Código: TCI.POL.002 Versão: 000	POLITICA TECNOLOGIA DA INFORMAÇÃO	Unimed Santa Bárbara d'Oeste e Americana

PSI - TERCEIROS E CONTRATADOS

CONTROLE DE REVISÃO		
Revisão	**Descrição**	**Data**
00	Criação	01/10/2020

PSI - TERCEIROS E CONTRATADOS

1 OBJETIVO

Estabelecer diretrizes para tratamento e proteção dos dados obtidos, utilizados e/ou armazenados na Cooperativa Unimed Santa Bárbara d'Oeste, Americana e Nova Odessa, na Unimed Participações, na CSC Unipart, nos Laboratórios UNICOO e na Usimed, aqui denominadas simplesmente EMPRESAS, sob os aspectos de confidencialidade, integridade, disponibilidade e legalidade, bem como orientar e informar nossos parceiros.

2 PROCEDIMENTO

2.1 EXECUTORES

Todos os parceiros das EMPRESAS e seus funcionários, aqui denominados simplesmente TERCEIROS, devem cumprir a presente norma para obter acesso às informações e aos recursos disponibilizados para que exerçam suas atividades.

2.2 PROPRIEDADE INTELECTUAL

A Cooperativa Unimed Santa Bárbara D'Oeste, Americana e Nova Odessa é a única e exclusiva titular dos direitos de propriedade sobre qualquer um de seus ativos tangíveis ou intangíveis.

Todas as informações produzidas por TERCEIROS no exercício de suas atividades são de propriedade exclusiva da Cooperativa Unimed Santa Bárbara D'Oeste, Americana e Nova Odessa e estão protegidas por sigilo profissional.

Caso o TERCEIRO necessite usar qualquer conteúdo externo para o exercício de suas atividades, ele deverá obter uma autorização formal e prévia do titular dos direitos de propriedade da informação, bem como o aval da Diretoria Executiva, obtido através de seu Gestor/Diretor das EMPRESAS, que poderá ser revogado a qualquer tempo.

2.3 RECURSOS

Os recursos tecnológicos existentes nos ambientes físicos e lógicos das EMPRESAS são de propriedade exclusiva da Cooperativa Unimed Santa Bárbara d'Oeste, Americana e Nova Odessa, devendo os TERCEIROS mantê-los e conservá-los.

Os recursos devem ser utilizados exclusivamente para fins profissionais, isto é, qualquer uso sem autorização ou para fins não relacionados à atividade que exerce será considerado como uso impróprio, estando o executor sujeito à notificação, intervenção ou desligamento.

2.4 PROTEÇÃO E PRIVACIDADE DE DADOS

Os dados obtidos, utilizados e/ou armazenados nas EMPRESAS, em formato físico ou lógico, devem ser protegidos de modificação, substituição, utilização inadequada, acesso indevido, divulgação não liberada, compartilhamento não autorizado, furto e roubo.

Portanto, o acesso a qualquer um dos recursos delegados à TERCEIROS somente será permitido para o executor que concordar com as normas presentes nessa política.

2.5 NORMAS

Todo e qualquer TERCEIRO somente poderá ter acesso às informações e aos recursos que são necessários para a execução de suas atividades, sem exceções.

2.5.1 DAS CREDENCIAIS E LIBERAÇÃO DE ACESSO

Sempre que possível, os recursos tecnológicos estarão protegidos por credencial de acesso, como medida de autenticação. Nesse sentido, cada TERCEIRO terá seu próprio *login* e senha para utilizar os recursos disponibilizados pelas EMPRESAS.

Tais cadastrados serão definidos, gerados e disponibilizados pelo departamento de Recursos Humanos, em conjunto com a equipe de Suporte Técnico, sendo que as senhas deverão possuir no mínimo 6 (seis) caracteres com, obrigatoriamente, 01 (uma) letra maiúscula, 01 (um) número e 01 (um) caractere especial, assim como renovadas a cada 03 meses (90 dias), não sendo permitida a reutilização das últimas 03 (três) senhas.

É responsabilidade do TERCEIRO manter suas credenciais de acesso seguras de qualquer uso indevido, considerando, ainda, que o cadastro será bloqueado após 3 (três) tentativas frustradas de autenticação, necessitando, assim, de uma nova senha inicial.

