Política de Segurança da Informação

1 Área responsável pelo assunto

Gerência da Tecnologia e Inovação.

2 Abrangência

2.1 Esta política orienta o comportamento de toda a SIM - Caixa de Assistência à Saúde, e deve ser seguramente cumprida por todos os empregados, membros estatutários e disseminada às outras partes envolvidas com a Entidade, como Patrocinadoras, fornecedores, prestadores de serviços e beneficiários, considerando as necessidades específicas e os aspectos legais e regulamentares.

3 Público-alvo

3.1 Esta Política alcança todos os membros de órgãos de governança, empregados e partes envolvidas com a Entidade, incluindo patrocinadoras, fornecedores, prestadores de serviços e beneficiários.

4 Base

4.1 A presente Política foi elaborada com base nas melhores práticas e condutas estabelecidas pelas normas internacionais que tratam sobre os sistemas de gestão de segurança da informação e da privacidade de dados, em especial:

- ABNT NBR ISO/IEC 27001/2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação - Requisitos;
- ABNT NBR ISO/IEC 27002/2013 - Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação;
- ABNT NBR ISO/IEC 27701/2020 - Técnicas de segurança - Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação - Requisitos e diretrizes.

5 Periodicidade de Revisão

5.1 Esta Política deverá ser revisada anualmente e submetida ao Conselho Deliberativo para aprovação. Extraordinariamente essa política poderá ser revisada a qualquer tempo.

6 Apresentação

6.1 A Política de Segurança da Informação (PSI) é o documento embasado em diretrizes e normas de gestão de segurança da informação, que orienta e estabelece as diretrizes corporativas aplicáveis a todos os usuários e setores da SIM, a fim de proteger os ativos de informação da entidade.

6.2 As diretrizes estabelecidas neste documento descrevem a conduta considerada adequada para a manipulação de ativos de informação da entidade. Quaisquer condutas em desacordo com as diretrizes aqui descritas podem ser consideradas incidentes de segurança da informação.

7 Glossário

- **Ativo**: Tudo aquilo que possui valor para a SIM.
- **Ativo de informação**: Patrimônio intangível da SIM, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, mercadológico, de recursos humanos, legal, bem como quaisquer informações criadas ou adquiridas por meio de parceria, aquisição, licenciamento, compra ou confiadas a SIM por parceiros, clientes, empregados e

SEDE ADMINISTRATIVA: Avenida Atílio Pedro Pagani, 115 | sala 1801 | 18º andar | 88132-149 | | Palhoça | SC
ATENDIMENTO: Avenida Mauro Ramos, 1450 | sala 301 | 3º andar | 88020-301 | Centro | Florianópolis | SC
Central de Atendimento: 0800 642 9200 | central@simplanodesaude.com.br | www.simplanodesaude.com.br | Fone 48 3216 9200
ANS - nº 356476

terceiros, em formato escrito, verbal, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da SIM ou por infraestrutura externa contratada pela entidade, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

- **Confidencialidade**: Propriedade dos ativos da informação da SIM, de não serem disponibilizados ou divulgados para indivíduos, processos ou entidades não autorizadas.
- **Controle**: Medida de segurança adotada pela SIM para o tratamento de um risco específico.
- **Disponibilidade**: Propriedade dos ativos da informação da SIM, de serem acessíveis e utilizáveis sob demanda, por partes autorizadas.
- **Incidente de segurança da informação**: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da SIM.
- **Integridade**: Propriedade dos ativos da informação da SIM, de serem exatos e completos.
- **Risco de segurança da informação**: Efeito da incerteza sobre os objetivos de segurança da informação da SIM.
- **Segurança da informação**: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da SIM.
- **Usuário da Informação**: Usuário com vínculo empregatício ou não de qualquer área da SIM ou terceiros alocados na prestação de serviços a esta, indiferentemente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar/manipular qualquer ativo de informação da SIM para o desempenho de suas atividades profissionais.
- **Vulnerabilidade**: Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da SIM.

8 Objetivos

8.1 Estabelecer diretrizes de orientação aos colaboradores, fornecedores, prestadores de serviços, clientes e demais partes interessadas (stakeholders) da SIM relacionadas à segurança da informação.

8.2 Definir normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos que atinjam esta finalidade.

8.3 Preservar as informações da SIM quanto à:

- Confidencialidade: garantir que o acesso à informação seja realizado somente por pessoas autorizadas;
- Integridade: garantir que a informação permaneça em seu estado original, protegendo-a de alterações indevidas, intencionais ou acidentais; e
- Disponibilidade: garantir que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes quando necessário à realização de suas atividades.

9 Aplicações

9.1 As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, prestadores de serviços e demais partes interessadas, aplicando-se à todas as informações obtidas e tratadas por meio de qualquer forma e/ou ferramenta.

10 Requisitos

10.1 Para a uniformidade das informações, a presente Política de Segurança da Informação deverá ser comunicada a todos os colaboradores, fornecedores e prestadores de serviços da SIM a fim de que a política seja cumprida dentro e fora da entidade.

