nós trabalham em conjunto para garantir que os serviços críticos permaneçam acessíveis, mesmo se um nó ou servidor falhe.

Em caso de falha de algum equipamento, rapidamente a equipe de T.I é capaz de redirecionar o serviço afetado para o servidor restante do cluster, restabelecendo assim os serviços. A carga dos serviços está dividida entre os membros do cluster, sendo um deles totalmente capaz de suprir a carga total da estrutura em caso de falha de um nó.

Uma vez identificada a falha e reestabelecidos os serviços, a equipe de T.I pode acionar a garantia dos equipamentos afetados, bem como solicitar apoio do seu parceiro de infraestrutura para retomar a estrutura em sua integridade.

A Unimed Alto da Serra ainda conta com um site B, com servidores em standby, que poderiam ser utilizados em caso de emergência, no caso do site A estar totalmente indisponível. O site B está localizado em um endereço diferente do A e conta com uma réplica do backup do ambiente principal, pronta para ser restaurada se necessário.

Para garantir o apoio de especialistas em infraestrutura em caso de emergências, a Unimed Alto da Serra tem firmado um contrato com uma empresas referência na área, que conta com profissionais com certificações nas mais diversas áreas e com um serviço de plantão, capaz de prestar apoio 24/7.

RESPONSABILIDADES

Encarregado de proteção de dados

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

Comitê de Gestão de Privacidade e Subcomitê

Cabe ao CGP e SCGP:

1. Validar as ações oriundas do Comitê Estadual de Gestão de Privacidade;
2. Apoio a disseminação e utilização da PSI.
3. Manter atualizada a PSI com base nas normas vigentes e melhores práticas;
4. Discutir modificações pertinentes;
5. Discutir a construção de documentação auxiliar padrão quando pertinente.

Diretoria/Superintendência/Gerência

Cabe à Diretoria, Superintendência e Gerência da Cooperativa:

1. Analisar a Política de Segurança da Informação e suas revisões;
2. Aprovar a Política de Segurança da Informação e suas revisões;
3. Tomar as decisões administrativas referentes aos casos de descumprimento da Política, de suas normas ou procedimentos;
4. Disponibilizar os recursos necessários à implantação da Política de Segurança;
5. Cumprir e fazer cumprir a Política de Segurança da Informação;
6. Mobilizar os gestores para o cumprimento da Política de Segurança.
7. **Definir** quais os colaboradores terão a permissão para portar dispositivos móveis no ambiente profissional.

Equipe de TI

A Equipe de TI terá as seguintes responsabilidades:

1. Ciência e Responsabilidade da Política de Segurança da Informação e assinatura da mesma;
2. Atualizar e divulgar esta política
3. Criar as contas dos usuários e providenciar acessos necessários
4. Apoiar na utilização de ferramentas de chat corporativas
5. Adequar os sistemas em conformidade com a Política de Segurança;
6. Avaliar tecnicamente e instruir na definição de novos softwares;
7. Monitorar os registros dos sistemas;
8. Reportar de imediato ao Coordenador, quando houver, qualquer incidente de segurança e, até mesmo, suspeitas iminentes ou então tomar as devidas precauções e medidas de segurança
9. Implementar medidas, pesquisar e executar trabalhos contidos nesse manual, que aumentem a disponibilidade, integridade e confidencialidade das informações manipuladas, através de sistemas de propriedade da cooperativa ou por ela mantidos;
10. Solicitar apoio e consultoria de segurança à área de segurança da informação quando se fizer necessário ou tomar as devidas precauções e medidas de segurança quando não houver área específica;
11. Fiscalizar periodicamente o cumprimento de regras de acesso aos recursos existentes nos sistemas;
12. Planejar, elaborar, delegar e acompanhar os diversos planos de ação, visando à aderência e difusão da PSI, suas diretrizes e os demais documentos por ela referidos para a cooperativa;
13. Verificar e validar os padrões, diretrizes e procedimentos operacionais necessários para garantir a segurança da informação em todas as áreas usuárias da informação sob a guarda ou custódia da cooperativa;
14. Executar verificação de vulnerabilidades dos sistemas e implementar as correções cabíveis;

15. Elaborar, simular e executar os planos de continuidade em conformidade com esta política;
16. Verificar vulnerabilidades dos sistemas e implementar as correções cabíveis;
17. Verificar em conjunto com cada área funcional da cooperativa os processos internos e recomendar as melhores práticas de segurança;
18. Fornecer suporte e assessoria em temas de segurança da informação e seus controles associados;
19. Documentar os procedimentos de operação para todos os sistemas conforme padrões da Cooperativa;
20. Documentar a infraestrutura da rede;
21. Revisar de forma contínua os controles de segurança estabelecidos;
22. Tratar a ocorrência de não conformidades;
23. Administrar a Rede Interna utilizando todas as ferramentas disponíveis para rastrear e resolver problemas;
24. Providenciar a segregação de ambientes distintos físicos e lógicos, impedindo acessos indevidos de pessoas não habilitadas, garantindo a integridade de instalações e equipamentos;
25. Cadastrar e desativar usuários;
26. Apoiar na resolução de problemas que causem impacto ao negócio em virtude de queda de performance e indisponibilidade dos serviços, aplicações e ativos físicos de rede;
27. Recomendar a equipe de desenvolvimento de sistemas um processo de melhores práticas e desenvolvimento seguro;
28. Estar incluída em uma ou demais etapas de projetos a equipe de segurança, quando houver para avaliação de riscos e conformidades;
29. Acompanhar as revisões e notificações de restauração dos Backups, informadas pelo próprio programa;
30. Destruir HD’s de forma segura e correta, utilizando ferramentas hábeis a destruição total das informações;
31. Verificar periodicamente se as instalações de hardware e software estão em conformidade às aquisições, podendo: ✓ Auditar os equipamentos para verificação da existência de software não homologado pela empresa, bem como aqueles de natureza ilegal; ✓ Auditar todos os equipamentos de rede para verificação de vulnerabilidades ou brechas de segurança; ✓ Observar a utilização de código de acesso, por usuário que não seja o proprietário do mesmo; ✓ Verificar se os recursos de hardware, equipamentos e periféricos, estão instalados e utilizados em conformidade com padrões da Cooperativa; ✓ Instalar e manter em condições de uso os recursos de informática disponíveis e homologados pela Cooperativa; ✓ Treinar e orientar os usuários quanto à utilização dos recursos da rede; ✓ Providenciar a instalação e garantir a manutenção da rede física; ✓ Testar e indicar ferramentas/aplicativos disponíveis no mercado; ✓ Avaliar as necessidades das áreas referentes aos recursos tecnológicos.
32. Sempre que identificada a necessidade de adquirir um novo software é realizado

uma análise do mesmo, a fim de validar se este, está em conformidade com os requisitos estabelecidos no documento “Requisitos de Segurança para aquisição de Software Proprietário”.
33. Qualquer solicitação de exceção deverá ser enviada para a equipe de TI da Unimed Alto da Serra para que seja feita uma análise de viabilidade e, caso seja necessária, para uma avaliação superior.
34.Gerenciar, manter e monitorar a infraestrutura de suporte ao funcionamento do correio eletrônico.
35. É de responsabilidade da Equipe de TI, monitorar e auditar o uso do correio eletrônico e comunicar junto aos gestores imediatos para que sejam tomadas as devidas providências em casos de não conformidade.
36. Elaborar a política de regramento conforme diretrizes da cooperativa;
37. Implementar controles conforme definições da política;
38. Monitorar e auditar a utilização dos dispositivos móveis bem como dar o devido encaminhamento em casos de não conformidade.
39. É de responsabilidade da equipe de TI providenciar o monitoramento dos acessos e dar os devidos encaminhamentos em casos de não-conformidades.
40. É de responsabilidade da equipe de TI a execução de bloqueios ou liberações de sites em acordo com a superintendência e os gestores de área.

