Atividade: Política Geral de Segurança da Informação

Responsável: Coordenação da Tecnologia da Informação

Controle Histórico		
Revisão	**Data**	**Motivo / Alteração**
00	31/07/2020	Emissão inicial
01	11/05/2021	Revisão – Adequação à Lei Geral de Proteção de Dados
01	11/05/2021	Aprovação Diretoria Executiva

Siglas e Definições

ABNT NBR ISO/IEC 27002 - Gestão de Segurança da Informação

ABNT NBR ISO/IEC 27701 - Técnicas de segurança:

Hardware - É a parte física do computador, ou seja, peças e equipamentos utilizados para que o computador funcione.

Malware - Termo genérico usado para se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, worm, bot, spyware, backdoor, cavalo de troia e rootkit.

PGSI – Política Geral de Segurança da Informação

Software – Todo programa rodado em um computador, celular ou dispositivo que permita ao mesmo executar suas funções

TI – Tecnologia da Informação

Walk-thrus – Processo de verificação

Materiais

Materiais de Escritório

Tarefas

1 Visão geral

A informação é a força vital do negócio. Qualquer ambiente tecnológico é inútil se seu propósito principal de existência - o processamento e compartilhamento de informações - for ameaçado ou eliminado.

As informações coletadas, analisadas, armazenadas, comunicadas e compartilhadas podem estar sujeitas a furto, uso indevido, perda, acesso não autorizado, corrupção de dados, etc. Ademais, as informações podem ser colocadas em risco por falta de educação, conscientização ou treinamento e por uma violação dos controles de segurança.

Incidentes de segurança da informação podem gerar constrangimento, perda financeira, não conformidade com normas e legislação, bem como possíveis processos judiciais contra a Cooperativa.

Desta forma, é necessário implementar uma Política Geral de Segurança da Informação (PGSI) a fim de orientar e estabelecer as diretrizes corporativas da Unimed Nordeste Paulista para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários.

Esta Política de Segurança da Informação de alto nível (*high level*) fornece um esboço dos controles de segurança da informação adotados baseados em risco.

Cumpre, por fim, informar, que a presente PGSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2013 e ABNT NBR ISSO/IEC 27701:2019, reconhecida mundialmente como um código de prática para a gestão da segurança da informação e gestão da privacidade da informação, bem como está de acordo com as leis vigentes em nosso país.

2 Objetivo

O objetivo desta política é fornecer diretrizes destinadas a proteger as informações da Cooperativa, reduzir o risco comercial e jurídico e salvaguardar os investimentos e a reputação da Cooperativa.

Ademais, busca-se nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento, com o fim de preservar as informações da Unimed Nordeste Paulista quanto à:

• Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

• Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

• Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

3 Aplicação

Esta política e seus controles, processos e procedimentos de suporte se aplicam:

- A todas as unidades, áreas, setores e departamentos da Cooperativa.
- A todos os analistas de segurança da informação e administradores de sistemas responsáveis pela manutenção de sistemas, softwares, aplicativos, programas, dispositivos e equipamentos de TI gerenciados pela Cooperativa.
- A todos os dirigentes, funcionários em tempo integral, funcionários em meio período, funcionários em tempo parcial, trabalhadores contratados, consultores, estagiários, aprendizes, trabalhadores temporários, prestadores de serviços, agentes, parceiros, fornecedores e usuários autorizados que acessam as dependências da Cooperativa.
- A todos os sistemas, aplicativos, dispositivos e equipamentos de TI gerenciados pela Cooperativa que armazenam, processam ou transmitem dados e informações, incluindo redes de computadores, *hardwares*, *softwares* e aplicativos, dispositivos móveis e sistemas de telecomunicações.

- A todas as informações utilizadas na Cooperativa, em todos os formatos. Isso inclui informações processadas por outras organizações em suas relações comerciais com a Unimed Nordeste Paulista.