SEDE ADMINISTRATIVA: Avenida Atílio Pedro Pagani, 115 | sala 1801 | 18º andar | 88132-149 | | Palhoça | SC
ATENDIMENTO: Avenida Mauro Ramos, 1450 | sala 301 | 3º andar | 88020-301 | Centro | Florianópolis | SC
Central de Atendimento: 0800 642 9200 | central@simplanodesaude.com.br | www.simplanodesaude.com.br | Fone 48 3216 9200
ANS - nº 356476

10.2 Constará como anexo em todos os contratos da SIM a Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela entidade.
10.3 A responsabilidade em relação à segurança da informação será comunicada na fase de contratação dos colaboradores, sendo os mesmos orientados sobre os procedimentos de segurança constantes neste documento, assim como o uso correto dos ativos, a fim de reduzir possíveis riscos.
10.4 A SIM exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, terceiros e parceiros, reservando-se o direito de punir os infratores, analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis. Ainda, quaisquer danos ou obrigações suportadas pela SIM em razão do uso indevido, negligente ou imprudente deverão ser ressarcidos imediatamente pelo colaborador responsável.

11 RESPONSABILIDADES ESPECÍFICAS

11.1 USUÁRIOS DA INFORMAÇÃO

11.1.1 Responder por todo o prejuízo ou dano que vier a sofrer ou causar à SIM e/ou a terceiros em decorrência da não obediência às diretrizes aqui estabelecidas.
11.1.2 Classificar e manter registros sobre os dados e informações tratados.
11.1.3 Manter-se atualizado em relação à presente Política e aos procedimentos e normas relacionadas.
11.1.4 Buscar orientação do responsável interno pela Segurança da Informação e do Encarregado de Proteção de Dados Pessoais (DPO) sempre que não estiver absolutamente seguro quanto à coleta, tratamento ou eliminação de informações.

11.2 GESTORES DE PESSOAS E/OU PROCESSOS

11.2.1 Portar-se como referência de conduta aos demais usuários quanto às medidas de segurança da informação aqui estabelecidas.
11.2.2 Coletar dos usuários da informação a assinatura do Termo de Compromisso referente à presente Política, para o devido cumprimento das normas aqui estabelecidas.
11.2.3 Orientar sobre as políticas estabelecidas neste documento, bem como instruir acerca das responsabilidades de seu cumprimento aos novos usuários da informação, celetistas ou não, prestadores de serviços e parceiros da SIM, bem como instruir sobre a manutenção do sigilo e confidencialidade sobre os ativos de informações da entidade, ainda que após eventual término de contrato.
11.2.4 Realizar questionamentos sobre possíveis experiências com incidentes de segurança da informação ou privacidade nas entrevistas para contratação de novos colaboradores.
11.2.5 Coletar a assinatura no Acordo de Confidencialidade de usuários da informação casuais que não estejam cobertos por contrato anterior à concessão de acesso às informações da entidade.

12 CUSTODIANTES DA INFORMAÇÃO

12.1 ÁREA DA TECNOLOGIA DA INFORMAÇÃO

12.1.1 Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.
12.1.2 Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes de segurança da informação e privacidade.

SEDE ADMINISTRATIVA: Avenida Atílio Pedro Pagani, 115 | sala 1801 | 18º andar | 88132-149 | | Palhoça | SC
ATENDIMENTO: Avenida Mauro Ramos, 1450 | sala 301 | 3º andar | 88020-301 | Centro | Florianópolis | SC
Central de Atendimento: 0800 642 9200 | central@simplanodesaude.com.br | www.simplanodesaude.com.br | Fone 48 3216 9200
ANS - nº 356476

12.1.3 Configurar os equipamentos, ferramentas e sistemas concedidos aos usuários da informação com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI, em especial a instalação e atualização de antivírus, anti-malware e firewalls.

12.1.4 Atribuir responsabilidades administrativas e operacionais a fim de restringir, ao mínimo necessário, os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de usuários que possam excluir logs e trilhas de auditoria das suas próprias ações.

12.1.5 Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes, implantando controles de integridade para torná-las juridicamente válidas como evidências.

12.1.6 Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas diferentes áreas da entidade.

12.1.7 Administrar, proteger e testar as cópias de segurança (backups) dos softwares e dados relacionados aos processos críticos e relevantes da SIM.

12.1.8 Realizar cópias de segurança (backups) dos dados gerados pelos sistemas internos e mantê-las em local adequado e separado do banco de dados.

12.1.9 Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário;
- os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

12.1.10 Segregar e controlar rigidamente os ambientes de produção, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

12.1.11 Proteger continuamente todos os ativos de informação da SIM contra código malicioso e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso ou indesejado.

12.1.12 Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da entidade.