Gestores/Coordenadores

Cabe aos gestores/coordenadores de área as seguintes responsabilidades:

1. Ciência da Política de Segurança da Informação;
2. Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;
3. Conhecer os procedimentos de segurança em vigência;
4. Informar a equipe de TI ou Segurança quando ocorrerem não conformidades ou quando sejam identificadas vulnerabilidades;
5. Tomar as devidas providências junto aos seus subordinados quando ocorrerem não conformidades;
6. Responder pelas violações registradas e participar da decisão a ser tomada, quando da ocorrência de não conformidade;
7. Solicitar para a área de segurança ou equipe de TI avaliar as necessidades de alterações na política, quando pertinentes.
8. Solicitar alteração, revogação e revisão de acesso aos seus coordenados;
9. Nas contratações de serviços de terceiros providenciar a assinatura do Termo de confidencialidade ou inclusão de termos de confidencialidade no contrato;
10. Registrar no ato do desligamento a área de TI para que a mesma efetue o redirecionamento do e-mail e ou a transferência do login.
11. Nos casos de desligamento de colaboradores deverá notificar previamente o setor de TI para que suspenda o acesso do colaborador desligado à ferramenta de correio eletrônico.

12. Cabe aos Gerentes/Gestores de área encaminhar a autorização junto a Gerência e formalizar a autorização junto ao setor de Gestão de pessoas, bem como disponibilizar o acesso as informações pertinentes e acompanhar o desenvolvimento da atividade/trabalho.
13. É de responsabilidade dos gestores de área acompanhar a utilização da internet por sua equipe.
14. Em caso de **transferência de colaboradores:**

✓ Registrar junto a Área de TI sobre ajuste de perfil de acesso. ✓ Notificar o comitê de Gestão de Privacidade e Subcomitê sobre incidentes e violações de sigilo de informações pessoais para que o mesmo tome as medidas cabíveis. ✓ Autorizar formalmente junto a equipe de TI qualquer acesso remoto disponibilizado a sua área de atuação.

Em caso de **demissão de colaboradores**:

✓ Registrar no ato do desligamento a área de TI para que a mesma efetue o bloqueio imediato o redirecionamento do e-mail e ou a transferência do login.

Em caso de **afastamento ou férias de colaboradores**:

✓ Em caso de necessidade, solicitar o bloqueio provisório dos acessos pertinentes ao colaborador, registrando junto a equipe de TI para que a mesma tome as devidas providências.

Em caso de **infração e não cumprimento da norma de segurança**:

✓ Registrar e formalizar, perante os responsáveis, as não conformidades de segurança, visando a aplicação das medidas disciplinares cabíveis descritas adiante.

Setor de Gestão de Pessoas

A Área de Gestão de Pessoas terá as seguintes responsabilidades:

1. Em caso de admissão de colaboradores:
   a. Divulgar aos novos colaboradores a existência da Política de Segurança da Informação e a maneira de acessá-la.
   b. Reforçar a importância de seguir a Política de Segurança da Informação;
   c. Informar a contratação de novos colaboradores para a área de TI e iniciar o processo de criação de login ou seguir o fluxo de criação do mesmo junto a área de TI.

2. Em caso de transferência de colaboradores:

a) Registrar junto a Área de TI sobre ajuste de perfil de acesso.
b) Em caso de demissão de colaboradores:
c) Registrar antecipadamente a área de TI para que a mesma efetue o bloqueio imediato.

3. Em caso de afastamento ou férias:
a) Recomenda-se o bloqueio provisório dos acessos pertinentes ao colaborador, registrando junto a equipe de TI para que a mesma tome as devidas providências;

4. Em caso de infração e não cumprimento da norma de segurança:
a) Registrar e formalizar, perante os responsáveis, as não conformidades de segurança, visando medidas disciplinares descritas adiante.

Colaboradores e demais usuários da informação

Cabe aos colaboradores as seguintes responsabilidades:

1. Ciência da Política de Segurança da Informação;
2. Aplicar e cumprir esta política em sua rotina;
3. Respeitar e preservar o grau de confidencialidade da informação, divulgando-a exclusivamente para as pessoas autorizadas a terem esse conhecimento;
4. Utilizar os recursos tecnológicos (equipamentos, sistemas, rede) e as informações somente para desempenho das suas atividades profissionais em conformidade com as regras definidas pela Política de Segurança;
5. Notificar à Área de TI as não conformidades de segurança;
6. Não divulgar suas credenciais de acessos;
7. Não instalar em hipótese alguma, qualquer software sem o parecer e/ou acompanhamento da Área de TI;
8. Prevenir a contaminação por vírus de computador, obedecendo aos seguintes critérios:
9. Não utilizar e/ou copiar programas piratas;
10. Não copiar e/ou acessar da Internet arquivos ou programas de sites que não justifica o uso profissional;
11. Não abrir e-mails de fontes duvidosas (ex.: correntes, spams, e-mail com anexos...) ou acessar links oriundos destes;
12. Não executar arquivos de nomes desconhecidos não relacionados ao contexto profissional.
13. Sugerir medidas que possam elevar os níveis de segurança da informação na sua área de atuação.
14. Salvar e guardar documentos físicos de acordo com as tabelas de temporalidade de cada setor, realizando sempre que possível o devido descarte;

15. Organização da estação de trabalho evitando acúmulo de documentos físicos sobre a mesa;
16. Evitar a coleta múltipla de dados, buscando sempre informações já existentes internamente;
17. Conhecer as instruções definidas neste documento, informando imediatamente a equipe de TI ou responsável pela guarda da informação sobre qualquer evento que vá contra as definições contidas neste documento;
18. Executar as definições sobre a classificação da informação contidas neste documento e por seu gerenciamento.
19. Em todas as estações de trabalho é bloqueado o acesso a mídias de armazenamento removíveis (ex.: pen drive, cd's, dvd's, hd's portáteis, cartões de memória, smartphones, tablets) para armazenar e/ou transportar informações, salvo exceções devidamente autorizadas.
20. Para liberação de acesso a mídias removíveis, deverá ser aberto um chamado, o qual deverá ser acompanhado de autorização formal do Gerente da área especificando a qual usuário o acesso será concedido.
21. Somente serão permitidos dispositivos móveis de propriedade da Unimed Alto da Serra e devidamente liberados pela área de TI
22. O gestor da área é corresponsável por ações que causam danos ao ambiente de informações da Unimed Alto da Serra ou vazamento de informações.
23. Dispositivos móveis de propriedade da Unimed Alto da Serra poderão ser auditados a qualquer momento pela equipe de TI.
24. Compreender as ameaças externas que podem afetar a segurança das informações da empresa, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos, etc.; bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação;
25. Todo tipo de acesso à informação que não for explicitamente autorizado é proibido;
26. Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais etc.);
27. Arquivos de origem desconhecida nunca devem ser abertos e/ou executados;
28. Qualquer tipo de dúvida sobre a Política de Segurança da Informação e suas Normas deve ser imediatamente esclarecido com o Gestor imediato, Coordenadora do Comitê de Privacidade ou área de TI.
29. Zelar pelo sigilo e confidencialidade das informações que lhe forem confiadas para a realização de sua operação, visando o atendimento das previsões legais.
30. Notificar o Comitê Gestão de Privacidade sobre qualquer violação de confidencialidade no trato das informações sensíveis que possa acontecer direta ou indiretamente, ou mesmo sobre violações que tenham ocorrido por outros e as quais cheguem ao seu conhecimento.
31. Notificar o gestor imediato sobre qualquer perda ou extravio de informações sensíveis.