4 Política

4.1 Das Diretrizes Gerais

Esta Política visa garantir uma gestão sistêmica e efetiva em todos os aspectos relacionados à segurança da informação, provendo suporte as operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos a instituição através de uma Gestão de Segurança da Informação.

A Segurança da Informação será tema tratado pelo Comitê de Governança, Riscos, Proteção de Dados e Segurança da Informação, que contará com a participação de pelo menos um representante da diretoria executiva e um membro das seguintes áreas: Tecnologia da Informação, Jurídico, Recursos Humanos, Qualidade e Auditoria Interna.

Serão adotadas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida por todos os níveis da organização. Para isto serão executadas revisões periódicas para garantir a contínua pertinência e adequação as necessidades da Unimed Nordeste Paulista.

Toda informação produzida ou recebida pelos funcionários como resultado da atividade profissional contratada pela Unimed Nordeste Paulista pertence à referida instituição.

O uso dos equipamentos computacionais da Unimed Nordeste Paulista deverá estar direcionado apenas para fins de pesquisa, consultas, prestações de serviços e o desenvolvimento dos trabalhos voltados às atividades da Cooperativa.

Todos os equipamentos utilizados devem ser homologados pelo Departamento de TI da Unimed Nordeste Paulista e somente estes equipamentos estão autorizados a ter acesso à Rede.

4.1. Normas, controles, processos e procedimentos de segurança da informação complementares e auxiliares

Um conjunto complementar e auxiliar de normas, controles, processos e procedimentos de nível inferior para a segurança da informação deverá ser definido, em apoio a esta Política Geral de Segurança da Informação de alto nível e seus objetivos declarados.

Este conjunto de documentação de apoio deverá ser aprovado, publicado e comunicado aos funcionários da Cooperativa e partes externas relevantes.

4.2. Organização da Segurança da Informação

A Cooperativa definirá e implementará arranjos de governança adequados para a gestão da segurança da informação. Isso incluirá a identificação e alocação de responsabilidades de segurança, para iniciar e controlar a implementação e operação da segurança da informação dentro da Cooperativa.

Deverá haver um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designado como Comitê de Governança, Riscos, Proteção de Dados e Segurança da Informação.

4.3. Segurança de Recursos Humanos

A política de segurança da Cooperativa, seu conjunto complementar e auxiliar de normas, controles, processos e procedimentos de nível inferior e as expectativas de uso aceitável deverão ser comunicadas a todos os usuários para garantir que eles entendam suas responsabilidades. A educação e o treinamento em segurança da informação deverão ser disponibilizados a todos os funcionários, e o comportamento inadequado será abordado.

A depender do caso, as responsabilidades de segurança deverão ser incluídas nas descrições de funções, especificações pessoais e planos de desenvolvimento pessoal.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos funcionários, mediante assinatura de termo de responsabilidade. Todos os funcionários devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos.

4.4. Gestão de ativos

Todos os ativos (informações, *softwares*, equipamentos de processamento eletrônico de informações, etc.) deverão ser documentados e registrados. Os proprietários deverão ser identificados para todos os ativos e deverão ser responsáveis pela manutenção e proteção de seus ativos.

Todos os ativos de informação deverão ser classificados de acordo com seus requisitos legais, valor do negócio, criticidade e sensibilidade, e a classificação indicará os requisitos de manuseio apropriados. Todos os ativos de informação terão normas apropriadas para o seu descarte adequado e seguro.

4.5. Controle de acesso

O acesso a todas as informações deverá ser controlado e orientado pelos requisitos de negócios. O acesso deverá ser concedido ou providenciado para os usuários de acordo com sua função e a classificação da informação, apenas até um nível que lhes permita cumprir suas funções.

Um procedimento formal de registro e cancelamento de registro deverá ser mantido para o acesso a todos os sistemas e serviços de informação. Isso incluirá métodos de autenticação obrigatórios com base na confidencialidade das informações acessadas e incluirá a consideração de vários fatores, conforme apropriado.