12.1.13 Realizar auditorias periódicas de configurações técnicas e análise de riscos.

12.1.14 Responsabilizar-se pelo uso, manuseio e guarda de assinaturas e certificados digitais.

12.1.15 Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da entidade operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

12.1.16 Monitorar o ambiente de TI, gerando indicadores, históricos e registros auditáveis de:

- uso da capacidade instalada da rede e dos equipamentos;
- tempo de resposta no acesso à internet e aos sistemas críticos da SIM;
- períodos de indisponibilidade no acesso à internet e aos sistemas críticos da SIM;
- incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e demais eventos);
- atividade de todos os usuários da informação durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos e enviados, uploads e downloads de arquivos, entre outros).

12.1.17 Comunicar previamente o gestor responsável sobre o fim do prazo de retenção de dados e informações.

12.1.18 Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários, sendo permitido, apenas, quando for necessário para a execução de atividades operacionais sob sua responsabilidade, como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

SEDE ADMINISTRATIVA: Avenida Atílio Pedro Pagani, 115 | sala 1801 | 18º andar | 88132-149 | | Palhoça | SC
ATENDIMENTO: Avenida Mauro Ramos, 1450 | sala 301 | 3º andar | 88020-301 | Centro | Florianópolis | SC
Central de Atendimento: 0800 642 9200 | central@simplanodesaude.com.br | www.simplanodesaude.com.br | Fone 48 3216 9200

ANS - nº 356476

12.1.19 Nas hipóteses de movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

12.1.20 Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da SIM em processos de mudança, sendo necessária a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso por terceiros.

13 ÁREA DE SEGURANÇA DA INFORMAÇÃO

13.1.1 Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

13.1.2 Propor e apoiar iniciativas que visem à segurança dos ativos de informação da SIM.

13.1.3 Promover a conscientização dos usuários da informação em relação à relevância da segurança da informação para o negócio da SIM, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.

13.1.4 Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

13.1.5 Buscar alinhamento com as diretrizes corporativas da entidade.

13.1.6 Avaliar os incidentes de segurança e propor ações corretivas.

13.1.7 Manter contato constante com o Encarregado pelo Tratamento de Dados Pessoais da SIM, visando manter as comunicações atualizadas, além de treinamentos e campanhas de conscientização constantes na entidade.

14 SEGURANÇA FÍSICA

14.1.1 Deve haver proteção das instalações físicas de processamento de informações da SIM, prevenindo o acesso físico não autorizado de terceiros e interferências com os recursos de processamento das informações da entidade.

14.1.2 As portas externas da SIM devem ser adequadamente protegidas contra acessos não autorizados, mediante fechaduras, alarmes ou outros mecanismos de segurança.

14.1.3 As portas e janelas devem permanecer trancadas quando estiverem sem monitoramento.

14.1.4 Armários, gavetas, arquivos e demais locais de armazenamento de informações, devem sempre ser trancados com chaves ou outros mecanismos de proteção quando não estiverem sendo utilizados.

14.1.5 Equipamentos e informações só podem ser retirados do local mediante autorização prévia e expressa do gestor direto, ou responsável designado por esta.

15 POLÍTICA DE MESA LIMPA E TELA PROTEGIDA

15.1.1 As informações sensíveis ou críticas devem ser guardadas em lugar seguro e não devem ser deixadas sobre a mobília, para evitar acesso de terceiros não autorizados.

15.1.2 Os terminais de acesso à informação (computadores e demais dispositivos) devem ser mantidos desligados quando sem monitoração e protegidos por bloqueio de tela quando não estiverem em uso, sendo necessário informar o login (usuário e senha) sempre que voltar a ser utilizado.

15.1.3 Os equipamentos devem ser programados para realizar seu bloqueio automático após o período de 1 minuto de inatividade.

15.1.4 A área de trabalho do computador (desktop ou notebook) deve possuir a menor quantidade possível de arquivos salvos, evitando a visualização não autorizada de terceiros.

15.1.5 Documentos que contenham informações confidenciais ou dados sensíveis devem ser removidos da impressora imediatamente após sua impressão.

SEDE ADMINISTRATIVA: Avenida Atílio Pedro Pagani, 115 | sala 1801 | 18º andar | 88132-149 | | Palhoça | SC
ATENDIMENTO: Avenida Mauro Ramos, 1450 | sala 301 | 3º andar | 88020-301 | Centro | Florianópolis | SC
Central de Atendimento: 0800 642 9200 | central@simplanodesaude.com.br | www.simplanodesaude.com.br | Fone 48 3216 9200

ANS - nº 356476

16 CONTROLES CRIPTOGRÁFICOS

16.1.1 A SIM assegura o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e integridade da informação, considerando as seguintes diretrizes:

- Identificar o nível de proteção exigido pelos ativos, empregando avaliação de risco, para definir a força e a qualidade do algoritmo de criptografia requerido, quando necessário;
- Utilizar criptografia para proteger as informações críticas, principalmente as que contenham dados sensíveis, transportadas e/ou armazenadas em dispositivos móveis, mídias removíveis ou através de redes de computadores;
- Convém que, quando possível, a entidade utilize-se de mídias físicas removíveis e/ou dispositivos que permitam a criptografia, quando do armazenamento de dados pessoais, especialmente em mídias que poderão ser transportadas fora do ambiente físico da entidade.
- Utilizar certificados SSL assinados por autoridades certificadoras confiáveis em sistemas web, prevenindo que as informações acessadas ou transmitidas não sejam interceptadas por pessoas não autorizadas;
- Utilizar assinaturas digitais ou códigos de autenticação, para validar a autenticidade ou integridade de informações críticas armazenadas ou transmitidas;
- Os algoritmos criptográficos e o tamanho de chaves devem ser selecionados de acordo com o nível de criticidade das informações e dos sistemas que a suportam, para que não ocorram impactos desnecessários, tanto de falta de segurança, quanto de segurança excessiva;
- As chaves criptográficas devem ser protegidas contra modificação e perda;
- As chaves privadas e secretas devem ser protegidas contra uso ou divulgação não autorizada;
- As chaves devem ser distribuídas de forma segura para os usuários devidamente autorizados;
- Revogar chaves comprometidas ou àquelas utilizadas por usuários que não possuírem mais autorização para tal utilização;
- Observar a utilização de ferramentas e meios de comunicação que tenham controles criptográficos na transmissão de arquivos, principalmente os que contenham informações críticas e dados pessoais; e
- Manter registro e auditoria das atividades relacionadas ao gerenciamento das chaves criptográficas.

17 PROTEÇÃO CONTRA MALWARE

17.1.1 A SIM assegura que as informações e os recursos de processamento da informação estarão protegidos contra malware, devendo-se considerar que:

- está expressamente proibida a utilização de softwares não autorizados;
- haverá prevenção e detecção de acessos não autorizados e do uso de software não autorizado, por meio da configuração de controles através de firewalls de aplicação;
- haverá restrição e ficarão registradas as tentativas de acesso por parte dos usuários a websites maliciosos ou suspeitos;
- será realizada a instalação e atualização periódica de software de detecção e remoção de malware para a varredura de computadores e mídias magnéticas;
- irá isolar-se, ao máximo possível, ambientes críticos que possam ser contaminados por malwares para evitar impactos às atividades do negócio;
- serão configuradas varreduras automáticas e completas, a serem realizadas regularmente por soluções de antivírus.

18 SEGURANÇA NAS COMUNICAÇÕES

SEDE ADMINISTRATIVA: Avenida Atílio Pedro Pagani, 115 | sala 1801 | 18º andar | 88132-149 | | Palhoça | SC
ATENDIMENTO: Avenida Mauro Ramos, 1450 | sala 301 | 3º andar | 88020-301 | Centro | Florianópolis | SC
Central de Atendimento: 0800 642 9200 | central@simplanodesaude.com.br | www.simplanodesaude.com.br | Fone 48 3216 9200
ANS - nº 356476

18.1 A SIM assegura a proteção das informações e dos recursos de processamento que as suportam dentro dos meios de comunicação disponibilizados pela entidade.

18.2 A proteção dos meios de comunicação para garantia da segurança da informação nas redes e os serviços a ela conectadas requer que as responsabilidades e procedimentos sobre os gerenciamentos de rede sejam observados, como responsabilidade operacional pelas redes; controles sobre os dados que trafegam sobre as redes públicas ou redes sem fio; mecanismos de monitoramento e detecção de ações que possam afetar a segurança da informação; e a restrição de conexão de sistemas à rede interna.

19 TRANSFERÊNCIA DE INFORMAÇÃO

19.1 SIM manterá a segurança das informações transferidas dentro da entidade e com quaisquer entidades externas, buscando sempre utilizar-se de procedimentos e controles para proteger a transferência de informações, principalmente as que contenham informações críticas e dados pessoais, contra a interceptação, cópia, modificação, desvio e/ou destruição.

19.2 A Transferência de Informações deverá observar controles criptográficos com o foco em proteger a confidencialidade, a integridade e a autenticidade das informações, conforme determina o item 6 deste Política.

