POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

UNIODONTO
PLANOS ODONTOLÓGICOS
AMAPÁ

SUMÁRIO

POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

UNIODONTO
PLANOS ODONTOLÓGICOS
AMAPÁ

1. INTRODUÇÃO

1.1. A ***UNIODONTO*** entende que os *dados corporativos*, *dados pessoais* e eventuais *dados sensíveis* coletados e gerenciados são bens de suma importância para o desempenho dos seus serviços pois é utilizado para manter qualidade e garantia dos produtos ofertados a seus clientes.

1.2. A ***UNIODONTO*** tem ciência que o tratamento de suas informações passa por diferentes etapas de coleta, armazenamento e comunicação, sendo estes passíveis de ameaças a fatores externos e internos que podem comprometer a segurança das informações corporativas.

1.3. Considerando tudo acima, a ***UNIODONTO*** estabelece sua *Política Geral de Segurança da Informação*, como parte integrante do seu sistema de gestão corporativo, alinhada às boas práticas e normas internacionalmente aceitas com o objetivo de garantir níveis adequados de proteção aos dados e informações sob sua responsabilidade, visando também sua adequação com a ***Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018***, a qual é a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet.

2. OBJETIVO

2.1. Esta política tem o objetivo de estabelecer diretrizes e normas de Segurança da Informação que permitam a todos os colaboradores da ***UNIODONTO*** adotar padrões de comportamento seguro, adequados às metas e necessidades da empresa;

2.2. O objetivo é garantir a **CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE** de todos os dados da empresa;

2.3. **Resguardar** as informações coletadas ou gerenciadas, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;

2.4. **Orientar** quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;

2.5. **Prevenir** possíveis causas de incidentes e responsabilidade legal da instituição e seus empregados, clientes e parceiros;

2.6. **Minimizar** os riscos de perdas financeiras, de participação no mercado, da credibilidade perante o mercado e seus clientes, ou de qualquer outro impacto negativo no negócio como resultado de falhas de segurança.

3. APLICABILIDADE

3.1. Esta política se aplica a todos os usuários da informação da ***UNIODONTO***, incluindo qualquer indivíduo ou organização que possui, ou possuiu vínculo com a empresa, tais como:

3.1.1. Empregados e ex-empregados;

3.1.2. Prestadores de serviço, ex-prestadores de serviço;

3.1.3. Colaboradores e ex-colaboradores;

3.1.4. Sócios e ex-sócios.

3.1.5. Todos aqueles que possuíram, possuem ou virão a possuir acesso às informações da ***UNIODONTO*** e/ou fizeram, fazem ou farão uso de recursos físicos e não computacionais (documentos físicos) e computacionais (dados eletrônicos), compreendidos na infraestrutura da empresa.

POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

UNIODONTO
PLANOS ODONTOLÓGICOS
AMAPÁ

4. DIRETRIZES

4.1. O objetivo da gestão de Segurança da Informação da ***UNIODONTO*** é tentar antecipar e minimizar riscos em todos os aspectos relacionados à segurança da informação, provendo formas de garantias e suportes ao cotidiano do negócio e minimizando riscos identificados e seus eventuais impactos na empresa.

5. NORMAS DE SEGURANÇA DA INFORMAÇÃO

5.1. **CLASSIFICAÇÃO/ROTULAGEM DA INFORMAÇÃO**: Para efeitos de classificação da informação, a empresa utiliza a categoria para todas as informações como:

5.1.1. INFORMAÇÃO INTERNA: A divulgação deste tipo de informação causa problemas para empresa ou a seus clientes.

5.1.2. INFORMAÇÃO CONFIDENCIAL: Informação de caráter sigiloso, que se for divulgada ou alterada pode gerar prejuízos para a empresa e/ou seus clientes. Devem ser guardados em locais seguros para impedir o acesso de pessoas não autorizadas, ou armazenados em ambientes com acesso controlado e senhas.

5.2. **CONFIDENCIALIDADE**: Em nenhuma hipótese o usuário poderá coletar, recepcionar, classificar, utilizar, acessar, reproduzir, transmitir, distribuir, processar, arquivar, armazenar, eliminar, avaliar, controlar, modificar, comunicar, transferir, divulgar DADOS PESSOAIS, DADOS SENSÍVEIS, DADOS CORPORATIVOS com TERCEIROS, fora do ambiente da empresa, fora dos limites contratualmente previstos, tanto no tocante à parte trabalhista para desempenho da função, quanto na parte comercial no tocante à prestação de serviços firmado com clientes.

5.2.1. O não cumprimento da confidencialidade pelo colaborador pode gerar **advertência**, **suspensão** ou até **demissão por justa causa**, dependendo da gravidade do descumprimento.

5.3. **DESCARTE DA INFORMAÇÃO**: O descarte da informação, quer seja física, quer seja eletrônica, deve ser realizado de forma a impedir a recuperação da mesma, independente do seu formato de armazenamento original;

5.4. **ACESSO À INFORMAÇÃO e SENHAS**: Os acessos são fornecidos exclusivamente para que os usuários possam executar suas atividades laborais.