32. É proibido utilizar conta de e-mail particular para transito de documentos, confidenciais, internas e sensíveis, mantendo seu compartilhamento exclusivamente no ambiente corporativo.
33. É de responsabilidade de todos seguir esta política;
34. Solicitar autorização formal para qualquer publicação que possa realizar o vínculo com a cooperativa;
35. Não publicar conteúdo que possa causar danos à imagem da cooperativa;
36. Notificar para a área responsável pela imagem da cooperativa qualquer não conformidade observada.
37. Utilizar de forma ética e responsável o correio eletrônico de acordo com as normas estabelecidas;
38. Notificar imediatamente seu gestor imediato e equipe de TI sobre furto ou roubo dos dispositivos móveis corporativos.
39. Cabe ao colaborador seguir esta política requerer ao gestor imediato autorização para utilizar informações da Unimed em trabalhos acadêmicos.
40. Cada colaborador é responsável pela sua conta e acessos de internet, não sendo permitido a utilização com credenciais de outro;

Cooperados

Cabe aos cooperados as seguintes responsabilidades:

1. Ciência da Política de Segurança da Informação;
2. Zelar pelo sigilo das informações que transitam em seu ambiente de trabalho;
3. Zelar por todo acesso disponibilizado para execução de sua atividade;
4. Notificar à Área de TI as não conformidades de segurança;
5. Não divulgar suas credenciais de acessos;
6. Respeitar e preservar o grau de confidencialidade da informação, divulgando-a exclusivamente para as pessoas autorizadas a terem esse conhecimento;
7. Tomar as devidas providências junto aos seus subordinados quando ocorrerem não conformidades;
8. Notificar a equipe de TI para bloqueios de credenciais de acesso, fornecidas a terceiros/secretárias, utilizados para acessos a sistemas da cooperativa em seu ambiente de trabalho, quando o acesso não se fizer mais necessário/pertinente.

Terceiros

Acessos de terceiros a estrutura através de VPN, são concedidos somente à empresas parceiras com contrato firmado com a organização. Esses acessos são registrados em chamados pela equipe de T.I, informando quem e quando acessou a

estrutura, bem como o motivo de tal acesso. É de responsabilidade de terceiros dispor de equipamentos em conformidade para operação do acesso remoto;

TRATAMENTO DA INFORMAÇÃO

Objetivo Definir níveis de proteção e determinar a necessidade de medidas especiais de tratamento da informação, estabelecendo procedimentos de identificação, tratamento, descarte, transmissão e distribuição das informações da cooperativa.

Abrangência

Aplica-se a todos os colaboradores, cooperados e terceiros que utilizam as informações da cooperativa.

Desenvolvimento do assunto

A Classificação da Informação é importante para que a organização possa determinar níveis de proteção, assegurando a circulação da sua informação perante suas partes interessadas. O tratamento das informações bem como a divulgação das mesmas estará vinculado aos critérios adequados de classificação da informação, referenciados neste documento.

Classificação da informação

As informações devem ser classificadas obedecendo os critérios abaixo:

• **Informações Confidenciais:** Estas informações são sensíveis e devem ficar restritas ao ambiente da empresa, com acesso somente por pessoas autorizadas e de acordo com a sua estrita necessidade. O acesso não autorizado a estas informações podem causar danos financeiros, perdas de mercado, danos à imagem da Unimed ou vazamento não autorizado de informações estratégicas, pessoais e pessoais sensíveis. São classificados confidenciais todo e qualquer documento com destinatário específico (pessoa, área, setor).
Informações Internas: Informações de uso interno da cooperativa, mas que não são sensíveis em caso de vazamento. Essas informações não devem sair do âmbito da organização. Se isto ocorrer, podem causar constrangimento da cooperativa e prejuízos indiretos não desejáveis. São classificados internos todo e qualquer documento que pode ser consultado dentro de nossa organização.
• **Informações Públicas:** Informações que podem ser divulgadas para o público em geral, não possuem restrições para divulgação, não ocorrendo nenhum impacto negativo, seja ele interno ou externo, financeiro ou de imagem, sobre a cooperativa.

São classificados públicos todo e qualquer documento que pode ser consultador por qualquer pessoa, incluindo o público externo.

Modelos dessa documentação estão disponíveis a todos os colaboradores da Unimed Alto da Serra, esses modelos também contemplam o controle de versionamento em seu nome e no cabeçalho.

Identificação da informação
As informações devem estar identificadas conforme sua classificação (confidenciais, internas ou públicas) estando elas em meio físico ou digital. Todo documento que contenha, ou que receberá informações pessoais, e que não possa ser anonimizado, deve ser identificado com uma tarja vermelha no cabeçalho do documento.

Reclassificação da informação

A classificação das informações deve ser reavaliada pelo seu responsável, uma vez que o mesmo identifique que o potencial de impacto da mesma foi alterado ele deverá proceder com a reclassificação. Uma vez que a informação teve seu rótulo alterado, o responsável deve comunicar a alteração aos demais interessados.

Armazenamento da informação

• **A Unimed Alto da Serra** possui um local adequado e seguro para o armazenamento das informações sensíveis, com acesso restrito aos seus responsáveis (servidor de arquivos quando se tratar de informações lógicas e os documentos físicos em ambiente controlado e monitorado).
• Não é recomendado o armazenamento de informações sensíveis em dispositivos móveis, como pendrives, discos externos, smartphones, tablets, notebooks, etc.

Manipulação da informação
É de extrema importância que não sejam deixados à vista, seja em papel ou em quaisquer dispositivos (eletrônicos ou não), nenhuma informação confidencial. Ao ausentar-se de sua estação de trabalho, a mesma deverá ser bloqueada e o monitor desligado. Os documentos físicos serão armazenados em gavetas, caixa de correspondência (com as informações viradas para baixo), caixas de arquivo e demais locais que não permitam o acesso às informações por pessoas não autorizadas.

Descarte da informação

O descarte físico das informações sensíveis de forma segura deve ser realizado inutilizando o meio físico, tornando a mesma ilegível. As informações sensíveis armazenadas em meio digital devem ser deletadas quando não são mais necessárias neste meio.

