Sumário

1. OBJETIVO 2
2. ABRANGÊNCIA 2
3. DEFINIÇÕES 2
4. DIRETRIZES 4
4.1. Regras Gerais 4
4.2. Classificação da Informação 4
4.3. Acordos de Confidencialidade 4
4.4. Encerramento ou mudança da contratação 5
4.5. Gestão de Fragilidades e Incidentes de Segurança da Informação 5
4.6. Controle de Acesso Físico 5
4.7. Cópias de Segurança 5
4.8. Senhas 5
4.9. Internet 5
4.10. Correio Eletrônico 6
4.11. Gestão de Ativos e Uso de dispositivos 6
4.12. Uso de Dispositivos Pessoais 6
4.13. Mesa e tela limpa 6
4.14. Segurança em Home Office 6
4.15 Qualidade de Dados 6
4.16 Auditoria e Monitoramento 7
5. PAPÉIS E RESPONSABILIDADES 7
6. GESTÃO DE CONSEQUÊNCIAS 9
7. DISPOSIÇÕES GERAIS 9
8. SEGURANÇA DA INFORMAÇÃO, PRIVACIDADE E PROTEÇÃO DE DADOS 10
9. CANAL DE COMUNICAÇÃO REFERENTE A SEGURANÇA DA INFORMAÇÃO 10
10. REFERÊNCIAS 10

1. OBJETIVO

A política de Segurança da Informação da Unimed Fesp tem como objetivo estabelecer os princípios, diretrizes e responsabilidades em relação aos ativos da informação e informações clínicas, visando proteger suas propriedades de confidencialidade, disponibilidade e integridade.

2. ABRANGÊNCIA

Todas as pessoas físicas e jurídicas, inclusive administradores (sejam sócios, diretores, estatutários ou não, membros do Conselho de Administração e demais gestores), colaboradores, prestadores de serviços, parceiros e/ou quaisquer outros terceiros que mantenham um relacionamento com a Unimed Fesp e que, no âmbito dessa relação, possam vir a ter acesso às áreas, equipamentos, informações, arquivos, redes e dados de titularidade do Sistema e de seus beneficiários, cujo acesso seja controlado.

3. DEFINIÇÕES

Acordo de Confidencialidade: É o documento formal, juridicamente respaldado, contendo a descrição de uso permitido da informação, tempo de duração, responsabilidades, utilização da informação e consequências por violação do acordo.

Ambientes Internos: áreas comuns, áreas internas que envolvem departamentos, datacenter, salas de reunião, auditório, dentre outros ambientes que explicitam informações e pessoas atuantes na Unimed Fesp.

Aplicativos de Mensagens: WhatsApp, Telegram, face time, Skype, Facebook, messenger, Instagram, Twitter e outros que tenham finalidade igual ou similar. Ativos de Tecnologia de Informação: equipamentos fixos (computador, impressoras etc.), equipamentos móveis (smartphone, notebooks, tablets etc.), demais equipamentos de propriedade da Unimed Fesp, e-mails e os softwares utilizados dentro de seu ambiente. Denominados nesta política somente como ativos de TI.

Endpoint: é qualquer dispositivo, móvel ou não, que se comunica diretamente a uma rede principal de conexão. Pode ser um computador de mesa, notebook, tablet, celular e etc.

Gestor: Funcionário que ocupa um cargo de liderança e que desempenha esse papel está apta a interpretar os objetivos levantados pela empresa, atuando sempre com base no planejamento, organização, liderança e controle, convergindo tudo para a obtenção do que foi estipulado.

Incidente de Segurança: É toda a ação que viole as políticas internas, tais como: quaisquer

ações ou situações que possam expor a Unimed Fesp a perdas financeiras ou de imagem, direta ou indiretamente, potenciais ou reais, uso indevido de dados corporativos ou institucionais, divulgação não autorizada de informações ou de segredos comerciais industriais sem a autorização expressa dos proprietários ou área competente, uso de dados, informações, equipamentos, softwares, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, a não comunicação imediata de quaisquer violações ou atitudes anormais de que porventura um usuário da informação venha a tomar conhecimento ou presencie ou ainda, a não aderência às políticas de Segurança da Informação.

Rede pública: é um tipo de rede em que o público em geral, tem acesso e, por meio dela, pode se conectar a outras redes ou à Internet.

Risco de Segurança da Informação: Ameaças possam explorar vulnerabilidades em um ou mais ativos de informação e causar dano a organização (ISO 27005:2011).