5.4.1. Ao usuário/colaborador NÃO é permitido o acesso a qualquer informação/dado decorrentes de análise do banco de dados dos clientes da ***UNIODONTO, se limitando exclusivamente à verificação dos metadados e a funcionalidade do datacenter;***

5.4.2. Toda conta de acesso é pessoal do usuário a qual foi delegada e intransferível. Desta forma, o usuário é integralmente responsável por sua utilização, BEM COMO das senhas associadas às contas de acesso, também de uso pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo.

5.4.3. A equipe de tecnologia da informação será responsável por fornecer senhas de acesso inicial ao usuário, tanto ao login no aparelho que usar, quanto do e-mail, que deverá proceder com a troca imediata da mesma;

5.4.4. Haverá diferenciação entre os níveis de autorização de acesso ativos/serviços de informação com base em perfis que definem o nível de privilégio dos usuários, não podendo por exemplo o empregado ter o mesmo nível de senha do que um gestor.

5.5. **USO DE EQUIPAMENTOS**: Os equipamentos eletrônicos (computador, e-mail, pendrive, nuvem, token, etc) têm o objetivo específico de permitir aos usuários

desenvolverem suas atividades profissionais, sendo expressamente proibida a utilização para fins pessoais particulares e armazenamento de informações pessoais, devendo sempre utilizar a tela de bloqueio, ou log off, ou desligar a máquina quando se ausentar.

5.5.1. Em caso de qualquer necessidade de manutenção a equipe de T.I deverá ser acionada, especialmente em caso de suspeita de malwares, e outros vírus.

5.6. **E-MAIL**: O usuário é o responsável exclusivo pelo uso inadequado de sua conta no serviço de comunicação instantânea, sendo constantemente monitorado, tendo a ciência de que não é permitido o envio de mensagens:

5.6.1. De caráter pessoal ou para fins que não sejam decorrentes do desempenho das suas funções;

5.6.2. Enviar qualquer informação de propriedade dos clientes para pessoas ou entidades que não fazem parte do domínio corporativo;

5.7. **MONITORAMENTO:** Qualquer ativo/serviço de informação ou recurso computacional da empresa, poderá ser monitorado a qualquer momento. O monitoramento, sem expor dados pessoais, não constitui qualquer violação à intimidade, vida privada, honra ou imagem da pessoa monitorada, visando resguardar a segurança dos ativos de informações, bem como segurança jurídica da empresa e clientes, como eventuais dados pessoais, sensíveis ou não, de funcionários, e terceiros.

5.8. **AVISO LEGAL:** A empresa faz uso de um aviso legal para garantir que usuários e demais pessoas e entidades que tentem obter acesso a ativos/serviços de informação ou recursos computacionais da organização estejam cientes das regras de segurança.

5.9. **PROTEÇÃO CONTRA AMEAÇAS:** A empresa disponibiliza ferramentas para proteção dos seus ativos/serviços de informação e recursos computacionais, incluindo

estações de usuários, dispositivos móveis e servidores corporativos, contra ameaças e códigos maliciosos.

5.9.1. Em caso de infecção ou suspeita de infecção de código malicioso, a mesma deverá ser imediatamente isolada da rede corporativa, para evitar a transmissão da ameaça, e em ato contínuo a notificação imediata do setor de T.I sobre o ocorrido.

5.9.2. Mesmo com a existência de ferramentas para proteção contra códigos maliciosos, os usuários da empresa devem adotar um comportamento seguro e preventivo, reduzindo a probabilidade de infecção ou propagação de códigos maliciosos, encaminhando qualquer e-mail suspeito para o setor de T.I.

5.10. **TRATAMENTO DE INCIDENTES:** Todas as ocorrências que gerem violações da confidencialidade, integridade ou disponibilidade dos ativos/serviços de informação serão caracterizadas como um incidente de segurança da informação, devendo ser tratadas de maneira a minimizar qualquer tipo de impacto e recuperar as características de segurança da informação dos itens afetados.

5.10.1. Devem ser imediatamente comunicados ao sócio diretor e setor de T.I.;

5.10.2. Devem ser isolados do ambiente corporativo;

5.10.3. Deve ser feito uma análise do dano do incidente para, em seguida, identificar qual o melhor procedimento a ser adotado para sanar e restaurar totalmente os ativos de informação afetados;

5.10.4. Deve revisar a ocorrência para evitar a repetição do incidente.

6. CARGOS, FUNÇÕES E RESPONSABILIDADES

6.1. **COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO - CGSI**

6.1.1. Fica constituído o **COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO (CGSI)**, contando com a participação de, pelo menos, um representante da diretoria **Dr. CALANDRINI** e:

6.1.1.1. Encarregado de Proteção de Dados: **TATIARA**

6.1.1.2. Tecnologia da Informação: **ANDRÉ**

6.1.1.3. Segurança da Informação: **HELDECIR**

6.1.1.4. Jurídico: **ARTUR AZEVEDO**

6.1.2. É **RESPONSABILIDADE** DO CGSI:

6.1.2.1. Deliberar sobre a aprovação de políticas e normas relacionadas à segurança da informação, após análises e revisões;

6.1.2.2. Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;

6.1.2.3. Garantir que as atividades de segurança da informação sejam executadas em conformidade com a política de segurança de informação;

6.1.2.4. Promover a divulgação da política de segurança de informação e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente interno da empresa.

