PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

LEI GERAL DE PROTEÇÃO DE DADOS

Lei nº 13.709/2018

Código:	
Versão:	0.1
Data da versão:	17/18/2021
Criado por:	Ricardo Monnazzi
Aprovado por:	Guilherme Galhardo Antonietto e Rafael Borim
Nível de confidencialidade:	Uso Interno

São José do Rio Preto – São Paulo

2021

Histórico de alteração

Data	Versão	Criado por	Descrição da alteração
17/08/2021	0.1	Ricardo Monnazzi, Guilherme Galhardo Antonietto e Rafael Borim.	Criar PSI

Índice

I - INTRODUÇÃO

UNIODONTO RIO PRETO. entende que as informações corporativas são um bem essencial para suas atividades, e, através deste documento, pretende definir a Política de Segurança da Informação (PSI) que rege as operações relativas a estes dados.

II - OBJETIVOS

Estabelecer os conceitos e diretrizes relativos à Segurança da Informação, visando proteger as informações da organização, mantendo tal política alinhada aos objetivos estratégicos da empresa. É objetivo dessa Política também:

Preservar as informações da UNIODONTO RIO PRETO quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

III - APLICAÇÕES DA PSI

Essa Política aplica-se a todos os colaboradores, estagiários, fornecedores, prestadores de serviço e visitantes das empresas da organização, incluídas as gerências de área e a alta direção da empresa.

Qualquer indivíduo ou empresa que tenha tido, tenha atualmente, ou venha a ter acesso

a qualquer dado ou ativo de informação, considerado de propriedade da organização, em qualquer tempo, em qualquer circunstância e em qualquer localização geográfica, estará sujeito ao determinado no presente documento.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador manter-se atualizado em relação a esta Política e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Sistemas sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

IV - PRINCÍPIOS DA PSI

Os regulamentos de segurança são políticas que uma instituição deve implementar em conformidade com legislação em vigor, garantindo aderência a padrões e procedimentos básicos de setores específicos.

Os padrões especificam o uso uniforme de determinadas tecnologias. Normalmente são mandatórios e implementados através de toda a instituição, a fim de proporcionar maiores benefícios.

Os fundamentos ou princípios são semelhantes aos padrões, com pequena diferença. Uma vez que um conjunto consistente de fundamentos seja definido, a arquitetura de segurança de uma instituição pode ser planejada e os padrões podem ser definidos. Os fundamentos devem levar em conta as diferenças entre as plataformas existentes, para garantir que a segurança seja implementada uniformemente em toda a instituição. Quando adotados, são mandatórios.

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela UNIODONTO RIO PRETO pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

A UNIODONTO RIO PRETO, por meio da Gerência de Tecnologia da Informação (TI), poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

V - REQUISITOS DA PSI

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da UNIODONTO RIO PRETO a fim de que a política seja cumprida dentro e fora da empresa.

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

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

Deverá constar em todos os contratos da UNIODONTO RIO PRETO o anexo de

Termo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um Código de Conduta.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao Encarregado de Proteção de Dados nomeado e ele, se julgar necessário, deverá encaminhar posteriormente ao Comitê de Segurança da Informação para análise.

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

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

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pela UNIODONTO RIO PRETO ou por terceiros. Os ambientes de produção

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

A UNIODONTO RIO PRETO exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta Política será implementada na UNIODONTO RIO PRETO por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

VI - DAS RESPONSABILIDADES ESPECÍFICAS

1 - Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à UNIODONTO RIO PRETO e/ou a terceiros, em decorrência da não

obediência às diretrizes e normas aqui referidas.

É dever ainda do colaborador:

- Ler, compreender, e cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação (PSI) da organização, como também, quaisquer outras leis e normas de segurança aplicáveis;
- Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a atual política, suas normas e procedimentos, ao Encarregado de Proteção de Dados nomeado;
- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela organização;
- Assegurar que os recursos tecnológicos, as informações e sistemas à sua disposição sejam utilizados apenas para as finalidades aprovadas pela organização;
- Cumprir as normas que regulamentam a propriedade intelectual;
- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou áreas expostas (automóveis, ônibus, restaurantes, encontros sociais) incluindo a emissão de comentários e opiniões em blogs, páginas e redes sociais;
- Não compartilhar informações confidenciais de qualquer tipo;
- Comunicar imediatamente ao Encarregado de Proteção de Dados qualquer descumprimento ou violação dessa política e/ou de suas Normas e Procedimentos, ou qualquer outro evento que coloque em risco a segurança das informações da organização.