19.3 E-mail

- O uso do e-mail de domínio da SIM é para fins exclusivamente corporativos e relacionados às atividades do usuário da informação dentro da instituição. A utilização desse recurso para fins pessoais não é permitida.
- As mensagens de e-mail sempre incluirão assinatura do usuário contendo: nome do usuário da informação, função desempenhada, nome da SIM, contato telefônico e e-mail corporativo.
- É proibido aos usuários da informação o uso do e-mail corporativo para:
  - enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas ao interesse legítimo da instituição e previa e expressamente autorizada por esta.
  - enviar mensagens através do e-mail do departamento/setor ao qual pertence ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
  - enviar qualquer mensagem que torne seu remetente ou a SIM vulneráveis a responsabilizações judiciais;
  - divulgar informações, dados, documentos e afins sem autorização expressa concedida pelo proprietário do ativo da informação;
  - falsificar informações de endereçamento ou adulterar cabeçalhos para esconder a identidade de remetentes ou destinatários;
  - excluir mensagens pertinentes do e-mail sem motivo justificado;
  - produzir, transmitir ou divulgar mensagem que:
    i. contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da SIM;
    ii. contenha ameaças eletrônicas, como: spam, mail bombing ou vírus de computador;
    iii. contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
    iv. inclua imagens criptografadas ou de qualquer forma mascaradas;
    v. tenha conteúdo considerado impróprio, obsceno ou ilegal;
    vi. seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico ou cause qualquer espécie de dano;
    vii. contenha perseguição preconceituosa baseada em sexo, raça, orientação sexual, incapacidade física ou mental ou qualquer outro tipo de preconceito;
    viii. tenha fins políticos com âmbito local ou nacional (propaganda política);
    ix. inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

SEDE ADMINISTRATIVA: Avenida Atílio Pedro Pagani, 115 | sala 1801 | 18º andar | 88132-149 | | Palhoça | SC
ATENDIMENTO: Avenida Mauro Ramos, 1450 | sala 301 | 3º andar | 88020-301 | Centro | Florianópolis | SC
Central de Atendimento: 0800 642 9200 | central@simplanodesaude.com.br | www.simplanodesaude.com.br | Fone 48 3216 9200
ANS - nº 356476

20 INTERNET

20.1 Qualquer informação acessada, transmitida, recebida ou produzida na internet utilizando-se da infraestrutura da SIM está sujeita a divulgação e auditoria. Assim, a SIM, em conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

20.2 Os equipamentos, tecnologias e serviços fornecidos para o acesso à internet são de propriedade da SIM, que pode analisar e, se necessário, bloquear qualquer arquivo, site, e-mail, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação e demais normas internas.

20.3 As tentativas de alteração dos parâmetros de segurança, por qualquer dos usuários da informação, sem o devido credenciamento e autorização, será julgada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo Gestor, podendo haver responsabilização.

20.4 O uso da internet para assuntos pessoais é tolerado com bom senso, e desde que não comprometa a banda da rede, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse.

20.5 Somente os usuários da informação que estão devidamente autorizados podem representar a SIM nos meios de comunicação, como e-mail, entrevista on-line, podcast, documento físico, bem como em outras hipóteses em que a entidade precise ser representada.

20.6 Apenas os usuários da informação autorizados poderão copiar, captar, imprimir ou enviar imagens da tela (print screen) para terceiros, devendo atender à norma interna de uso de imagens.

20.7 Os usuários da informação poderão fazer o download somente de programas ligados diretamente às suas atividades na da SIM e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados.

20.8 Os usuários da informação não poderão efetuar upload de qualquer software licenciado à SIM ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

20.9 É proibido o uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente.

20.10 É proibido a utilização dos recursos da SIM para fazer o download ou distribuição de software ou dados ilegais.

20.11 Os usuários da informação não poderão utilizar os recursos da SIM para, deliberadamente, propagar qualquer tipo de malware, vírus, worm, cavalo de troia, spam, perturbação, programas de controle de outros computadores ou qualquer espécie de código malicioso.

20.12 O acesso a softwares peer-to-peer e sites de proxy não são permitidos.

20.13 O download e a utilização de programas de entretenimento, jogos ou música, bem como serviços de streaming e comunicação poderão ser realizados mediante solicitação e aprovação do responsável interno pela Segurança da Informação e do Encarregado de Proteção de Dados Pessoais (DPO).

20.14 O acesso à rede de internet da SIM pelos dispositivos pessoais dos usuários da informação é permitido, desde que cumpridos os mesmos requisitos previstos neste documento, e demais normas de segurança, para os dispositivos de propriedade da SIM.

21 COMPUTADORES E RECURSOS TECNOLÓGICOS

21.1 Os equipamentos disponibilizados aos usuários da informação são de propriedade da SIM, cabendo a todos a correta utilização e manuseio para as atividades de interesse da entidade, assim como o cumprimento das recomendações constantes neste documento.

SEDE ADMINISTRATIVA: Avenida Atílio Pedro Pagani, 115 | sala 1801 | 18º andar | 88132-149 | | Palhoça | SC
ATENDIMENTO: Avenida Mauro Ramos, 1450 | sala 301 | 3º andar | 88020-301 | Centro | Florianópolis | SC
Central de Atendimento: 0800 642 9200 | central@simplanodesaude.com.br | www.simplanodesaude.com.br | Fone 48 3216 9200

ANS - nº 356476

21.2 É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento e autorização prévia e expressa da SIM.

21.3 Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente.

21.4 Em caso de suspeita de vírus, malware ou problema técnico, o usuário deverá comunicar ao seu gestor imediato e ao responsável interno pela Segurança da Informação.

21.5 Os equipamentos devem permanecer conectados em rede local e permitir o monitoramento de recursos através de softwares específicos.