6.2. **SETOR DE SEGURANÇA DA INFORMAÇÃO**

6.2.1. É responsabilidade do *Setor de Segurança da Informação*:

6.2.1.1. Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções do comitê.

6.2.1.2. Propor ao comitê normas e procedimentos de segurança da informação, necessários para se fazer cumprir a política geral de segurança de informação;

6.2.1.3. Analisar as ameaças mais comuns à segurança da informação, bem como implantar medidas corretivas para reduzir o risco;

6.2.1.4. Tomar as ações cabíveis para se fazer cumprir os termos desta política;

6.2.1.5. Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

6.3. **RESPONSABILIDADE DOS GESTORES DA INFORMAÇÃO:**

6.3.1. Gerenciar as informações obtidas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte;

6.3.2. Classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados;

6.3.3. Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

6.3.3.1. Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pela ***UNIODONTO***.

6.3.3.2. **Confeccionar** o *Termo de Uso de Sistemas de Informação* ou *Termo de Ciência* da ***UNIODONTO,*** formalizando a ciência dos seus funcionários e demais pessoas envolvidas sobre o aceite integral das disposições da *Política Geral de Segurança da Informação,*

bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

6.4. USUÁRIOS DA INFORMAÇÃO

6.4.1. É responsabilidade dos *Usuários da Informação*:

6.4.1.1. **Ler**, **compreender** e **cumprir** integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

6.4.1.2. Em casos de dúvidas, solicitar esclarecimentos sobre a *Política Geral de Segurança da Informação*, suas normas e procedimentos a Gerência de Segurança da Informação ou, quando pertinente, ao Comitê Gestor de Segurança da Informação;

6.4.1.3. Comunicar à *Gerência de Segurança da Informação* qualquer evento que viole ou ponha em risco a segurança das informações ou dos recursos computacionais;

6.4.1.4. **ACEITAR E ASSINAR** o *Termo de Uso de Sistemas de Informação* ou *Termo de Ciência*, formalizando a ciência dos seus funcionários e demais pessoas envolvidas sobre o aceite integral das disposições da *Política Geral de Segurança da Informação*, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

6.4.1.5. Responder pela inobservância da Política Geral de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

7. SANÇÕES E PUNIÇÕES

POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

UNIODONTO
PLANOS ODONTOLÓGICOS
AMAPÁ

7.1. 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:

7.1.1. Advertência verbal,

7.1.2. Advertência por escrito,

7.1.3. Suspensão não remunerada e

7.1.4. Demissão por justa causa;

7.2. A aplicação de sanções e punições será realizada após a análise do incidente de segurança da informação, **devendo-se considerar, para fins de aplicação da punição, a gravidade da infração, efeito alcançado, recorrência** e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo aplicar a pena que entender cabível quando tipificada a falta grave, com o apoio do *CGSI* (comitê) pelo:

7.2.1. Síndico; ou

7.2.2. Gerente de Cada Área;

7.3. No caso de terceiros contratados ou prestadores de serviço, o *CGSI* (comitê) deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato;

7.4. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a ***UNIODONTO***, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes sem prejuízo aos termos descritos nos itens 6.1, 6.2 e 6.3 desta política.

POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

UNIODONTO
PLANOS ODONTOLÓGICOS
AMAPÁ

8. CASOS OMISSOS

8.1. Os casos não previstos serão avaliados pelo *Comitê Gestor de Segurança da Informação* para posterior deliberação.

8.2. As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças.

8.3. A ***UNIODONTO*** pretende sempre que possível, adotar outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção as informações da empresa e de seus clientes que estão sob sua posse.

9. REVISÕES

9.1. Esta política é revisada com periodicidade ANUAL.

9.2. A periodicidade será determinada conforme entendimento dos Sócios Diretor da Empresa, com auxílio, caso entendam necessário do *Comitê Gestor de Segurança da Informação*.

9.3. Poderão existir revisões extraordinárias decorrentes de fatores novos ocorridos.

10. GESTÃO DA POLÍTICA

10.1. A Política Geral de Segurança da Informação é analisada e aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria da ***UNIODONTO***.

10.2. A presente política foi aprovada no dia 24/10/2022

Presidente

POLÍTICA GERAL DE SEGURANÇA DA INFORMAÇÃO

UNIODONTO
PLANOS ODONTOLÓGICOS
AMAPÁ

Vice-presidente

Superintendente

REVISÕES

DATA DA REVISÃO	ITEM REVISADO	RESPONSÁVEL
07/07/2022	ITEM	HUGO FERREIRA