Cabe ao TERCEIRO comunicar as EMPRESAS sempre que do seu lado houver o desligamento ou mudanças no quadro de funcionários, para que os mesmos tenham seus acessos devidamente cancelados.

2.5.2 DO ACESSO AO AMBIENTE FÍSICO

As EMPRESAS estabelecerão limites físicos para controle de acesso de TERCEIROS e proteção de seus ativos, logo, cabe à cada um respeitar o que lhe foi estabelecido e permitido.

É expressamente proibido filmar ou fotografar equipamentos e áreas internas das EMPRESAS sem prévia autorização formal.

2.5.3 DO ACESSO AO AMBIENTE LÓGICO

De acordo com a necessidade da atividade a ser executada, os computadores e dispositivos dos TERCEIROS só poderão ser conectados na rede interna das EMPRESAS após aprovação do Comitê de Segurança da Informação, que avaliará, junto da equipe de Suporte Técnico, o *status* de proteção desses objetos.

Pois, solicitada e permitida a conexão, o TERCEIRO está ciente seus computadores e dispositivos estão sujeitos a vistoria, sempre que a lei vigente permitir.

Quando necessário, o acesso remoto ao ambiente lógico das EMPRESAS ocorrerá via VPN (Virtual Private Network), mediante a utilização de tuneis criptografados para manter a segurança das informações trafegadas. Nesses casos, a equipe de Suporte Técnico disponibilizará o acesso VPN para facilitar o trabalho remoto, ficando como responsabilidade para o TERCEIRO, conectar-se usando esse meio disponível e de acordo com as orientações que receberá por escrito.

As EMPRESAS sempre que necessário tornarão disponível para os TERCEIROS o acesso gratuito à internet por meio de sua rede wireless e registrará a data e hora de início e término do acesso, além o cadastro de acesso do utilizador que, nesse período, será inteiramente responsável por seus atos e eventuais prejuízos causados às EMPRESAS ou terceiros.

Esse formulário registrará a data e hora de início e término do acesso, além o cadastro de acesso do utilizador que, nesse período, será inteiramente responsável por seus atos e eventuais prejuízos causados às EMPRESAS ou terceiros.

2.6 GESTÃO DE INCIDENTES

Todos os TERCEIROS devem reportar, formal e imediatamente, para o Comitê de Segurança da Informação, os incidentes sobre os quais tenham tomado conhecimento que afetou, ou que tiveram potencial para afetar, a confidencialidade, integridade ou disponibilidade dos ativos das EMPRESAS, incluindo a conduta de outros colegas colaboradores internos ou TERCEIROS, através do e-mail: seguranca.informacao@unimedsa.com.br.

A não comunicação de incidentes será considerado falta grave, podendo representar inclusive conluio ou coparticipação na infração.

2.7 CONTATOS ÚTEIS

Departamento de Segurança da Informação:
(19) 3471 4268
E-mail: seguranca.informacao@unimedsa.com.br

Equipe de Suporte Técnico:
(19) 3471 3040
0800 21233
E-mail: helpdesk@unimedsa.com.br

3 REFERÊNCIA

A presente Política de Segurança de Dados é baseada e complementada pelas seguintes normas e procedimentos:

- ISO/IEC 27002:2006;
- Norma Interna: TCI-007-NOR-TECNOLOGIA DA INFORMAÇÃO-SUPORTE;
- Política Interna: TCI-014-POL-SEGURANÇA DA INFORMAÇÃO;
- Lei nº 13.709/2018 – LGPD; e
- Portaria nº 93, de 26 de setembro de 2019, Glossário de Segurança da Informação.

4 ANEXO

Não aplicável.

Elaboração: GABRIELA MORAIS - Auxiliar Qualidade
Aprovação: Coordenação Tecnologia da Informação,
Publicação:

PSI - TERCEIROS E CONTRATADOS

SQ_QUALIDADE_OPS

Código: TCI.POL.002 Versão: 000	POLITICA TECNOLOGIA DA INFORMAÇÃO	Unimed Santa Bárbara d'Oeste e Americana
PSI - TERCEIROS E CONTRATADOS		