21.6 A transferência ou divulgação de qualquer software, programa ou instrução de computador para terceiros, por qualquer meio (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante e se for autorizado pela SIM.

21.7 Arquivos pessoais ou não pertinentes ao negócio da SIM (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para os drives de rede, evitando a sobrecarga do armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem comunicação prévia ao usuário.

21.8 Todos os arquivos imprescindíveis para as atividades da entidade deverão ser salvos no sistema nuvem determinado pelo responsável interno pela Segurança da Informação e do Encarregado de Proteção de Dados Pessoais (DPO). Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador.

21.9 Os usuários da informação da SIM e detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e autorização da SIM.

21.10 No uso dos computadores, equipamentos e recursos de informática de propriedade da entidade, deve-se atender às seguintes regras:

- Os usuários da informação devem informar ao seu gestor imediato e ao responsável interno pela Segurança da Informação sobre qualquer dispositivo estranho conectado ao seu computador;
- É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos;
- O usuário da informação deverá manter a configuração do equipamento disponibilizado pela SIM seguindo os devidos controles de segurança exigidos pela presente PSI e pelas normas específicas da entidade, assumindo a responsabilidade como custodiante de informações;
- Deverão ser protegidos por senha (bloqueados) todos os terminais de computador que não estiverem sendo utilizados;
- Todos os recursos tecnológicos adquiridos pela SIM devem ter imediatamente suas senhas padrões (default) alteradas;
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos usuários da informação, datas e horários de acesso.

21.11 É proibido o uso de computadores e recursos tecnológicos da SIM para:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Acessar informações confidenciais sem explícita autorização do proprietário;
- Acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Vigiar secretamente alguém por dispositivos eletrônicos ou softwares, como, por exemplo, através de analisadores de pacotes (sniffers);
- Interromper um serviço, servidor ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

SEDE ADMINISTRATIVA: Avenida Atílio Pedro Pagani, 115 | sala 1801 | 18º andar | 88132-149 | | Palhoça | SC
ATENDIMENTO: Avenida Mauro Ramos, 1450 | sala 301 | 3º andar | 88020-301 | Centro | Florianópolis | SC
Central de Atendimento: 0800 642 9200 | central@simplanodesaude.com.br | www.simplanodesaude.com.br | Fone 48 3216 9200
ANS - nº 356476

- Hospedar pornografia, material racista ou preconceituoso, ou qualquer outro tipo que seja considerado ilegal ou indevido;
- Utilizar software ilegal ou que de qualquer modo viole direitos autorais do efetivo proprietário.

22 DISPOSITIVOS MÓVEIS

22.1 Por dispositivo móvel entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da SIM ou de particulares conectados à rede da entidade, como: notebooks, smartphones e pen drives.

22.2 Para os equipamentos de propriedade da SIM, a entidade reserva-se o direito de inspecioná-los a qualquer tempo.

22.3 Todo usuário da informação deve realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel, devendo mantê-las separadas em dispositivo diverso.

22.4 Deve ser utilizado bloqueio automático nos dispositivos móveis, assim como desbloqueio mediante senha ou outro mecanismo que garanta a segurança das informações ali contidas.

22.5 É proibida a alteração de configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e geração de logs, exceto nas hipóteses de autorização pela SIM.

22.6 É proibido a instalação e utilização de softwares para fins pessoais no equipamento fornecido pela entidade sem a devida autorização pelo responsável pela Segurança da Informação e do Encarregado de Proteção de Dados Pessoais (DPO).

22.7 É permitido o uso de rede banda larga de locais conhecidos pelo usuário, a exemplo de sua casa, hotéis, fornecedores e clientes, sendo proibido o acesso a redes wi-fi públicas.

22.8 Em caso de furto ou roubo de um dispositivo móvel de propriedade da SIM, notificar imediatamente o gestor responsável, ao responsável interno pela Segurança da Informação e o Encarregado de Proteção de Dados Pessoais (DPO) da entidade, bem como realizar o registro de um boletim de ocorrência (B.O.) junto à autoridade policial e encaminhar uma via ao gestor imediato e ao Encarregado de Proteção de Dados Pessoais (DPO).

22.9 O uso do dispositivo móvel é de responsabilidade do usuário, principalmente nas hipóteses de uso indevido, negligente ou que ocasionem qualquer tipo de dano à SIM ou terceiros.

22.10 O usuário da informação que deseje utilizar equipamentos móveis particulares ou adquirir acessórios e posteriormente conectá-los à rede da SIM deverá submeter previamente tais equipamentos ao processo de autorização pelo responsável pela Segurança da Informação e do Encarregado de Proteção de Dados Pessoais (DPO).

23 IDENTIFICAÇÃO

23.1 O uso dos equipamentos e sistemas corporativos devem ser permitidos somente mediante a identificação do usuário, através de login e senha ou outro meio de identificação pessoal e intransferível.

23.2 É dever do responsável pela Tecnologia da Informação a criação da identidade lógica dos usuários da informação na entidade, devendo distinguir os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas ou jurídicas.