Transmissão e transporte da informação
As informações sensíveis em formato digital ou físico que serão transportadas para o ambiente externo é de responsabilidade do usuário e deve ser autorizado pelo gestor ou proprietário da informação.

ACESSOS

Objetivo
Estabelecer o controle de acesso lógico e físico de todos os utilizadores dos recursos computacionais da Unimed Alto da Serra.
Definir a responsabilidade dos mesmos quanto aos seus acessos e as obrigações da organização na proteção das credenciais dos usuários.

Abrangência

Aplica-se a todos que utilizam os recursos computacionais ou softwares da UnimedAlto da Serra, bem como os acessos físicos aos ambientes organizacionais.

Desenvolvimento do assunto

O controle de acessos é estabelecido a fim de garantir a segurança das informações da organização e proporcionar a garantia de cumprimento aos valores éticos e comportamentais dos envolvidos.

Diretrizes

Usuários e aplicações que necessitem ter acesso aos recursos da Unimed Alto da Serra deverão ser identificados e autenticados;

• A equipe de TI deve manter atualizada uma lista de todos os usuários dos recursos de software da cooperativa. No caso de terceiros, o gestor imediato da área de atuação do terceiro deverá solicitar a TI a criação das credenciais do usuário, informando o período de atuação do mesmo. No caso de colaboradores a informação para a criação, e exclusão das credenciais de acesso, deve ser fornecida pela gestão de pessoas da Unimed Alto da Serra;
• Para acesso físico às dependências da empresa por terceiros, o gestor imediato da área de atuação do terceiro deverá solicitar a criação das credenciais do usuário, informando o período de atuação do mesmo.
• Para acesso específico a informações deve existir uma solicitação e autorização formal do gestor da área a ser acessada.
• As autorizações são definidas de acordo com a necessidade de desempenho das funções e deve ser considerado o princípio dos privilégios mínimos, ou seja, o colaborador deve ter acesso apenas aos recursos ou sistemas necessários para a execução de suas tarefas profissionais;

• As credenciais de acesso do colaborador, login e senha de acesso, são individuais, secretas, intransferíveis;
• O usuário que esquecer ou bloquear a senha de acesso deve solicitar a troca através de chamado de suporte para a equipe de TI informado pelo próprio colaborador ou seu superior imediato;
• Ao se ausentar do ambiente de trabalho e deixar o computador, o colaborador deverá bloquear a sua estação para impossibilitar o acesso indevido por outro usuário;
• Deve existir um registro formal da aprovação de autorização para acesso remoto a ser realizada pelo gestor imediato da área;
• Deve ser mantido o registro dos acessos individuais realizados para internet na rede de visitantes;
• O acesso aos rack's de TI são restritos aos colaboradores da área de tecnologia, controlados por leitores de biometria facial, com registro de acesso.
• A equipe de TI deve auditar os acessos com privilégios específicos, removendo particularidades que não forem mais pertinentes.
• A equipe de TI está previamente autorizada a questionar qualquer solicitação de acesso ou acesso previamente concedido, no momento em que detectar algum risco potencial ou falha de segurança.
• Áreas que manipulam informações sensíveis na organização não devem ser expostas à visitações de estranhos ou terceiros, sem acompanhamento.
• Os logins dos usuários devem ser cadastrados pelo primeiro nome, seguido de ponto e o sobrenome.

Diretrizes para acesso remoto

• Deve ser realizado um registro formal da aprovação de autorização para acesso remoto a ser realizada pelo gestor imediato da área em acordo com a equipe de TI;
• Todo acesso remoto deverá ser realizado por VPN;
A equipe de TI está previamente autorizada a revogar qualquer concessão de acesso remoto, no momento em que detectar algum risco potencial, falha de segurança ou por decisão estratégica.
• O acesso remoto deverá ser nominal quando não acompanhado e a equipe de TI deve prover soluções que possibilitem o rastreamento de atividades executadas;
• Recomenda-se que o usuário com autorização de acesso remoto utilize redes externas seguras, para acessar o ambiente tecnológico da cooperativa evitando por exemplo, redes wi-fi públicas.
• Os usuários autorizados ao acesso remoto, devem proteger suas credenciais e em nenhum momento devem disponibilizar seu login e senha de rede, e-mail, VPN, ou qualquer informação de acesso, para outra pessoa;
• Os usuários com acesso remoto devem cuidar para que informações sigilosas não sejam capturadas por terceiros que estejam próximos ao equipamento;

SERVIÇOS DE MENSAGENS INSTANTÂNEAS

Objetivo

Definir as normativas para a utilização de aplicações do tipo “Mensagens Instantâneas” dentro da organização ou com equipamentos pertencentes à Unimed Alto da Serra. Cabe a Unimed Alto da Serra avaliar a necessidade de utilização de tais ferramentas e em caso de adoção deve existir uma solicitação formal à equipe de TI com prévia autorização da gerência para a concessão do acesso.

Abrangência

Aplica-se a todos os colaboradores que possuam acesso às ferramentas de “mensagens instantâneas”.

Desenvolvimento

A mensagem instantânea é uma aplicação que permite o envio e o recebimento de mensagens de texto e arquivos em tempo real. Através destes programas o usuário é informado quando algum de seus contatos, cadastrados em sua lista, está online. A partir daí eles podem manter conversações através de mensagens de texto as quais são recebidas pelo destinatário instantaneamente.

Diretrizes

• Os programas de mensagens instantâneas homologados pela empresa são Microsoft Teams, e Whatsapp Corporativo. • As ferramentas Skype, WhatsApp (pessoal) e Telegram não devem ser utilizadas para transmissão de arquivos e informações sensíveis. Não é permitido o uso de qualquer outra ferramenta de comunicação instantânea sem a validação da equipe de TI;

• Para a utilização de ferramentas de mensageria instantânea deve existir autorização formal com os gestores imediatos;
• A Unimed disponibiliza acesso ao Microsoft Teams a todos os usuários que possuem licença Office 365
• O acesso ao WhatsApp web na rede corporativa deverá ocorrer somente para fins corporativos para usuários que utilizem telefone corporativo ou conforme o interesse da empresa. O usuário que fizer uso desta ferramenta na rede corporativa para fins pessoais fica ciente que pode ser auditado a qualquer momento sem aviso prévio e pode ter seu acesso revogado por má utilização;
• Não é permitido usar linguagem ofensiva ou grosseira nem publicar material calunioso, abusivo ou que invada a privacidade de qualquer indivíduo;
• É terminantemente proibida a discriminação, seja ela de gênero, social ou racial.
• Não enviar material não condizente com as atividades da Instituição, tais como conteúdo pornográfico, antiético ou discriminatório;

• Não efetuar o envio ou cópia de qualquer material protegido por direitos autorais, patentes ou outras propriedades intelectuais ou leis e regulamentações similares, como digitalização de fotos de revistas, livros, ou outras fontes, softwares e músicas protegidas por direitos autorais, utilizando os recursos disponibilizados pela Instituição;
• Não divulgar informações que possam causar danos físicos, materiais ou morais a terceiros.