2 - Dos Colaboradores em Regime de Exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pelo Comitê de Segurança da Informação.

A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

3 - Dos Gestores de Pessoas e/ou Processos

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.
- Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política da Segurança da Informação (PSI) da UNIODONTO RIO PRETO;
- Exigir dos colaboradores a assinatura do Código de Conduta, Termo de Confidencialidade, Normas Internas, além de todos os outros termos pertinentes à organização, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da UNIODONTO RIO PRETO;
- Antes de conceder acesso às informações da instituição, exigir a assinatura do Termo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais;
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI, bem como aos termos da Norma Educacional.

4 - Dos Custodiantes da Informação

4.1 - Da Gerência de Tecnologia da Informação

- Testar a eficácia dos controles utilizados e informar aos gestores e ao Encarregado de Proteção de Dados os riscos residuais.

- Acordar com os gestores e com o Encarregado de Proteção de Dados o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.
- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI, e em sua versão educacional, pelas Normas de Segurança da Informação complementares.
- Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido 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.
- Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Garantir segurança especial para sistemas com acesso público, incluindo o ambiente educacional, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a UNIODONTO RIO PRETO.
- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
- 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.

- Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.
- 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 empresa.
- Realizar auditorias semestrais de configurações técnicas e análise de riscos.
- Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.
- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.
- Monitorar o ambiente de TI, gerando indicadores e históricos de:
  - uso da capacidade instalada da rede e dos equipamentos;
  - tempo de resposta no acesso à internet e aos sistemas críticos da UNIODONTO RIO PRETO;
  - períodos de indisponibilidade no acesso à internet e aos sistemas críticos;
  - incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por

diante);

- atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

4.2 - Da Área de Segurança da Informação e Encarregado de Proteção de Dados

- Atuar como enlace fundamental entre Alta Direção da empresa e todas as outras gerências garantindo fluidez da comunicação entre as mesmas;
- Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
- Propor e apoiar iniciativas que visem à segurança dos ativos de informação da UNIODONTO RIO PRETO. Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação.
- Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da UNIODONTO RIO PRETO, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.
- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.
- Analisar criticamente incidentes em conjunto com o Comitê de Segurança da Informação.
- Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.
- Manter comunicação efetiva com o Comitê de Segurança da Informação sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a UNIODONTO RIO PRETO.
- Buscar alinhamento com as diretrizes corporativas da instituição.

4.3 - Do Comitê de Segurança da Informação

- Deve ser formalmente constituído por colaboradores com nível hierárquico mínimo regencial**,** nomeados para participar do grupo pelo período de um ano.
- A composição mínima deve incluir um colaborador de cada uma das áreas: Alta Direção, Jurídico, Recursos Humanos, Administrativo, Operacional e Encarregado de Proteção de Dados.
- Deverá o Comitê reunir-se formalmente pelo menos uma vez a cada três meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a UNIODONTO RIO PRETO.
- O Comitê poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.
- Cabe ao CSI:
    - propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
    - propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;
    - avaliar os incidentes de segurança e propor ações corretivas;
    - definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.

5 – Do Monitoramento e da Auditoria do Ambiente

Para garantir as regras mencionadas nesta PSI, bem como de sua versão educacional, a UNIODONTO RIO PRETO poderá:

- implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;
- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