23.3 No primeiro acesso ao ambiente de rede local, o usuário deverá alterar imediatamente a sua senha conforme as orientações apresentadas.

23.4 Os acessos devem ser registrados, contendo, no mínimo, informações de data, hora, usuário e recurso acessado.

23.5 O uso dos dispositivos e senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

SEDE ADMINISTRATIVA: Avenida Atílio Pedro Pagani, 115 | sala 1801 | 18º andar | 88132-149 | | Palhoça | SC
ATENDIMENTO: Avenida Mauro Ramos, 1450 | sala 301 | 3º andar | 88020-301 | Centro | Florianópolis | SC
Central de Atendimento: 0800 642 9200 | central@simplanodesaude.com.br | www.simplanodesaude.com.br | Fone 48 3216 9200
ANS - nº 356476

23.6 Todos os dispositivos de identificação utilizados na SIM, as identificações de acesso aos sistemas, os certificados e assinaturas digitais, bem como os dados biométricos, devem estar associados à pessoa física e atrelados aos seus documentos de identificação oficiais.

23.7 O usuário será o responsável pelo uso correto dos seus dispositivos identificadores.

23.8 É proibido o compartilhamento de login e outros dispositivos de identificação pessoal com outras pessoas em qualquer hipótese, especialmente nas funções relacionadas à administração de sistemas.

23.9 Na hipótese de existir login de uso compartilhado por mais de um usuário da informação, a responsabilidade pelo uso será daqueles que o utilizam. O gestor só será responsabilizado se for identificado seu conhecimento ou solicitação acerca do uso compartilhado.

23.10 Os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários, em especial nos casos de desligamento de colaborador, cabendo ao responsável pela Tecnologia da Informação tomar essa providência. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenham se encerrado, aos usuários de testes e outras situações similares.

23.11 As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (word, excel, etc.) ou físicos (post-it, agenda, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como nome próprio, nome de familiares, data de nascimento, endereço, placa de veículo, nome da entidade, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321” entre outras, atendendo, ainda, aos seguintes requisitos:

- Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível;
- Os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

23.12 É de responsabilidade de cada usuário a memorização de sua própria senha, podendo, ainda, utilizar-se de aplicações de gerenciamento criptografado de senhas, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

23.13 Após 3 (três) tentativas infrutíferas de acesso, a conta do usuário deverá bloqueada, sendo necessário que o usuário entre em contato com o responsável pela Segurança da Informação e o Encarregado de Proteção de Dados Pessoais (DPO) para regularizar o acesso, mediante processo de renovação de senha, após a confirmação de sua identidade.

23.14 Os usuários podem alterar a própria senha a qualquer tempo, devendo tomar tal providência imediatamente em caso de suspeita de que terceiros obtiveram acesso indevido ao seu login/senha.

23.15 A periodicidade máxima para troca das senhas é 90 (noventa) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a entidade, bem como os logins com privilégios administrativos, devem exigir a troca de senhas a cada 60 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

23.16 Caso o usuário esqueça sua senha, ele deverá requisitar formalmente a troca junto ao responsável pela Tecnologia da Informação.

24 PROTEÇÃO DE DADOS PESSOAIS

24.1 Os usuários da informação, fornecedores e parceiros da SIM deverão observar o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

SEDE ADMINISTRATIVA: Avenida Atílio Pedro Pagani, 115 | sala 1801 | 18º andar | 88132-149 | | Palhoça | SC
ATENDIMENTO: Avenida Mauro Ramos, 1450 | sala 301 | 3º andar | 88020-301 | Centro | Florianópolis | SC
Central de Atendimento: 0800 642 9200 | central@simplanodesaude.com.br | www.simplanodesaude.com.br | Fone 48 3216 9200
ANS - nº 356476

24.2 A SIM se compromete a tratar os dados pessoais relacionados ao seu objeto social, observando a boa-fé e os princípios da finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

24.3 A entidade cumpre as diretrizes estabelecidas na Política de Privacidade, informando aos titulares de dados sobre as finalidades e as bases legais de tratamento de dados pessoais.

25 RESPONSABILIZAÇÃO

25.1 As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e demissão por justa causa.

25.2 A aplicação de sanções e punições será realizada conforme a análise conjunta do gestor direto, do diretor geral e do corpo jurídico ("Conselho") da SIM, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o Conselho, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.

25.3 No caso de terceiros contratados ou prestadores de serviço, o Gestor deverá, em conjunto com o Encarregado e o Diretor da área, analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato.

25.4 Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em danos à SIM, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos acima.

26 TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

26.1 A SIM realiza a gestão dos incidentes de segurança da informação, incluindo a comunicação sobre vulnerabilidades e eventos de segurança da informação, conforme segue:

26.2 Estabelecendo responsabilidades e procedimentos para tratamento de incidentes, como forma de garantir respostas rápidas e efetivas, bem como definindo canal de comunicação de incidentes de segurança da informação, de modo que as partes interessadas possam notificar sobre os eventos detectados.