Segurança da Informação: Conjunto de conceitos, técnicas e estratégias, as quais visam proteger os ativos de informação da Unimed Fesp a fim de preservá-las de ações não autorizadas relativas à manipulação, transferência ou destruição.

Spam: Qualquer mensagem, independentemente de seu conteúdo, enviada para vários destinatários, sem que os mesmos o tenham solicitado.

Spywares: Programas que espionam os hábitos de navegação dos usuários, a fim de instanciar janelas (do tipo pop-up) que exibem conteúdos de interesse dos usuários.

Vírus: São pequenos programas que, como os vírus biológicos, têm a propriedade de se juntar a outros arquivos, alterar seu funcionamento normal e se reproduzir (fazer cópias de si), contaminando outros arquivos, computadores e até servidores.

4. DIRETRIZES

A formulação desta Política deu-se com base na missão, nos princípios e valores da Unimed Fesp e em conformidade com as legislações vigentes e melhores práticas com relação a segurança da informação.

Os usuários da informação não deverão testar fragilidades de segurança, pois tais eventos serão interpretados como uso impróprio do sistema/exploração de vulnerabilidades.

Para garantir o objetivo referente a segurança da informação, 4 (quatro) pilares devem ser estabelecidos em linha com o praticado pelo mercado:

a) Confidencialidade: Garantia de que a informação estará disponível ou será divulgada somente para indivíduos, entidades, pessoas ou processos devidamente autorizados.
b) Integridade: Garantia de que a informação, armazenada ou em trânsito, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não;
c) Disponibilidade: Garantia de que a informação estará disponível sempre que for necessário.
d) Autenticidade: Garantia de que a informação provenha de uma fonte confiável e seja respaldada por frameworks testados e certificados por órgãos especializados em segurança da informação.

4.1. Regras Gerais

A Unimed Fesp estabelece regras com embasamento na lei de proteção de dados e privacidade assim como diretrizes de práticas de mercado de segurança da informação onde os colaboradores da Unimed Fesp conhecem e dão aceite dessas práticas.

4.2. Classificação da Informação

A Unimed Fesp estabelece, a partir de políticas e conscientização junto aos colaboradores, práticas de classificação da informação conforme diretrizes internas para proteção da marca Unimed Fesp.

4.3. Acordos de Confidencialidade

A disponibilização de informações confidenciais, seja para execução de projetos ou para elaboração de propostas de consultorias, auditorias e/ou fornecedores, deverá ser precedida da assinatura de um Acordo de Confidencialidade que, em sua contratação o colaborador já

a realiza.

Todos os contratos com prestadores de serviços ou demais entidades que irão se relacionar com a Unimed Fesp e que venham a acessar informações privilegiadas deverão conter, obrigatoriamente, a cláusula de confidencialidade, responsabilidade e consequências, caso as exigências previstas não sejam adequadamente cumpridas.

4.4. Encerramento ou mudança da contratação

A Unimed Fesp estabelece, a partir de políticas e diretrizes junto aos contratos, práticas de garantias de que seu encerramento ou mudança estejam em conformidade com as práticas de Segurança da Informação e Privacidade e Proteção de Dados.

4.5. Gestão de Fragilidades e Incidentes de Segurança da Informação

A Unimed Fesp tem o papel de proteger os ativos digitais e informações sensíveis contra possíveis ameaças cibernéticas. Isso envolve o monitoramento contínuo, detecção e resposta a incidentes de segurança, implementação de medidas de prevenção e conscientização, além de garantir conformidade com regulamentações.

4.6. Controle de Acesso Físico

A Unimed Fesp estabelece, a partir de políticas e normativos, práticas de proteção de controle de acesso físico com base no critérios da ISO 27001.

4.7. Cópias de Segurança

A Unimed Fesp estabelece as diretrizes para a realização de backup das informações. Arquivos corporativos, sistemas de produção, programas, aplicativos, sistemas operacionais, bancos de dados, scripts, parâmetros de configuração e testes periódicos de restauração de arquivos armazenados nos servidores.

4.8. Senhas

A Unimed Fesp estabelece, a partir de políticas, diretrizes e conscientização de seus colaboradores, práticas de gerenciamento de senhas e acessos que estejam em conformidade com as práticas de Segurança da Informação e Privacidade e Proteção de Dados.

4.9. Internet

A Unimed Fesp estabelece diretrizes e controles tecnológicos referentes aos acessos a todos

os sites que contemplam a web. Os colaboradores são conscientizados a quais acessos são permitidos e, ocorrendo quaisquer desvios, a orientação de comunicar à área responsável da Unimed Fesp que garante a segurança dos acessos web.