CORREIO ELETRÔNICO

Objetivo

Definir diretrizes relativas ao acesso e uso do correio eletrônico corporativo.

Abrangência
Aplica-se a todos os colaboradores que utilizam o recurso de correio eletrônico corporativo.
Desenvolvimento
O envio e recebimento de mensagens de e-mail são realizados através de um sistema de correio eletrônico. Um sistema de correio eletrônico é composto de programas de computador que suportam a funcionalidade de cliente de e-mail de um ou mais servidores de e-mail que, através de um endereço de correio eletrônico, conseguem transferir uma mensagem de um usuário para outro. O serviço de correio eletrônico permite catalogar contatos e transferir arquivos. O uso deste serviço não se restringe a utilização interna, também é um veículo para a comunicação externa com outras empresas, clientes, fornecedores e etc.

Diretrizes

• As contas de correio eletrônico deverão seguir um padrão definido pela cooperativa e serão criadas pela equipe de TI;

• Ao observar os aspectos éticos e de responsabilidade no manuseio do correio eletrônico, é proibido enviar: ✓ E-mails de piadas; ✓ Arquivos em anexo de imagens, filmes, apresentações ou qualquer outra mensagem sem conteúdo profissional (salvo áreas em que sua função exija); ✓ Correntes de qualquer tipo; ✓ Qualquer mensagem sem fim profissional; ✓ Mensagens com conteúdo ofensivo a qualquer pessoa;
• É proibido acessar o correio eletrônico de outro usuário sem sua permissão, salvo nos casos em que a gestão imediata tiver esta necessidade mediante registro formal junto a Equipe de TI;

• A utilização da ferramenta pode ser monitorada a qualquer momento pela **Unimed Alto da Serra** sem aviso prévio. A solicitação de acesso ao monitoramento somente poderá ser realizada por colaborador em nível hierárquico superior;
• Não é permitida a alteração das informações na assinatura padrão definida pela organização;
• É proibido enviar mensagens contendo informações sobre os negócios da organização a pessoas não autorizadas;
• O e-mail corporativo pode ser acessado somente dentro do horário de expediente do colaborador. Somente pessoas devidamente autorizadas pela gerência da **Unimed Alto da Serra** podem acessar essa ferramenta fora de seu horário de expediente, porém a **Unimed Alto da Serra** não incentiva essa prática;
• Nos casos de afastamentos por atestado, licença saúde, licença maternidade e cursos o gestor imediato ou colaborador devem tomar as devidas tratativas quanto ao redirecionamento de mensagens ou notificação de mensagem automática.
• Nos casos de férias ou ausências programadas o próprio colaborador deve configurar o encaminhamento de mensagens, bloqueio ou resposta automática ou solicitar auxílio para a Equipe de TI mediante registro formal através do Sistema de Chamados.
• É proibido acesso ao e-mail para colaboradores que estiverem em férias ou afastamentos por motivo de saúde;
• Não efetuar o envio ou cópia de qualquer material protegido por direitos autorais, patentes ou outras propriedades intelectuais ou leis e regulamentações similares, como digitalização de fotos de revistas, livros, ou outras fontes, softwares e músicas protegidas por direitos autorais, utilizando os recursos disponibilizados pela Instituição;
• Nos casos de desligamento de colaboradores em que os mesmos utilizem uma conta de correio eletrônico com credenciais que fazem referência a sua pessoa, a conta deve permanecer ativa por um período máximo de 30 dias, a disposição do gestor da área, sendo alteradas as credenciais de acesso no ato do desligamento, salvo em casos de interesse da cooperativa mediante solicitação formal da gerência. Após este período a conta é excluída definitivamente.
• As contas de e-mail são criadas seguindo o padrão adotado pela cooperativa (nome.sobrenome@unimed-as.com.br) de acordo com as boas práticas em segurança da informação facilitando auditorias.
• Orienta-se aos colaboradores não enviarem mensagens de e-mail para mais de 20 destinatários simultâneos na mesma mensagem, pois tal atividade pode ser classificada como Spam pelos órgãos mantenedores de listas negras, fazendo com que o domínio da cooperativa seja cadastrado nessas listas.
• Quando uma mensagem for enviada para diversos usuários simultâneos, os destinatários devem ser ocultados na mensagem.
• Não é permitida utilização de e-mails para cadastro com fins particulares (ex. lojas, sites de relacionamento, sites impróprios, compras por internet, participação de correntes etc.).

Toda e qualquer conta de e-mail relacionada ao domínio da **Unimed Alto da Serra**, adicionada a grupos de envio e recebimentos de mensagens em massa devem ser analisadas junto a área TI para evitar congestionamentos e superlotação.
• Qualquer identificação de contas enviando spams são automaticamente bloqueadas pelo servidor de e-mail. Em situações de falha de envio de mensagem, o e-mail do erro deve ser enviado a área de TI para sua análise e correção.

DISPOSITIVOS MÓVEIS
Objetivo

Definir diretrizes relativas à utilização de dispositivos móveis pessoais e fornecidos pela Unimed Alto da Serra no ambiente profissional.

Abrangência
Aplica-se a todos que utilizam dispositivos móveis no ambiente profissional.

Desenvolvimento do assunto

Devido ao acesso pessoal a diversas tecnologias de ponta, muitos profissionais querem utilizar equipamentos móveis no ambiente profissional. Esta política estabelece os critérios de manuseio, manutenção e responsabilidade sobre o uso destes dispositivos. Entende-se por dispositivos móveis os seguintes equipamentos: notebooks, tablets, celulares e afins.

REDES

A Unimed Alto da Serra tem segmentado redes destinadas a dmz web, gerenciamento e redes internas para diferentes estabelecimentos e escritórios regionais.
A organização conta com Redes Wifi destinadas a colaboradores, médicos e visitantes. Essas totalmente isoladas da estrutura da organização. A rede para visitantes é inclusive um contrato a parte e tem estrutura própria.

Diretrizes

• É permitido que os colaboradores portem seus dispositivos móveis corporativos e pessoais no ambiente profissional;
• Não é permitido que os dispositivos móveis pessoais portados no ambiente profissional acessem a rede corporativa

• A equipe de TI não fornece suporte aos dispositivos móveis pessoais portados no ambiente profissional;
• A equipe de TI deve homologar, controlar e suportar os dispositivos móveis corporativos permitidos.

• Não é permitido usar dispositivos móveis corporativos e pessoais para fomentar linguagem ofensiva ou grosseira nem publicar material calunioso, abusivo ou que invada a privacidade de qualquer indivíduo no ambiente profissional;
• Não é permitido fazer uso de dispositivos móveis corporativos e pessoais para promover a discriminação, seja ela de gênero, social ou racial no ambiente profissional, amparada pela Lei nº 12.888/2010 – Lei da Igualdade;
• Não é permitido utilizar dispositivos móveis corporativos e pessoais para enviar material não condizente com as atividades da Instituição, tais como conteúdo pornográfico, antiético ou discriminatório no ambiente profissional;
• Não é permitido utilizar os dispositivos móveis corporativos para armazenar, distribuir ou executar qualquer tipo de aplicativo, informação ou arquivo não autorizado;
• Não é permitido a utilização de dispositivos móveis para efetuar o envio ou cópia de qualquer material protegido por direitos autorais, patentes ou outras propriedades intelectuais ou leis e regulamentações similares, como digitalização de fotos de revistas, livros, ou outras fontes, softwares e músicas protegidas por direitos autorais, utilizando os recursos disponibilizados pela Instituição no ambiente profissional;
• Não é permitido utilizar dispositivos móveis no ambiente profissional para divulgar informações que possam causar danos físicos, materiais ou morais a terceiros ou a própria cooperativa.

