



DENTSUL
COOPERATIVA DE ASSISTÊNCIA ODONTOLÓGICA VALE DO CAÍ

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
– PRIVACIDADE E PROTEÇÃO DE DADOS

Setembro, 2022

Versão: 1.1



1. APRESENTAÇÃO

A Revolução Digital consolidada nas últimas décadas tornou possível um enorme avanço: a coleta, contabilização e processamento de quantidades significativas de dados do turbilhão de eventos que ocorrem todos os dias na sociedade. Hoje podemos extrair mais facilmente desses dados muitas informações que servem como farol orientador importantíssimo para tomada de decisões e identificação de oportunidades.

Considerando que os dados podem ser usados na tomada de decisões importantes, seu valor é reconhecido e deve ser preservado. O grande valor atrai grandes ameaças. Não devem cair nas mãos erradas. Adulterações e indisponibilidade podem levar a decisões erradas ou falta de ação.

Estas são as bases e justificativas para a Segurança da Informação, que visa a manutenção da Confidencialidade, Integridade e Disponibilidade das informações. E o instrumento importante para isso é a Política de Segurança da Informação, um conjunto de diretrizes, normas, procedimentos e padrões a serem observados e seguidos por todas as pessoas que utilizarem a infraestrutura da Cooperativa.

Salienta-se que há compartilhamento de dados com terceiros, de maneira única e exclusiva para fins de cumprimento de obrigação legal ou regulatória, uma vez que a Cooperativa possui obrigação legal de prestar informações a agências regulatórias como a ANS (Agência Nacional da Saúde), Receita Federal, INSS, entre outras entidades públicas que fiscalizam a atividade da Cooperativa. Além disso, tal compartilhamento objetiva atender aos interesses do titular dos dados, de modo a possibilitar o fiel cumprimento do contrato de prestação de serviços entabulado entre as partes.

2. DIRETRIZES

Estes são os princípios básicos que regem a Política de Segurança da Cooperativa de Assistência Odontológica Vale do Cai – DENTSUL, estabelecidos de acordo com as necessidades da instituição.

1. À Cooperativa de Assistência Odontológica Vale do Cai – DENTSUL é atribuída a guarda de informações de seus cooperados, clientes diretos e indiretos, fornecedores e empregados. Portanto, a criação de um ambiente que garanta a disponibilidade e proteção é essencial para a continuidade de negócio da Cooperativa.
2. Toda a informação deverá ser classificada formalmente quanto à sua confidencialidade, integridade e disponibilidade, e ser tratada de acordo com a sua



classificação, independente da sua forma de armazenamento, digital ou não.

3. Dados Pessoais e informações relacionadas à pessoa natural identificada ou identificável, devem obrigatoriamente ser protegidos de acordo com a Lei Geral de Proteção de Dados (LGPD) e tratados como confidenciais quando não houver justificativa legítima em contrário. Cuidados redobrados devem ser tomados em relação aos Dados Pessoais Sensíveis, aqueles que podem revelar enfermidades, origem racial, étnica, opinião política, convicção religiosa, filosófica, filiação sindical, dados genéticos ou biométricos, relacionados a saúde, vida sexual ou orientação sexual.
4. As informações devem ter o ciclo de vida programado. Informações consideradas confidenciais, quando não mais necessárias, devem ser eliminadas através de mecanismos apropriados. O descarte ou reutilização de mídias contendo essas informações deve ser feito de forma a inviabilizar sua recuperação.
5. Todo o indivíduo que tenha acesso às dependências da Cooperativa de Assistência Odontológica Vale do Cai – DENTSUL deverá ser identificado. O acesso de terceiros em áreas onde exista o processamento físico ou digital de informações deverá ser fundamentado pela estrita necessidade, e deverá ocorrer sempre com o acompanhamento de empregado da Cooperativa, responsável pelas informações naquele setor.
6. Todos os equipamentos na Cooperativa deverão estar inventariados e identificados de forma individual.
7. Credenciais de acesso às instalações e sistemas são pessoais, não compartilháveis e intransferíveis. O usuário é responsável por todas as atividades desenvolvidas mediante autenticação com sua credencial, por isso deve zelar por sua proteção e sigilo, e realizar as ações de manutenção apropriadas para cada tipo de credencial, como a troca periódica de senhas.
8. Alterações no ambiente de produção devem ser previamente estudadas, formalizadas por processo padronizado, comunicadas, autorizadas e, sempre que possível, testadas em ambiente apropriado e isolado, anteriormente à efetiva colocação dos recursos em produção, para verificação e avaliação dos impactos causados no processo produtivo, com o objetivo de garantir a estabilidade do ambiente.
9. Os empregados, durante a vigência e após o término do contrato de trabalho ou prestação de serviço, não podem se apropriar de informações ou de mídias, equipamentos, componentes ou acessórios que as contêm, como por exemplo: e-mails corporativos, planilhas, arquivos de dados ou vídeos.
10. A responsabilidade de manter a segurança é compartilhada por todos os colaboradores. A Cooperativa de Assistência Odontológica Vale do Cai – DENTSUL deverá ministrar treinamentos para promover a conscientização e preparo.