26.3 Implementando ferramentas de monitoramento de sistemas, capazes de emitir alertas de vulnerabilidades e indisponibilidade dos serviços e sistemas.

26.4 Todos os usuários da informação são responsáveis por notificar qualquer evento de segurança da informação, assim que esses eventos forem detectados, ou o mais breve possível.

26.5 Planejando e implantando planos de contingência, como resposta aos incidentes, para manter a continuidade do negócio em um nível aceitável.

26.6 Cumprindo as diretrizes estabelecidas na Política de Gestão de Incidentes de Segurança da Informação e Privacidade.

27 DISPOSIÇÕES FINAIS

27.1 O usuário da informação assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na SIM, mesmo depois de terminado o vínculo contratual com a entidade.

27.2 Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da SIM. Ou seja, qualquer incidente de segurança deve ser imediatamente comunicado ao responsável interno pela Segurança da Informação e o Encarregado de Proteção de Dados Pessoais (DPO), especialmente no caso de incidentes envolvendo dados pessoais, para que sejam

SEDE ADMINISTRATIVA: Avenida Atílio Pedro Pagani, 115 | sala 1801 | 18º andar | 88132-149 | | Palhoça | SC
ATENDIMENTO: Avenida Mauro Ramos, 1450 | sala 301 | 3º andar | 88020-301 | Centro | Florianópolis | SC
Central de Atendimento: 0800 642 9200 | central@simplanodesaude.com.br | www.simplanodesaude.com.br | Fone 48 3216 9200
ANS - nº 356476

tomadas todas as providências cabíveis para mitigação das consequências e reparação dos danos causados.

27.3 A SIM, por meio do responsável interno pela Segurança da Informação e do Encarregado de Proteção de Dados Pessoais (DPO), poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

28 DOCUMENTOS RELACIONADOS

28.1 Para efeitos de conformidade, análise de risco, auditoria, registro de incidentes e aplicação de medidas disciplinares, esta Política de Segurança da Informação relaciona-se aos seguintes documentos organizacionais:

- Inventário de Ativos da Informação;
- Política de Privacidade e Proteção de Dados Pessoais.

29 Data da Última aprovação pelo Conselho Deliberativo

29.1 27 de março de 2023, revisão aprovada.

30 Tabela de Controle de Versionamento

Vigência	27.03.2023 a 27.03.2024
Versão	**3**
Histórico de Alterações	Atualização para aprovação do CODEL

SEDE ADMINISTRATIVA: Avenida Atílio Pedro Pagani, 115 | sala 1801 | 18º andar | 88132-149 | | Palhoça | SC
ATENDIMENTO: Avenida Mauro Ramos, 1450 | sala 301 | 3º andar | 88020-301 | Centro | Florianópolis | SC
Central de Atendimento: 0800 642 9200 | central@simplanodesaude.com.br | www.simplanodesaude.com.br | Fone 48 3216 9200

ANS - nº 356476

ANEXO I

TERMO DE COMPROMISSO
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Declaro que recebi e li integralmente a Política de Segurança da Informação da **SIM – Caixa de Assistência à Saúde**, concordando com as regras e orientações nela contidas e assumindo o compromisso de cumpri-las em sua totalidade.

Estou ciente de que:

- havendo dúvida sobre a aplicação de algum ponto deste documento, devo saná-las junto ao responsável pela Segurança da Informação e ao Encarregado de Proteção de Dados Pessoais (DPO) da **SIM**;
- os ambientes, sistemas, computadores e redes da entidade poderão ser monitorados e gravados, seguindo as normas legais vigentes, bem como de que devem manter-se atualizados em relação a eventuais alterações e atualizações deste documento e de procedimentos e normas relacionadas;
- são de propriedade da **SIM** todas as criações, materiais, ideias, conhecimentos, know-how, processos, produtos, métodos, programas de computador, algoritmos, códigos fonte, desenhos, e tudo o mais que venha a ser desenvolvido/descoberto ou produzido em razão da atuação da **SIM**;
- a partir da data de assinatura do presente Termo, a não observância desta Política de Segurança da Informação (PSI) e demais normas organizacionais poderá implicar na caracterização de falta grave, permanecendo passível de aplicação das penalidades cabíveis, a critério da entidade.

_____
Nome

_____
CPF

_____, ___/____/20__.
Local e data

_____
Assinatura

SEDE ADMINISTRATIVA: Avenida Atílio Pedro Pagani, 115 | sala 1801 | 18º andar | 88132-149 | | Palhoça | SC
ATENDIMENTO: Avenida Mauro Ramos, 1450 | sala 301 | 3º andar | 88020-301 | Centro | Florianópolis | SC
Central de Atendimento: 0800 642 9200 | central@simplanodesaude.com.br | www.simplanodesaude.com.br | Fone 48 3216 9200

ANS - nº 356476