INTERNET

Objetivo
Definir diretrizes relativas ao acesso e uso da internet em ambiente corporativo.

Abrangência

Aplica-se a todos que utilizam o recurso de internet no ambiente corporativo.
Desenvolvimento do assunto
A internet é um dos meios de comunicação mais utilizados nos tempos de hoje, para tanto essa ferramenta precisa ser utilizada de forma segura e ética, pois permite acesso e troca de diversos tipos de informações.

Diretrizes

• O acesso à internet é monitorado para todos os colaboradores e de maneira individual;
• O acesso à internet é disponibilizado ao interesse da cooperativa;
• Não é permitido a utilização de internet para acesso a sites de conteúdo impróprio, jogos, programas de compartilhamento de arquivos (ex.: eMule, Ares, torrent, P2P, etc.…), visualização de vídeos e músicas (salvo para fins profissionais), material pornográfico e sites de relacionamento;

• Em caso de identificação de utilização indevida da internet o acesso poderá ser bloqueado sem aviso prévio;
• Existe uma lista padrão de acesso pré-aprovada pela superintendência corporativa para colaboradores, a qual categoriza os sites conforme seu conteúdo e libera as categorias pertinentes a todos os colaboradores;
• Existe uma lista padrão de acesso pré-aprovada pela superintendência corporativa para gestores, a qual categoriza os sites conforme seu conteúdo e libera as categorias pertinentes a todos os gestores;
• Existem listas de acesso a sites e categorias específicos por setor, a qual é alimentada com novos acessos mediante solicitação formal do gestor e liberadas caso a equipe de TI não identifique problemas no acesso;
• Algumas categorias são controladas em níveis de aplicação, sendo permitidas apenas os acessos pertinentes das referidas categorias (redes sociais e mensageria instantânea);
• Sites não categorizados pelo fornecedor de tecnologia são bloqueados por padrão;
• Não é permitido divulgar ou compartilhar informações da empresa em grupos de discussões, respeitando as regras de classificação da Informação, apresentadas nesta política;
• É proibido transmissão, propagação ou divulgação de ameaças, difamação, calúnia, pornografia, material preconceituoso ou qualquer outro tipo de informação ou arquivo que viole as leis vigentes, bem como o Código de Conduta Unimed.
• Não é permitido aos colaboradores ou terceiros a criação de grupos, comunidades, páginas, blogs ou similares, utilizando o nome ou marca da **Unimed Alto da Serra** sem a devida autorização formal da superintendência corporativa.
• É proibido atacar, burlar ou pesquisar em áreas não autorizadas (Hacking).

MÍDIAS E REDES SOCIAIS

Objetivo

Orientar e estabelecer normas e padrões em relação ao acesso às Redes Sociais e a circulação de informações relacionadas a Cooperativa dentro destas ferramentas.

Abrangência

Aplica-se a todos colaboradores, cooperados e terceiros que tem vínculo com a Cooperativa e que utilizem de forma pessoal Mídias e/ou Redes Sociais.

Diretrizes

É facultativa aos colaboradores a utilização de Mídias e Redes Sociais, de forma pessoal, fora do local de trabalho e horário de expediente; A Unimed Alto da Serra, como detentora de sua marca, não autoriza a divulgação da mesma, de sua imagem ou de informações de sua propriedade nas mídias e redes sociais salvo em caso de

consentimento; A Unimed Alto da Serra não incentiva a publicação de imagens do ambiente interno ou externo, de atividades que ocorram no trabalho, como reuniões, treinamentos, ou outras situações que demonstrem o vínculo com a cooperativa, salvo as publicações que sejam realizadas pela própria cooperativa em seu perfil oficial na rede ou devidamente autorizadas pela mesma; A Unimed Alto da Serra permite a utilização das mídias sociais no horário de expediente, somente para a execução de atividades profissionais, das rotinas de trabalho que necessitem destes acessos, sua utilização deve seguir as normas previstas no Código de Conduta da cooperativa.

SENHAS

Objetivo

Estabelecer normas e padrões para o uso de senha e procedimentos adequados para correta utilização das contas de acessos autorizados à informação, visando apoiar e reforçar a política de segurança da informação da Unimed seguindo normativas e orientações dos órgãos regulamentadores.

Abrangência
Aplica-se a todos os colaboradores, cooperados e terceiros que utilizarem rede ou sistemas na Unimed.

Desenvolvimento do assunto
A senha serve para autenticar o seu login, ou seja, é usada no processo de verificação da sua identidade, assegurando que você é realmente quem diz ser e que possui o direito de acessar o recurso em questão. As senhas são as credencias de segurança dos usuários, para tanto, devem seguir as diretrizes abaixo. A senha deverá ser individual e intransferível devendo ser escolhida pelo próprio usuário. Não deve ser possibilitado acesso aos sistemas com login compartilhado (único login para várias pessoas).

Diretrizes
As senhas dos usuários devem conter no mínimo 10 caracteres, sendo obrigatório a utilização de no mínimo um caractere numérico, um símbolo, e variando pelo menos um caractere maiúsculo e minúsculo;
• Todos os sistemas devem permitir que o usuário troque sua senha a qualquer momento;
• O login do usuário será bloqueado após a sexta tentativa inválida e sequencial com a senha errada;
• O procedimento de entrega dos logins e senhas de acessos iniciais para o colaborador é realizado pela equipe de Gestão de Pessoas a qual registra chamado ao setor T.I

• O tempo máximo de vida da senha é de 45 dias, devendo ser redefinido ao término desse prazo;
• O usuário deverá bloquear sua estação de trabalho quando afastar-se da mesma. No caso de esquecimento deste bloqueio, o sistema bloqueará a estação de trabalho automaticamente após 05 minutos de inatividade;
• Na troca de senha, é vedada a reutilização da última senha.
• A equipe de TI somente poderá redefinir a senha por solicitação formal pelo sistema de chamados.
• Na composição de senhas: o Não utilizar informações pessoais fáceis de serem obtidas, como o número de telefone, nome da rua, nome do bairro, cidade, data de nascimento, nome, sobrenome, nome de pessoas próximas (cônjuge ou filhos); o Não utilizar palavras que estão no dicionário (nacionais ou estrangeiras); o Não utilizar senhas pessoais para os logins profissionais; o Não anotar a senha em papel ou em outros meios de registro de fácil acesso de outras pessoas; o Evitar senhas com sequências lógicas (ex.: a123567, abcdfgh1, …); o A senha do colaborador deve ser trocada no primeiro acesso à rede corporativa;
• Evitar senhas repetitivas (ex.: aaaa1111, ababab11, …).