3. NORMAS

Violações das normas abaixo relacionadas, incidentes ou falhas de segurança devem ser notificadas imediatamente à equipe de Segurança da Informação da Cooperativa de Assistência Odontológica Vale do Cai – DENTSUL em principalmente o CONTROLADOR, na forma do artigo 48 da LGPD.

Se houver mera possibilidade de vazamento de Dados Pessoais, deve ser notificado também imediatamente o Encarregado de Processamento de Dados (DPO), bem como o CONTROLADOR.

3.1. Segurança Física

1. Todo o indivíduo ao ingressar nas instalações da Cooperativa de Assistência Odontológica Vale do Cai – DENTSUL deverá usar crachá de identificação.
2. Pessoas externas à Cooperativa deverão ser identificadas na recepção e o seu ingresso nas instalações da Cooperativa de Assistência Odontológica Vale do Cai – DENTSUL será realizado mediante autorização e acompanhamento do empregado da Cooperativa.
3. Todo o equipamento que ingressar ou sair da Cooperativa de Assistência Odontológica Vale do Cai – DENTSUL, deverá estar acompanhado da respectiva nota fiscal e autorização do setor de Patrimônio.
4. Os prestadores de serviços da Cooperativa de Assistência Odontológica Vale do Cai – DENTSUL são responsáveis pelas ações ou prejuízos causados por seus empregados ao patrimônio da Cooperativa de Assistência Odontológica Vale do Cai – DENTSUL, bem como deverão garantir a manutenção da confidencialidade das informações acessadas.
5. Documentos ou papéis contendo informações confidenciais, quando não mais necessários, deve ser triturados ou destruídos de forma a impossibilitar leitura.
6. Mídias do tipo somente leitura (discos CD-ROM, CD-R, DVD, etc) contendo informações confidenciais, quando não mais necessárias, devem ser quebradas ou destruídas de forma a impedir seu uso indevido.
7. Mídias graváveis (drives HD ou SSD, pen drives, cartões SD, fitas, discos CD ou DVD do tipo RW, ou assemelhados) contendo informações confidenciais, quando não mais necessárias, devem ser zeradas com o procedimento seguro e adequado indicado pela equipe de Segurança da Informação antes de seu reuso ou descarte.
8. A entrega de documentos com informações confidenciais pode ocorrer apenas com registro e a garantia de identificação de quem recebe e mediante prévia assinatura de termo de confidencialidade.
9. Os equipamentos e seus componentes internos serão inventariados



periodicamente e somente colaboradores autorizados podem fazer remanejo de equipamentos e peças.