4.10. Correio Eletrônico

A Unimed Fesp estabelece em diretrizes e controles tecnológicos a proibição de utilização de e-mails pessoais e do e-mail corporativos para fins pessoais.

4.11. Gestão de Ativos e Uso de dispositivos

A Unimed Fesp estabelece a importância de se manter um registro meticuloso de todos os ativos, gerenciamento atento de seu uso e acesso, e garantias que a segurança desses ativos seja uma preocupação constante em todas as nossas operações.

4.12. Uso de Dispositivos Pessoais

É proibido o uso de dispositivos de computação pessoais de propriedade individual para a realização das atividades de trabalho relacionadas à Unimed Fesp.

4.13. Mesa e tela limpa

A Unimed Fesp estabelece a prática de mesa limpa e tela limpa; esta prática visa reduzir o risco de acesso não autorizado, perda e dano de informação tanto em formato digital quanto físico, durante e fora do horário normal de trabalho.

4.14. Segurança em Home Office

A Unimed Fesp pode adotar, para alguns colaboradores, a modalidade de trabalho home office, porém estabelece diretrizes a serem seguidas pelos colaboradores e terceiros que fazem uso dos recursos da Unimed Fesp.

4.15 Qualidade de Dados

A qualidade de dados significa garantir, aos titulares de dados, exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. Antes, vale esclarecer que a qualidade de dados não é, em si, um processo, mas a condição do estado qualitativo das informações em posse da companhia. Normalmente, entendemos que os dados de uma empresa são qualificados quando eles estão de acordo com sua atuação, seu planejamento e seu processo de tomada de decisões. No

campo da qualidade, lidamos com diferentes dimensões que, de maneiras diversas, evidenciam a pertinência de um conjunto de dados qualquer, dentre eles:

- **Acurácia**: mede-se o quanto um conjunto de dados reflete e representa, de fato, a realidade;
- **Completude**: certifica-se se cada dado possui todas suas informações requeridas discriminadas apropriadamente;
- **Consistência**: garante-se se os dados fazem sentido entre si e procura-se por contradição entre eles;
- **Validez**: confere-se se o dado em questão está em um formato adequado e pode ser utilizado segundo as diretrizes da empresa;
- **Unicidade**: verifica-se se cada informação aparece uma única vez ao longo da análise das bases de dados ou se ela se repete.

4.16 Auditoria e Monitoramento

O processo de monitoramento e auditoria é autorizado exclusivamente para atender o objetivo de averiguar o cumprimento das diretrizes corporativas, identificar conteúdo e/ou acessos indevidos, detectar fraudes ou coletar evidências para suportar a companhia em processos judiciais ou em atendimento às auditorias internas e externas, órgãos reguladores e fiscalizadores.

A Unimed Fesp reserva o direito de registrar e examinar todos os eventos relacionados ao acesso à Internet, a fim de garantir que os recursos não estejam sendo utilizados de forma indevida, ou, para fins não autorizados.

5. PAPÉIS E RESPONSABILIDADES

Alta Administração

- É a última instância responsável por supervisionar o desempenho e implementação das políticas, procedimentos e controles de segurança da informação.

Gestores

- Assegurar que os colaboradores estejam conscientes da importância da prática da boa segurança nas atividades diárias, e solicitar/providenciar educação e treinamento adequados e apropriados às suas responsabilidades, incluindo aspectos relevantes da legislação, regulamentos, direitos autorais e contratos;
- Acompanhar o cumprimento dessa política e assegurar que os riscos de segurança

em suas áreas de atuação estejam avaliados e controlados adequadamente;

- Orientar suas equipes sobre o uso adequado das informações e recursos de informações disponibilizados pela empresa;
- Sempre que necessário, devem documentar orientações específicas, regulamentando os níveis de confidencialidade das informações que geram e processam, bem como os direitos de acesso a essas informações;
- Prover informações necessárias para a identificação e tratamento de riscos e incidentes de Segurança da Informação.