VII - CORREIO ELETRÔNICO

O objetivo desta norma é informar aos colaboradores da UNIODONTO RIO PRETO quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico da UNIODONTO RIO PRETO é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a UNIODONTO RIO PRETO e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da UNIODONTO RIO PRETO:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a UNIODONTO RIO PRETO vulneráveis a ações civis ou criminais;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a

identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

- apagar mensagens pertinentes de correio eletrônico quando a UNIODONTO RIO PRETO estiver sujeita a algum tipo de investigação.
- produzir, transmitir ou divulgar mensagem que:
    - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da UNIODONTO RIO PRETO;
    - contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
    - 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;
    - vise obter acesso não autorizado a outro computador, servidor ou rede;
    - vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
    - vise burlar qualquer sistema de segurança;
    - vise vigiar secretamente ou assediar outro usuário;
    - vise acessar informações confidenciais sem explícita autorização do proprietário;
    - vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
    - inclua imagens criptografadas ou de qualquer forma mascaradas;
    - contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet).
    - tenha conteúdo considerado impróprio, obsceno ou ilegal;
    - seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
    - contenha perseguição preconceituosa baseada em sexo, orientação sexual, raça, incapacidade física ou mental ou outras situações protegidas;
    - tenha fins políticos locais ou do país (propaganda política);

- inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador;
- Gerência ou departamento;
- Nome da empresa;
- Telefone(s);
- Correio eletrônico

VIII - INTERNET

Todas as regras atuais da UNIODONTO RIO PRETO visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a UNIODONTO RIO PRETO, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, 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.

A UNIODONTO RIO PRETO, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao Encarregado de Proteção de Dados. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

Somente os colaboradores que estão devidamente autorizados a falar em nome da UNIODONTO RIO PRETO- para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades na UNIODONTO RIO PRETO.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela Gerência de Tecnologia da Informação.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da UNIODONTO RIO PRETO para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado à UNIODONTO RIO PRETO ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos da UNIODONTO RIO PRETO para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Porém, os serviços de comunicação instantânea (Signal) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente à Gerência de TI.

Não é permitido acesso a sites de proxy.

IX - IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante à UNIODONTO RIO PRETO e/ou terceiros.

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

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados na UNIODONTO RIO PRETO, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante à UNIODONTO RIO PRETO e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

O Departamento de Recursos Humanos da UNIODONTO RIO PRETO é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

A Gerência de Tecnologia da Informação responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

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.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 16 (dezesseis) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente. O uso deste perfil é exclusivo para atividades administrativas do ambiente, para demais atividades o usuário deve usar uma conta sem perfil administrativo, de forma separada.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a Gerência de TI da UNIODONTO RIO PRETO. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 45 (quarenta e cinco) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 30 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato à Gerência de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

X - COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade da UNIODONTO RIO PRETO, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Gerência de Sistemas da UNIODONTO RIO PRETO, ou de quem este determinar. As gerências que necessitarem fazer testes deverão solicitá-los previamente à Gerência de TI ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar imediatamente o Encarregado de Proteção de Dados.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da UNIODONTO RIO PRETO (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede ou nuvem. 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, sendo, portanto, de responsabilidade do próprio usuário.

Os colaboradores da UNIODONTO RIO PRETO e/ou 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 a autorização da Gerência de TI.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas, sendo elas:

- Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Gerência de TI da UNIODONTO RIO PRETO, que terá acesso a elas para manutenção dos equipamentos.
- Os colaboradores devem informar ao Encarregado de Proteção de Dados qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Gerência de TI da UNIODONTO RIO PRETO ou por terceiros devidamente contratados para o serviço.
- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e da área de informática.
- É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.
- O colaborador deverá manter a configuração do equipamento disponibilizado pela UNIODONTO RIO PRETO, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição,

assumindo a responsabilidade como custodiante de informações.

- Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.
- Caso o usuário se afaste provisoriamente de seu local de trabalho, não desejando desligar o equipamento, deverá ativar o bloqueio de tela protegido por senha.
- Todos os recursos tecnológicos adquiridos pela UNIODONTO RIO PRETO devem ter imediatamente suas senhas padrões (default) alteradas.
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da UNIODONTO RIO PRETO:

- 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.
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
- Usar qualquer tipo de recurso tecnológico para 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;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

Não é permitida ainda a conexão de equipamentos particulares na rede administrativa

da organização, seja em segmentos cabeados ou *wifi*, sem autorização formal e inspeção do equipamento pela Gerência de TI, sempre em observância aos pontos anteriores.