3.2. Credenciais

1. Credenciais, identificações e senhas de acesso devem ser individuais e mantidas em sigilo, não devem ser transferidas ou compartilhadas.
2. Cada colaborador deve trocar periodicamente suas senhas e é de sua responsabilidade escolher senhas robustas, complexas e longas.
3. As senhas devem ser únicas, não devem ser usadas senhas idênticas ou semelhantes para identificação em sistemas, sites ou serviços não gerenciados pela Cooperativa de Assistência Odontológica Vale do Cai – DENTSUL, sejam de natureza pessoal ou não

3.3. Uso da Rede

1. O acesso à Internet é fornecido para atividades e finalidades da Cooperativa. Acessos com fins particulares lícitos podem ser feitos ocasionalmente, preferencialmente fora do horário de expediente, desde que não violem as demais normas.
2. É proibido usar a rede para acessar ou enviar conteúdo pornográfico, ofensivo ou difamatório, bem como para constranger terceiros ou qualquer outro indivíduo titular de dados.
3. O uso para fins particulares de redes sociais como Facebook ou Twitter e sítios de vídeos como YouTube, Vimeo e Netflix durante o horário de expediente é considerado inadequado e pode estar bloqueado a qualquer horário a critério da Cooperativa.
4. Qualquer sítio conhecido de conteúdo vedado ou inadequado pode estar em listas de bloqueio automático. Eventuais erros na classificação de determinado sítio podem ser comunicados à equipe responsável pela tecnologia de informação para retificação.
5. Os acessos à Internet podem ser monitorados e registrados pela Cooperativa. Os registros ficam à disposição da Cooperativa pelo tempo que esta julgar adequado.
6. O compartilhamento de recursos nas estações de trabalho deve ser limitado a atividades de interesse da Cooperativa, com liberação somente para leitura por conjunto restrito de usuários.
7. Não é permitido instalar, usar ou configurar equipamentos (hardware ou software) que deem acesso à rede corporativa sem autorização formal e conhecimento da Equipe de Segurança da Informação. Em especial, não é permitida a instalação de ponto de acesso wifi, bluetooth, modem, hub, switch, vpn, roteador ou software de acesso remoto para fins pessoais.



8. Não é permitido copiar arquivos ou realizar acessos com fins particulares que onerem excessivamente a utilização da rede.
9. Todas as mensagens enviadas por correio eletrônico com o endereço profissional são de propriedade da Cooperativa, portanto devem ser usadas para assuntos de interesse da Cooperativa de Assistência Odontológica Vale do Cai – DENTSUL e não se deve manter qualquer expectativa de privacidade de seus conteúdos.
10. É vedado o envio de mensagens com conteúdo eleitoral, difamatório, ofensivo, preconceituoso, obsceno, pornográfico ou que dê margem a interpretação de discriminação racial, sexual, religiosa ou política.
11. Não é permitido distribuir, via correio eletrônico, grupos de discussão, fóruns e formas similares de comunicação mensagens não solicitadas do tipo “corrente” e mensagens em massa, comerciais, de propaganda política ou o envio de correio eletrônico não solicitado, SPAM.
12. Notebooks, laptops, tablets e outros equipamentos pessoais ou de terceiros não devem ser ligados diretamente na rede da Cooperativa sem autorização. Tais equipamentos podem ser conectados à rede wifi e ter acesso a serviços internos via VPN gerenciada pela Cooperativa.

3.4. Proteção de Estações

1. Em todas as estações de trabalho e dispositivos tecnológicos em geral deve estar instalado, ativo e atualizado, os mecanismos de segurança indicado pelo responsável pela administração da tecnologia de informação para a operacionalização segura de todos os sistemas.
2. O usuário não deve impedir a operação e atualização do antivírus sem autorização e conhecimento da equipe de administração do antivírus.
3. Constatado qualquer problema com o antivírus, o usuário deverá comunicar ao responsável técnico que tomará as providências cabíveis.

3.5. Utilização de Programas

1. As estações de trabalho são disponibilizadas com os programas – sistema operacional e aplicativos – mínimos necessários para o desempenho de sua função básica.
2. São considerados legítimos os softwares instalados e utilizados conforme suas licenças de uso e que não contrariem as demais regras da Cooperativa e a legislação. Em especial, esta norma contempla a possibilidade de uso de software livre para fins legítimos e não abusivos.
3. Não é permitida a instalação nos equipamentos da Cooperativa de qualquer software, gratuito ou não, sem as devidas licenças para uso comercial da Cooperativa.