INFORMAÇÃO EM TRABALHOS ACADÊMICOS

Objetivo

Orientar sobre direitos e deveres relacionados à utilização de informações da cooperativa em trabalhos acadêmicos.

Abrangência
Aplica-se a todas as pessoas devidamente autorizadas e matriculadas em cursos de segundo grau, técnicos, graduação, pós-graduação, mestrado e doutorado que desejam utilizar as informações da cooperativa para fins acadêmicos.

Desenvolvimento do assunto

A informação é um dos ativos mais importantes da organização e por esse motivo ela deve ser protegida e gerenciada. Ela está em todos os níveis hierárquicos da empresa, permeando todas as áreas e é classificada de acordo com os critérios estabelecidos na seção de classificação da informação desta política. Sua utilização deve ser acompanhada pela organização para que a mesma se mantenha competitiva no mercado. Em virtude desses fatores o uso de informações pertencentes a cooperativa deve ser monitorada nos trabalhos acadêmicos/científicos buscando a confidencialidade.

Diretrizes

• É permitida a utilização de informações da **Unimed Alto da Serra** em trabalhos acadêmicos/científicos mediante autorização prévia da Gerência;

• Deverá ser apresentado e entregue em meio físico e eletrônico projeto com indicação do tema, objetivo geral, objetivos específicos, justificativa e cronograma que contenha todas as etapas de realização da pesquisa.
• Os encaminhamentos para solicitação de estágios curriculares e pesquisas deverão ser direcionados pelo gestor da área;
• Deverá existir uma solicitação formal expressa do interessado no acesso às informações a qual deve ser encaminhada ao setor responsável. Em caso de aprovação deve ser entregue a autorização devidamente assinada ao solicitante;
• Somente serão autorizadas as pesquisas, trabalhos e/ou estágios que tenham o tema relevante para a cooperativa, e que esteja alinhado aos referenciais e objetivos estratégicos da mesma;
• As informações pertinentes serão disponibilizadas pelo setor responsável;
• No momento da autorização por parte da cooperativa, o solicitante deverá assinar o Termo de ciência e responsabilidade para trabalhos acadêmicos, que diz respeito ao uso das informações liberadas pela cooperativa, comprometendo-se a utilizar as mesmas apenas para uso e desenvolvimento do trabalho e para nenhum outro fim.
• Uma vez autorizado, o aluno compromete-se ao final das atividades a apresentar uma cópia do trabalho, em formato digital.

BACKUP

Objetivo

Definir as diretrizes relativas à geração, recuperação e retenção de cópias de informações importantes para a cooperativa de forma a garantir a segurança física e lógica das mesmas.

Abrangência

Aplica-se a todos os colaboradores, cooperados e terceiros que manipulam informações importantes para a organização.

Desenvolvimento do assunto

O backup é garantia de que as informações importantes serão preservadas mediante cópia de segurança das mesmas. Estas cópias deverão ser realizadas sistematicamente por meio de ferramentas adequadas e que garantam a preservação e recuperação das informações quando necessário.

O restore é processo inverso onde as informações mantidas sob backup são disponibilizadas novamente para a manipulação.

Diretrizes

O backup da Unimed Alto da Serra está estruturado em dois ambientes, um ambiente principal e um segundo ambiente de replicação. Esses ambientes estão localizados fisicamente em locais distintos.
A organização conta com uma ferramenta líder de mercado para gerenciar o seu BKP, nela está estrutura a política de periodicidade e de retenção, sendo ela realizada a cada quatro horas com retenção de 2 dias, diária com retenção de 7 dias, semanal com retenção de 4 semanas e mensal com retenção de 6 meses.
Essa estrutura de backup é administrada pela própria equipe de T.I a qual também é capaz de realizar alguma restauração se necessário. A própria ferramenta de backup é capaz de identificar falhas na realização e na integridade dos backups que são realizados. De forma bimestral é realizado uma restauração de teste pela equipe de T.I, a fim de validar a integridade e o ambiente de recuperação, os resultados desses testes são registrados na ferramenta de chamados do setor.

PRÁTICAS DE SEGURANÇA ADOTADAS PELA UNIMED ALTO DA SERRA

Objetivo

Apresentar as práticas de segurança adotadas pela Unimed Alto da Serra

Abrangência

Aplica-se a todos os colaboradores, jovens aprendizes, cooperados e terceiros que utilizarem rede ou sistemas na Unimed.

Práticas adotadas

Segurança lógica

Segregação de ambientes

Existem ambientes do sistema ERP da operadora destinados a realização de testes, estes ambientes herdam as permissões do ambiente de produção, logo os colaboradores têm o mesmo nível de acesso que possuem em produção nos ambientes destinado a homologação e testes.

Banco de dados

• Controle de Acesso e Autenticação: O acesso aos dados contidos no banco de dados é protegido por autenticação de usuário e senha, ficando o controle desses sob a responsabilidade da Área de TI;

Segmentação de ambientes

• Todas as redes estão protegidas por firewall, o qual controla a comunicação da rede com o meio externo em ambos os sentidos;
• Todas as portas lógicas de entrada estão bloqueadas por padrão, exceto aquelas devidamente autorizadas para o funcionamento de aplicações de uso necessário.
• As redes dos diferentes ambientes estão segmentadas em vlan's, impossibilitando dessa forma acessos não autorizados entre as redes.

Serviço de segurança – Antivírus

A Unimed Alto da Serra faz uso de uma solução de endpoint, ferramenta líder no quadrante magico do Gartner, integrado ao seu firewall. Esse endpoint integrado ao firewall é capaz de levar as políticas de acesso e periféricos nos dispositivos, mesmo eles estando conectados a outras redes. O endpoint conta com recursos de varredura em tempo real, além de diversas outras tecnologias de proteção. Esse antivírus conta com recursos como:

- Endpoint Detection and Response (EDR): integra a poderosa detecção e resposta de endpoints (EDR) à melhor proteção de endpoints do setor. Desenvolvido para operações de segurança de TI e caça a ameaças, ele detecta e investiga atividades suspeitas com análise direcionada por IA.
- Exploit Prevention: Interrompe as técnicas usadas em ataques sem arquivo, sem malware e baseados em exploit.
- Anti-ransomware: Oferece tecnologias avançadas de proteção que desestabilizam toda a cadeia de ataque, incluindo Deep Learning, que prevê e previne ataques, e o CryptoGuard, que reverte a criptografia não autorizada de arquivos em segundos.

Segurança física do ambiente

Perímetro da segurança física

• Os servidores estão armazenados em local físico com acesso controlado, restrito somente a pessoas da área de TI, devidamente autorizadas;
• Esta Cooperativa adota barreiras físicas de modo a isolar o ambiente de processamento da informação dos demais departamentos.

• As portas permanecem fechadas com controle de acesso;
• O controle de acesso às salas técnicas é restrito a equipe de T.I por meio de biometria facial;

• A entrada e saída de equipamentos nessas áreas é controlada e fiscalizada pela Área de TI, a fim de evitar o roubo/perda ou danos nos ativos que tratam da informação.

