POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Nome do documento: **Política de Segurança da Informação**			
Tipo de documento: **Política**	Divulgação: **Interno**	Aprovado em:	Versão: **20230330**

1. Objetivo

1.1 Esta Política de Segurança da Informação ("**Política**") tem como objetivo informar as diretrizes corporativas de segurança, privacidade e tratamento de dados da Unio Soluções em Tecnologia Ltda. ("**UNIO**"), e seus respectivos procedimentos com vista à proteção das informações em seus diversos meios, estando assim em conformidade com o Programa de Integridade (Programa de *Compliance*), às normas da Lei Geral de Proteção de Dados (LGPD) e preservando os princípios básicos da **Política**, quais sejam, Integridade, Confidencialidade e Disponibilidade.

1.2 A Segurança da Informação é entendida pela **UNIO** como parte da cultura da empresa como a simplicidade, a excelência e a ética, portanto, incidentes de vazamento de informação são entendidos como ações que vão contra a cultura corporativa da **UNIO**.

2. Aplicação

2.1 Esta **Política** se aplica à **UNIO** e todos seus Colaboradores, incluindo Alta Administração (Diretores e membros do Conselho de Administração) e, em sua medida, a clientes, fornecedores e prestadores de serviço e quaisquer parceiros, tem abrangência sobre todo e qualquer conteúdo e dados produzidos, armazenados, processados ou tratados por eles no exercício de sua função em meio digital ou físico, e sendo, portanto, consideradas informações de titularidade da **UNIO**.

2.2 Esta **Política** deve ser aplicada em conjunto com o Código de Ética e Conduta e suas demais políticas, que integram o Programa de Integridade da **UNIO**, dá ciência a todos, de que os locais físicos, ambientes em nuvem, computadores, redes da **UNIO** e sistemas poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras. É obrigação de cada um manter-se atualizado em relação a esta **Política** e aos procedimentos, guias e normas relacionadas, buscando orientação de sua gerência sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

2.3 Todos os projetos desenvolvidos pelos Colaboradores, Parceiros da **UNIO** deverão, a partir da formulação desse documento, observar as diretrizes e princípios estabelecidos nele, e os sistemas desenvolvidos e projetos em andamento, revisados a fim de garantir a aplicação adequada dos princípios aqui estabelecidos.

3. Definições

3.1 As seguintes definições devem ser aplicadas quando da interpretação desta **Política**:

a. **Alta Administração:** Diretores, Conselho de Administração, Comitê de Ética e *Compliance*;
b. **Colaboradores:** Toda e qualquer pessoa física, contratada CLT ou prestadora de serviço, permanente ou temporário, que exerça atividade dentro ou fora da **UNIO**;
c. **Parceiros:** Toda pessoa física ou jurídica que tenha firmado contrato de colaboração empresarial com a **UNIO**, mesmo que não oneroso e que de alguma forma sua atividade se relacione com o nome e a imagem da **UNIO**;
d. **Equipe de Operação:** Corpo técnico e gerencial com atribuição de gerir o sistema de segurança de informação no âmbito da organização;
e. **Comitê de Segurança da Informação:** Grupo de pessoas das áreas finalísticas com a responsabilidade de assessorar a implementação das ações de Segurança da Informação no âmbito da organização;
f. **Dados Pessoais:** qualquer informação de uma pessoa física viva identificável ou identificada;
g. **Confidencialidade:** Garantia que a informação seja acessível apenas àqueles autorizados a ter acesso a ela, ou seja, se há um acesso não autorizado de uma informação confidencial, seja ele intencional ou não, ocorre uma quebra da confidencialidade;
h. **Integridade:** Garantir que a informação disponível é confiável, correta e em formato compatível com a sua utilização, ou seja, íntegra;
i. **Disponibilidade:** Garantia que o usuário tenha acesso à informação quando necessário;
j. **Encarregado de Dados ou *Data Protection Officer* (DPO):** responsável pela implementação da Lei Geral de Proteção de Dados;
j. **Incidente de Segurança da Informação:** evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades e que afete algum dos aspectos da Segurança da Informação: confidencialidade, integridade ou disponibilidade;
k. **Programa de Integridade (Programa de *Compliance*):** Conjunto de medidas estabelecidas pela **UNIO** visando garantir a integridade em suas atividades perante a Administração Pública e cumprir as exigências da Lei 12.846/13;
l. **Informação Confidencial**: Alto nível de confidencialidade. São aquelas que, se divulgadas interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem da **UNIO**. São protegidas, por exemplo, por criptografia;
m. **Informação Restrita**: Médio nível de confidencialidade. São informações estratégicas que devem estar disponíveis apenas para grupos restritos de Colaboradores. Podem ser protegidas, por exemplo, restringindo o acesso à uma pasta ou diretório da rede;
n. **Informação Uso Interno**: Baixo nível de confidencialidade. São aquelas que não podem ser divulgadas para pessoas de fora da organização, mas que, caso isso aconteça, não causarão grandes prejuízos. A preocupação nesse nível está relacionada principalmente à integridade da informação;
o. **Informação Pública**: Todos podem ter acesso. São dados que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público. No entanto, sempre cabe lembrar dos outros dois pilares: a disponibilidade e a integridade.

4. Princípios

4.1 A informação é, para o mundo corporativo, patrimônio de valor incomensurável, e por isso, uma boa gestão desse ativo é muito importante para o sucesso de uma empresa, tornando imprescindível, uma boa Política de Segurança da Informação a fim de alcançá-lo. A **UNIO**, que tem por princípio a excelência e a simplicidade na criação, implantação e operação de soluções de sistemas para o segmento de saúde suplementar vê a matéria como fundamental, e trata a segurança como parte de sua cultura corporativa.