4. O uso ou instalação de software sem licença de uso, ou em nome de outros sem autorização, caracteriza crime de pirataria, ficando o usuário da estação e o instalador sujeitos às sanções administrativas, legais e penais da legislação.
5. Ocasionalmente, serão realizadas verificações no inventário dos equipamentos, com relação a hardware e software permitindo identificar desvios das normas.

3.6. Cópias de Segurança ou Backup

1. Cada usuário é responsável pela manutenção de cópias de segurança de seus arquivos de dados.
2. Arquivos gerados nos dispositivos tecnológicos da Cooperativa que necessitem cópia de segurança deverão ser armazenados em servidor de arquivos apropriado da mesma, desde que autorizado pelo responsável. É responsabilidade do colaborador confirmar com o responsável pela tecnologia de informação que as pastas estão incluídas nas rotinas de cópias de segurança.
3. Não é permitida a cópia de dados confidenciais para processamento ou armazenamento em serviços externos, de terceiros não autorizados pela Cooperativa ou cliente.
4. Sempre que possível, os dados confidenciais devem estar criptografados nos backups.
5. O responsável pelo servidor deverá ativar processo de backup das informações críticas, incluindo serviços como correio eletrônico, banco de dados e aplicações.
6. Todo o backup deve periodicamente passar por teste de restauração.
7. Meios de armazenamento devem ser guardados em local seguro e de acesso limitado, armário, cofre ou sala com chave ou controle de acesso e devem ser respeitados os tempos de vida útil sugeridos pelo fabricante.
8. Alguns backups têm tempo de vida determinado por lei, portanto a equipe responsável pelos backups deve ser informada e zelar por mantê-los disponíveis durante esse tempo, bem como os equipamentos necessários para sua recuperação quando necessário.

3.7. Sistemas e Aplicações

1. Não é permitida a transferência de dados para processamento ou armazenamento em serviços externos, de terceiros não autorizados expressamente pela Cooperativa ou cliente.
2. Armazenamento e transferências de dados confidenciais devem ser sempre criptografadas com mecanismos aprovados pela Cooperativa.
3. Os sistemas deverão gerar registros (logs) de eventos de segurança. Devem ser utilizados para este fim funções do Sistema de Segurança em uso, recursos



do sistema operacional, recursos de banco de dados e/ou recursos da aplicação. Os registros deverão conter ao menos as seguintes informações: identificação da aplicação e função, momento da ocorrência (timestamp), informações que identifiquem a máquina ou local da ocorrência e os dados relevantes manipulados pela aplicação. O Sistema de Segurança poderá se encarregar do registro de algumas dessas informações. Informações confidenciais não devem ser registradas em log sem estarem criptografadas.

4. No desenvolvimento e manutenção de sistemas é obrigatório o uso de software e repositório de controle e versionamento de arquivos (como fontes, modelos, documentos, diagramas, páginas web) aprovado pela Cooperativa.
5. Cada desenvolvedor é responsável pela integridade dos arquivos de sistema que estão sendo trabalhados, devendo utilizar preferencialmente áreas de trabalho em servidores designados. Caso estejam residentes em sua máquina, o desenvolvedor deve providenciar cópia de segurança (backup) dos mesmos, quando necessária.
6. Todo o desenvolvedor de aplicações deverá seguir, quando disponíveis e forem aplicáveis, as recomendações de segurança para o desenvolvimento.