A seu critério exclusivo, a organização poderá permitir a utilização de equipamento particular para o desempenho de atividades profissionais, devendo os mesmos passar por inspeção de forma a garantir adequação aos requisitos e controles de segurança adotados pela empresa.

Em tal circunstância será emitida uma Autorização para Uso de Equipamento Particular, que deverá ser portada pelo usuário requerente;

O usuário requerente renuncia, no ato da solicitação para autorização de uso de tal equipamento, à sua privacidade, aceitando implícita e explicitamente que os dados e informações que trafeguem ou sejam armazenados por este equipamento estarão dentro da rede da organização, podendo ser auditado a qualquer momento, e cujos dados e informações podem ser entregues à autoridade policial ou judicial competente, caso solicitado, sem aviso prévio;

A instalação de ferramentas de proteção será exigida e realizada pela Gerência de TI, conforme critério definido pela mesma.

XI - DISPOSITIVOS MÓVEIS

A UNIODONTO RIO PRETO deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Gerência de TI, como: notebooks, smartphones e pendrives.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

A UNIODONTO RIO PRETO, na qualidade de proprietário dos equipamentos

fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O colaborador, portanto, 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 UNIODONTO RIO PRETO, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel vinculada com a conta disponibilizada pela área Gerência de TI. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não os carregar juntos.

O suporte técnico aos dispositivos móveis de propriedade da UNIODONTO RIO PRETO e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da Gerência de Sistemas.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da Gerência de Sistemas da UNIODONTO RIO PRETO.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel

fornecido pela UNIODONTO RIO PRETO, notificar imediatamente seu gestor direto e o Encarregado de Proteção de Dados. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à UNIODONTO RIO PRETO e/ou a terceiros.

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da UNIODONTO RIO PRETO deverá submeter previamente tais equipamentos ao processo de autorização da Gerência de TI.

A Gerência de TI manterá um registro de dispositivos e usuários autorizados.

XII - DATACENTER

O acesso ao Datacenter somente deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético entre outros.

Todo acesso ao Datacenter, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio.

Deverá ser executada semanalmente uma auditoria nos acessos ao Datacenter por meio do relatório do sistema de registro.

O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do coordenador de infraestrutura, de acordo com o Procedimento de Controle de Contas Administrativas.

A lista de funções com direito de acesso ao Datacenter deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Datacenter, e salva no diretório de rede.

Nas localidades em que não existam colaboradores da área de tecnologia da

informação, pessoas de outros departamentos deverão ser cadastradas no sistema de acesso para que possam exercer as atividades operacionais dentro do Datacenter, como: troca de fitas de backup, suporte em eventuais problemas, e assim por diante.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado.

Deverão existir duas cópias de chaves da porta do Datacenter. Uma das cópias ficará de posse do coordenador responsável pelo Datacenter, a outra, de posse do coordenador de infraestrutura.

O Datacenter deverá ser mantido limpo e organizado.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com a solicitação e autorização à Gerência de TI.

No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de colaboradores autorizados.

XIII - BACKUP

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas semestrais para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de backup devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Quaisquer atrasos na execução de backup ou restore deverão ser comunicados ao Encarregado de Proteção de Dados.

Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 60 dias, de acordo com a criticidade do backup.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo Encarregado de Proteção de Dados.

Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante as tarefas operacionais quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

XIV - DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da UNIODONTO RIO PRETO. Ou seja, qualquer incidente de segurança subentende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição. Essa Política

de Segurança da Informação foi aprovada pelo Comitê Gestor de Segurança da Informação no dia 03 de Agosto de 2021.

Comitê de Segurança da Informação

José Carlos Afonso Cuginotti– Diretor UNIODONTO RIO PRETO
Lilian Mara Secches Mansor – Diretora UNIODONTO RIO PRETO
Frederico Abdulmassih Espir – Diretor UNIODONTO RIO PRETO
Mileidi Haddad Monserrat - Cobaboradora – UNIODONTO RIO PRETO

Marcelo Gomes Miguel

Jurídico – UNIODONTO RIO PRETO

ANEXT

Gerência de TI

Recursos Humanos

MILEIDI

Operacional / Comercial

ANEXT

Encarregado de Proteção de Dados