Área Segurança da Informação

- Desenvolver e manter atualizada a política de Segurança da Informação;
- Monitorar o seu cumprimento, de forma proativa e sob demanda, sempre que solicitado por alguma área de negócio da Unimed Fesp;
- Definir e executar e/ou coordenar o programa de conscientização de usuários em Segurança da Informação;
- Identificar, planejar e coordenar programas para melhoria da segurança das informações, implementando e aprimorando os controles em todos os recursos tecnológicos e em projetos e processos de negócio;
- Revisar os impactos na segurança do ambiente tecnológico quando da alteração dos atuais recursos, inclusão de novos recursos, ou devido à aquisição de serviços e ativos da informação, emitindo parecer sobre as necessidades de adequação dos mesmos antes de iniciarem suas operações;
- Comunicar às áreas responsáveis a identificação de ocorrências de incidentes de segurança, para que medidas disciplinares cabíveis sejam adotadas;
- Manter registros e documentação de segurança em nível corporativo, incluindo um banco de dados de riscos e assuntos de segurança;
- Avaliar o risco de assuntos relacionados à segurança e comunicar os eventuais problemas às áreas competentes, provendo suporte nas eventuais ações preventivas e/ou corretivas;
- Registrar formalmente todos os incidentes de segurança da informação identificados e/ou reportados;
- Detectar, identificar e registrar violações, ou, tentativas de acessos relevantes e significativas não autorizadas, para tomada de providências corretivas, legal e de auditoria;

- Monitorar os acessos visando verificar: vazamento de informações; acessos ou tentativas de acessos a sites com conteúdo inadequado, repasse de conteúdo inadequado, tentativa de quebra de controles de segurança da informação e armazenamento de arquivos multimídia que não façam parte do negócio da Unimed Fesp;
- Revisar anualmente as regras de proteção estabelecidas;
- Restringir e controlar os acessos e os privilégios de usuários, incluindo os daqueles com privilégios de acesso remoto e externo;
- Em qualquer tempo ou momento, solicitar a restrição, bloqueio, suspensão e/ou cancelamento de acessos e/ou tecnologias (hardware e/ou software) que estejam infringindo as políticas de segurança ou nos casos em que sejam verificados incidentes de segurança, ou em que haja identificação de vulnerabilidades que necessitem de tempo para serem analisadas e se possível, corrigidas.

Usuários dos recursos de TI

- Os colaboradores da Unimed Fesp são reponsáveis pelo cumprimento das diretrizes estabelecidas na Política de Seguança da Informação, publicada e aprovada pela Alta Administração.

Auditoria Interna

- Supervisionar e monitorar a qualidade e integridade dos mecanismos de controles internos, gestão de riscos e Compliance da empresa, apresentando as recomendações de aprimoramento de políticas, práticas e procedimentos que entender necessárias, manifestando-se às áreas interessadas do negócio.

6. GESTÃO DE CONSEQUÊNCIAS

O descumprimento das diretrizes desta Política acarretará aplicação de medidas cabíveis conforme o respectivo grau de importância e de acordo com normativos internos.

7. DISPOSIÇÕES GERAIS

É competência da área Tecnologia da Informação, juntamente a todas as áreas envolvidas no processo, alterar esta Norma sempre que se fizer necessário e sua aprovação deverá ser feita via Alta Administração.

Esta Norma entra em vigor na data de sua publicação e revoga quaisquer normas e procedimentos em contrário.

As disposições desta Política têm validade pelo prazo de 1 (um) ano, quando deverá ser realizada a sua revisão, ou a qualquer momento no caso de necessidade de alteração.

8. SEGURANÇA DA INFORMAÇÃO, PRIVACIDADE E PROTEÇÃO DE DADOS

A Unimed Fesp se compromete em zelar pelo tratamento adequado de dados pessoais e sensíveis para fins legítimos que possam ser objeto de suas atividades e reforça tal compromisso com boas práticas de privacidade e proteção de dados, consubstanciado em sua política de segurança da informação.

Assim, declara que emprega medidas técnicas e organizacionais adequadas no trato com dados pessoais e sensíveis, e empenha esforços para protegê-los contra acessos não autorizados, perda, destruição, compartilhamento não autorizado, dentre outras hipóteses.

9. CANAL DE COMUNICAÇÃO REFERENTE A SEGURANÇA DA INFORMAÇÃO

A Unimed Fesp fornece o e-mail de contato dpo@unimedfesp.coop.br para tratativas de dúvidas, sugestões, reclamações e desvios de conduta da política de segurança da informação.

10. REFERÊNCIAS

Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 Tecnologia da informação. Técnicas de segurança. Código de prática para a gestão da segurança da informação, incluindo sua versão original e posteriores atualizações.

Lei do Marco Civil da Internet e suas respectivas alterações.

Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais, “LGPD”.

Lei federal 11.846 – Anticorrupção e Política de Relacionamento com Órgãos Públicos.

Resolução Normativa 443 da ANS, que dispõe sobre adoção de práticas mínimas de governança corporativa, com ênfase em controles internos e gestão de riscos, para fins de solvência das operadoras de planos de assistência à saúde.