3.8. Administração de Servidores

1. Todas as instalações de novos servidores deverão seguir procedimentos padrões e incluir pacotes, Service Packs, Hot Fixes obrigatórios.
2. Após sua instalação o responsável deverá encaminhar à Equipe de Segurança solicitação para verificação complementar do servidor.
3. A instalação das atualizações de segurança deverá ser realizada pelo responsável direto de cada servidor, seguindo as orientações de segurança no que tange ao backup antes do procedimento, adequação de horário e plano de recuperação de falhas;
4. Acessos remotos devem ser feitos sempre usando mecanismos criptografados. Devem ser desativados os serviços de acesso remoto que não usam criptografia, tais como TELNET, FTP e VNCSERVER;
5. Os dispositivos tecnológicos utilizados devem possuir sistema operacional atualizado e com recursos de segurança.
6. A ativação de novos serviços de rede será condicionada a uma análise de riscos (a ser realizada pelo responsável pela tecnologia da informação), onde, no mínimo, os seguintes aspectos serão considerados: requisitos de segurança do serviço, objetivo, alvo do serviço, forma de acesso, forma da administração e volume de tráfego.
7. Não é permitida a instalação de serviços de rede não autorizados pelo responsável pela tecnologia da informação.
8. Todo o tráfego de informações confidenciais por meio compartilhado será



protegido através de criptografia.

9. Sistemas de proteção de acesso (firewall) devem ser utilizados para permitir apenas às redes ou máquinas alvo dos serviços o acesso aos mesmos mediante solicitação para a equipe de Segurança.
10. A equipe de Segurança da Informação pode indicar e usar ferramentas de detecção e prevenção de intrusos, para emitir alertas e registrar possíveis tentativas de invasão.

3.9. Registros e Auditoria

1. Os administradores devem habilitar registros de segurança (logs), de forma a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditorias;
2. Os registros de segurança deverão ser analisados periodicamente (manual ou automaticamente).

3.10. Documentação Exigida

1. É fortemente recomendado que sistemas críticos tenham documentado Plano de Continuidade de Negócio ou Recuperação de Desastre.
2. Todas as instalações e atualizações deverão ser documentadas pelo responsável, administrador ou desenvolvedor, inclusive:
 - Procedimentos para instalação;
 - Correções instaladas (service packs, hot fixes, patches);
 - Softwares instalados/atualizados;
 - Configurações a serem realizadas;
 - Permissões de acesso;
 - Contatos para suporte;
 - Informações Complementares.

3.11. Segurança Física de Servidores

1. O acesso físico aos servidores e equipamentos de infraestrutura deve ser restrito aos empregados e terceiros autorizados.
2. Os servidores e equipamentos de infraestrutura devem operar em ambiente adequado, sob condições (temperatura, nível de poeira, umidade, etc) indicadas pelo fabricante.



3.12. Do Encarregado de Proteção de Dados

1. A Cooperativa de Assistência Odontológica Vale do Caí - DENTSUL constitui a Sra. Eloísa Inês de Oliveira como Encarregada de Proteção de Dados (DPO), uma vez que possui grande conhecimento sobre o ciclo de dados da Cooperativa, além de deter domínio técnico sobre os aspectos técnicos. Seu contato é por meio do e-mail dpo@dentsul.com.br.

3.13. Do Controlador

1. A Cooperativa de Assistência Odontológica Vale do Caí - DENTSUL constitui a **Dra. Denise Giron como Controladora**, uma vez que possui maior cargo hierárquico na Cooperativa, além de deter conhecimento de todos os processos, procedimentos e normas de proteção aos dados da instituição. Seu contato é por meio do e-mail controlador@dentsul.com.br.

3.14. Dos dados para admissão no plano

1. Os documentos solicitados para cadastro dos usuários são cumprimento da RN 529 de 02/05/2022, da Agência Nacional de Saúde, que dispõe sobre a identificação de clientes e manutenção dos registros. São exigidos o nome do titular, seu CPF e RG, endereço completo, profissão e telefone. Registra-se que a “ficha de registro do empregado”, fornecida pelo contratante, é o documento que concentra todos estes dados, incluindo dados que não são de interesse e necessidade tanto pela Cooperativa quanto pela ANS e demais órgãos. Neste sentido, sugere-se que a ficha de registro do empregado seja entregue à Cooperativa sem dados sensíveis como salário – cobertos por tarja ou etiqueta. Ainda, de forma alternativa, sugere-se a realização de um documento conjunto entre a Cooperativa e a contratante, no qual constem exclusivamente os dados requisitados pela ANS e demais órgãos.