Controles específicos deverão ser implementados para usuários com privilégios elevados de acesso, para reduzir o risco de uso negligente ou deliberado do sistema. A segregação de funções deverá ser implementada, sempre que possível.

Para concessão de acesso aos ativos de informação disponibilizados pela Unimed Nordeste Paulista, faz-se necessário, formalização de Acordo de Confidencialidade ou Cláusula de Confidencialidade em contrato.

4.6. Segurança Física e Ambiental

As instalações de processamento de informações deverão estar alojadas em áreas seguras, fisicamente protegidas contra acesso não autorizado, danos e interferência por perímetros de segurança definidos. Controles de segurança internos e externos deverão ser implementados para impedir o acesso não autorizado e proteger os ativos, especialmente aqueles que são críticos ou sensíveis, contra ataques cibernéticos.

4.7. Segurança de operações

A Cooperativa deverá garantir o funcionamento correto e seguro dos sistemas de processamento de informações.

Isso inclui:

- Procedimentos operacionais documentados;
- O uso de mudança formal e gerenciamento de capacidade;
- Controles contra *malware;*
- Controles de acesso;

- Gerenciamento de vulnerabilidade.

4.8. Segurança das comunicações

A Cooperativa deverá manter controles de segurança de rede para garantir a proteção da informação dentro de suas redes, e deverá fornecer as ferramentas e orientações para garantir a transferência segura de informação tanto dentro de suas redes quanto com entidades externas, de acordo com os requisitos de classificação e tratamento associados.

4.9. Aquisição, desenvolvimento e manutenção do sistema

Os requisitos de segurança da informação serão definidos durante o desenvolvimento dos requisitos de negócios para novos sistemas de informação ou mudanças nos sistemas de informação existentes.

Controles para mitigar quaisquer riscos identificados serão implementados quando apropriado.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

4.10. Relações com fornecedores

Os requisitos de segurança da informação da Cooperativa deverão ser considerados no estabelecimento de relações com fornecedores, para garantir que os ativos acessíveis aos fornecedores sejam protegidos.

A atividade do fornecedor será monitorada e auditada de acordo com o valor dos ativos e os riscos associados.

4.11. Gerenciamento de Incidentes de Segurança da Informação

A orientação deverá abordar o que constitui um incidente de segurança da informação e como isso deve ser relatado.

Violações reais ou suspeitas de segurança da informação deverão ser relatadas e serão investigadas.

Ações corretivas apropriadas deverão ser tomadas e qualquer aprendizado integrado aos controles.

Em caso de incidentes que afetem a segurança da informação deverá ser aberto chamado ao Departamento de Tecnologia da Informação, e se julgar necessário, deverá encaminhar posteriormente ao Comitê de Governança, Riscos, Proteção de Dados e Segurança da Informação para análise.

4.12. Aspectos de Segurança da Informação da Gestão de Continuidade de Negócios

A Cooperativa deverá estabelecer mecanismos para proteger processos de negócios críticos dos efeitos de grandes falhas de sistemas de informação ou desastres e para garantir sua recuperação oportuna de acordo com as necessidades de negócios documentadas.

Isso incluirá rotinas de *backup* adequadas e resiliência integrada.

Os planos de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados, no mínimo, anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

4.13. Conformidade

O projeto, operação, uso e gerenciamento de sistemas de informação deverão cumprir todos os requisitos de segurança estatutários, regulamentares e contratuais.

Atualmente, isso inclui a legislação de proteção de dados e as normas e padrões nacionais e internacionais voltados à segurança da informação.

A Cooperativa usará uma combinação de auditoria interna e externa para demonstrar conformidade com os padrões e melhores práticas escolhidos, incluindo políticas e procedimentos internos.

Isso incluirá verificações da “saúde” da TI, análises de lacunas em relação a padrões documentados, verificações internas de conformidade da equipe e feedbacks dos responsáveis pelos ativos de informação.