Controles de entrada e saída de pessoas

O acesso de pessoas de outras áreas aos ambientes restritos de TI, como visitantes e pessoal de limpeza, deverá ocorrer sempre com o acompanhamento ou presença de um funcionário da área de TI.

Criação de novas áreas

Quando da criação de nova área na Cooperativa todos os itens de segurança física serão avaliados com relação à área criada.

Proteção do prédio, dos equipamentos e da infraestrutura

• Os equipamentos próprios, considerados de difícil reposição em função do custo financeiro, estão segurados contra incêndio e roubo;
• As instalações prediais estão seguradas contra incêndio;
• A manutenção preventiva dos equipamentos é feita conforme as especificações do fabricante; • Todas as áreas da Cooperativa, inclusive as salas onde se encontram os servidores, possuem equipamentos de combate a incêndio;
• A sala onde se encontram os servidores está devidamente climatizada conforme especificações do fabricante;
• Existe um sistema de nobreak e gerador, que alimentam os equipamentos e os locais críticos (datacenter, sala de servidores e ativos de rede).

Penalidades

As penalidades aos colaboradores pelo não cumprimento desta política estão descritas a seguir:

Em caso de descumprimento o colaborador poderá receber as seguintes medidas:

Advertência verbal: o Colaborador é advertido verbalmente por seu Gestor imediato de forma respeitosa e privada, sem exposição nem constrangimento. É preciso deixar claro que se trata de uma advertência verbal e os motivos que levaram a tal medida. **Advertência escrita**: o Colaborador é advertido de forma escrita por seu Gestor imediato de forma respeitosa e privada, sem exposição nem constrangimento. É preciso

assinar a carta de advertência disciplinar, emitida pela área de Gestão de Pessoas, onde estarão claros os motivos que levaram a tal medida.
Suspensão: o Colaborador é afastado de suas atividades por um período determinado, não remunerado por três dias. O Colaborador deve ser comunicado por seu Gestor imediato de forma respeitosa e privada, dando ciência através da assinatura de um formulário, emitido pela área de Gestão de Pessoas, onde estarão claros os motivos que levaram a tal medida.
Demissão sem justa causa: o Colaborador é demitido pelo Gestor imediato, com apoio da área de Gestão de Pessoas; e com o pagamento de todos os seus direitos. A medida é aplicada quando não se tem elementos graves o suficiente para justificar uma demissão por justa causa.
Demissão por justa causa: - o Colaborador é demitido pelo Gestor imediato, com apoio da área de Gestão de Pessoas, de forma respeitosa e privada por meio de carta de desligamento, constando a alínea que justifica, através da lei trabalhista vigente (Art. 482), o motivo da medida. Neste caso, devem existir elementos suficientes que comprovem o ato, pautada em dispositivos legais previstos na legislação.

REVISÕES E APROVAÇÕES

Os documentos integrantes da estrutura normativa da Segurança da Informação da UNIMED deverão ser aprovados e revisados conforme os seguintes critérios:

Política
Nível de Aprovação: Diretoria, Gerente, Coordenadora do Comitê de Privacidade e Responsáveis de TI
Periodicidade de Revisão: A Unimed se reserva ao direito de revisá-la na periodicidade que melhor entender, não ultrapassando o período de 12 meses da última aprovação.

Histórico de Revisões do Documento		
Data	Versão	Descrição
01/12/2021	01	Criação da Política de Segurança da Informação.
10/01/2024	02	Revisão da Política e inclusão de novos dispositivos.
15/05/2024	03	Revisão da Política e ajustes nas diretrizes de senhas
19/08/2024	04	Revisão diretrizes de classificação de documentos

Data da última alteração	18/08/2024

PSI - Rev 04 - 19-08-2024 pdf

Código do documento f3f6d875-9bab-4df6-95c7-56cf36e4125a

Assinaturas

Rafael Borille da Fonseca
rafael.borille@unimed-as.com.br
Assinou

Carlos José Borges de Almeida
carlos.almeida@unimed-as.com.br
Assinou

George A.M. Silvestre
george.silvestre@unimed-as.com.br
Assinou

Daniel Freitas Andrade
daniel.freitas@unimed-as.com.br
Assinou

Eventos do documento

19 Aug 2024, 17:23:43
Documento f3f6d875-9bab-4df6-95c7-56cf36e4125a **criado** por DANIEL FREITAS ANDRADE (53bf65b2-3a47-49d4-b881-7fb219420c93). Email:informatica@unimed-as.com.br. - DATE_ATOM: 2024-08-19T17:23:43-03:00

19 Aug 2024, 17:25:15
Assinaturas **iniciadas** por DANIEL FREITAS ANDRADE (53bf65b2-3a47-49d4-b881-7fb219420c93). Email: informatica@unimed-as.com.br. - DATE_ATOM: 2024-08-19T17:25:15-03:00

19 Aug 2024, 17:32:44
RAFAEL BORILLE DA FONSECA **Assinou** - Email: rafael.borille@unimed-as.com.br - IP: 200.225.111.250 (200.225.111.250 porta: 49276) - Geolocalização: -28.4198 -50.9433 - Documento de identificação informado: 032.453.070-63 - DATE_ATOM: 2024-08-19T17:32:44-03:00

20 Aug 2024, 09:11:20
CARLOS JOSÉ BORGES DE ALMEIDA **Assinou** (c50edc65-920e-4fad-8597-27b067abcada) - Email: carlos.almeida@unimed-as.com.br - IP: 200.225.111.250 (200.225.111.250 porta: 53538) - Geolocalização: -28.4198 -50.9433 - Documento de identificação informado: 965.743.640-00 - DATE_ATOM: 2024-08-20T09:11:20-03:00

21 Aug 2024, 09:25:10

33 páginas - Datas e horários baseados em Brasília, Brasil
Sincronizado com o NTP.br e Observatório Nacional (ON)
Certificado de assinaturas gerado em 26 de August de 2024, 13:53:59

DANIEL FREITAS ANDRADE **Assinou** (e2241674-1b22-40ea-8aa5-57dc28a841d7) - Email: daniel.freitas@unimed-as.com.br - IP: 200.225.111.250 (200.225.111.250 porta: 8962) - Geolocalização: -28.4198 -50.9433 - Documento de identificação informado: 007.925.580-90 - DATE_ATOM: 2024-08-21T09:25:10-03:00

26 Aug 2024, 10:31:20
GEORGE A.M. SILVESTRE **Assinou** (b59b4552-260a-451c-b92b-574b20ca6aad) - Email: george.silvestre@unimed-as.com.br - IP: 200.225.111.250 (200.225.111.250 porta: 52314) - Geolocalização: -28.5026918 -50.9386399 - Documento de identificação informado: 229.779.700-10 - DATE_ATOM: 2024-08-26T10:31:20-03:00

Hash do documento original
(SHA256):cd4e5a07a16e7fcbba16a8bda510cefe2c94b1692e3bb569b3c44993b771c419
(SHA512):a5c4dc270a5308844209f5b7f40141322b14c508f18729daaaa15509e473d720fbc99f38dbe70b8694132479e14f397a58a6db207e0f9f463a2272ceff3d34d5

Esse log pertence **única** e **exclusivamente** aos documentos de HASH acima

Esse documento está assinado e certificado pela D4Sign