5 Responsabilidade

É responsabilidade da área de Segurança da Informação da Unimed Nordeste Paulista:

- Elaborar, implantar e seguir por completo a política, normas e procedimentos de segurança da informação, garantindo confidencialidade, integridade e disponibilidade da informação da Unimed Nordeste Paulista através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas.

- Disponibilizar para todos os funcionários, terceiros e fornecedores os procedimentos e normas de Segurança da Informação.

- Garantir a conscientização e educação de todos os funcionários, terceiros e fornecedores das práticas adotadas pela Unimed Nordeste Paulista referente a Segurança da Informação.
- Atender a todos os requisitos de Segurança da Informação aplicáveis ou exigidos por regulamentações, Leis ou Cláusulas Contratuais.
- Tratar todos os incidentes de Segurança da Informação registrando, classificando, investigando, corrigindo, documentando e quando necessário comunicando as autoridades apropriadas.
- Garantir através de adoção de implantação, testes e melhoria contínua a continuidade do negócio.
- Trazer sempre melhorias à Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

É responsabilidade de cada coordenador de departamento, área, setor ou unidade da Cooperativa garantir a aplicação desta política.

6 Verificação da Conformidade

O departamento de TI, o departamento de Gestão de Pessoas e os coordenadores de cada departamento, área, setor ou unidade da Cooperativa verificarão a conformidade com esta política por meio de vários métodos, incluindo, mas não se limitando a, *walk-thrus* periódicos, logs de auditoria de sistemas e banco de dados, auditorias de TI e feedbacks para o responsável pela política.

Qualquer mudança nesta política deve ser aprovada pelo departamento de TI.

Tanto a Política Geral de Segurança da Informação quanto as demais normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê responsável.

7 Exceções

Não há exceções a esta política. Qualquer exceção à esta norma deverá ser previamente aprovada pela equipe de TI.

8 Violação

Qualquer violação desta norma pode resultar em ação disciplinar, incluindo a rescisão do contrato de trabalho.

A Cooperativa reserva-se o direito de notificar as autoridades responsáveis pela aplicação da lei sobre qualquer atividade ilegal e de cooperar em qualquer investigação de tal atividade. A Cooperativa não considera que a conduta que viole esta norma esteja dentro do curso e âmbito das atividades de um funcionário, parceiro ou prestador de serviço, ou como consequência direta da execução de suas funções.

Consequentemente, na medida do permitido por lei, a Unimed Nordeste Paulista exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus funcionários, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Registros

Não se aplica

Anexos

INS.TI.001 - Instruções de Trabalho sobre Mesa e Tela Limpas

INS.TI.002 - Instruções de Trabalho sobre Construção de Senhas Fortes

INS.TI.003 - Instruções de Trabalho sobre Gerenciamento de Acesso

NOR.TI.001 - Normas sobre Avaliação de Vulnerabilidades

INS.TI.004 - Instruções de Trabalho sobre uso e segurança de dispositivos móveis

NOR.TI.002 - Normas sobre privilégios de acesso do usuário

NOR.TI.003 - Normas sobre acesso remoto

NOR.TI.004 - Normas para acesso ao datacenter

NOR.TI.005 - Normas sobre uso aceitável de sistemas e equipamentos

NOR.TI.006 - Normas sobre Backup e Restauração

INS.TI.005 - Instruções de Trabalho sobre eliminação segura de equipamentos, dispositivos, mídias e dados

INS.TI.006 - Instruções de Trabalho sobre trilhas (logs) de auditoria

Referências Bibliográficas

Não se aplica

Aprovação Diretoria

Ribeirão Preto, 11 de Maio de 2021

Dr. Edmilson Rocha Souza
Diretor Presidente

Dr. Luiz Roberto Lins Ferras
Diretor Vice-Presidente

Dr. Gustavo Ribeiro de Oliveira
Diretor Financeiro

Dr. Nilson Ricardo Salomão
Diretor de Desenvolvimento

Dr. Eurico Pelissari
Diretor Administrativo

Gustavo Priuli
Coordenador de TI

Mariana Ruzzi
Analista Compliance e Controles Internos