4.2 A **Política**, é o documento que estabelece as instruções e procedimentos, que visam estabelecer as diretrizes corporativas da **UNIO** para a proteção da informação. Deve, portanto, ser aplicada e cumprida por todos os Colaboradores e Parceiros, incluindo trabalhos executados externamente que utilizem o ambiente de processamento da **UNIO**, ou tenham acesso às informações pertencentes a **UNIO**.

4.3 A presente **Política** está em acordo as boas práticas de Governança e Gestão de Tecnologia da Informação, as normas internacionais padronizadas para Sistemas de Gestão de Segurança da Informação e as leis voltadas para a Proteção de Dados Pessoais, internacionalmente reconhecida como guia para a gestão da Segurança da Informação, visando atingir os objetivos elencados acima.

4.4 A **UNIO** poderá monitorar o acesso e a utilização das informações e dos sistemas e serviços internos, inclusive por meio de vídeo, visando garantir a Confidencialidade, a Disponibilidade e a Integridade das informações não utilizadas.

5. Responsabilidades

5.1 Da Alta Administração, dos Colaboradores e Parceiros:

a. Todos devem conhecer integralmente esta **Política** e zelar pelo seu cumprimento, responsabilizando-se por todo dano ou prejuízo sofrido ou causado à **UNIO** e/ou terceiros, em decorrência do não cumprimento das instruções e normas aqui referidas;
b. Alguns Colaboradores podem, por característica de sua função, acessar os arquivos e dados de outros Colaboradores. No entanto, isso só será legítimo quando for necessário para a execução das atividades sob sua responsabilidade ou com autorização expressa para fazê-lo;
c. Fiscalizar e informar qualquer violação ou supeita a esta **Política**, informar situações que comprometam a Segurança da Informação da **UNIO**, seja dentro ou fora do local de trabalho, através do Canal de Integridade ou outro meio, sempre com maior brevidade possível;
d. Ter conhecimento e cumprir as normas e orientações estabelecidas nesta **Política**, no Código de Ética de Conduta e demais Políticas da **UNIO**.

5.2 Dos Colaboradores e Parceiros:

a. Todos devem conhecer integralmente este documento e zelar pelo seu cumprimento, responsabilizando-se por todo dano ou prejuízo sofrido ou causado à **UNIO** e/ou terceiros, em decorrência do não cumprimento das instruções e normas aqui referidas;

5.3 Da Alta Administração:

a. É compromisso constante da Alta Administração empenhar todos os esforços a fim de garantir o pleno cumprimento das regras desta **Política** e sua permanente atualização, liberando recursos, humanos e financeiros, aplicando sanções, entendendo ser esta **Política** um ativo estratégico para a **UNIO** motivando a cada Colaborador e Parceiro a conhecê-la e cumprí-la;
b. Ter postura exemplar em relação à Segurança da Informação, servindo como modelo de conduta para todos os Colaboradores, Parceiros e terceiros da **UNIO.**

5.4 Dos Gestores de Pessoas e/ou Processos:

a. Ter uma postura exemplar em relação à Segurança da Informação, sendo modelo para os Colaboradores e Parceiros sob sua gestão;
b. Definir em conjunto com a equipe de operação os níveis de controle necessários à proteção dos recursos de tecnologia da informação sob sua responsabilidade;
c. Conferir aos Colaboradores, em fase de contratação ou formalização de parceria, a responsabilidade ao cumprimento desta **Política**, exigindo deles a assinatura de Termo de Compromisso e Ciência, que formaliza o dever de seguir as instruções e normas estabelecidas, bem como o compromisso de manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da **UNIO**;
d. Adaptar normas, procedimentos, processos e sistemas sob sua responsabilidade para atender a esta **Política** e legislação vigente a respeito da Segurança da Informação.

5.5 Dos Custodiantes da Informação:

5.5.1. Da Equipe de Operação:

a. Configurar os equipamentos, ferramentas e sistemas da **UNIO** para atender os controles necessários para cumprir os requerimentos de segurança estabelecidos nesta **Política** e pelos procedimentos de Segurança da Informação complementares a **Política**;
b. Definir regras para instalação de *software* e *hardware*;
c. Monitorar os acessos às informações e aos ativos de tecnologia (sistema, bancos de dados, recursos de rede), tendo como referente a **Política**;
d. Implementar ferramentas e melhores práticas que garantam a Segurança da Informação e proteção de dados;
e. Gerar e manter as trilhas para auditoria com nível de detalhes suficiente para rastrear possíveis falhas e/ou fraudes;
f. Manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando, sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações;
g. Proteger, administrar e testar cópias de segurança dos sistemas e dados sob a tutela da **UNIO**;
h. Manter o Comitê de Segurança da Informação informado sobre Incidentes de Segurança;
i. Realizar auditorias técnicas e análise de riscos periodicamente;
j. Responsabilizar-se pelo uso, manuseio, guarda dos certificados digitais.

5.5.2. Do Comitê de Segurança da Informação:

a. Composto por membros permanentes das áreas de tecnologia, mercado, administrativo e o DPO, devendo reportar à Alta Administração;

b. Reunir-se ordinariamente 1 (uma) vez a cada 6 (seis) meses, realizando reuniões extraordinárias sempre que necessário, especialmente para deliberações em casos de incidentes graves;
c. Gerenciar, orientar a Alta Administração e todos os Colaboradores, Parceiros, promovendo ações e projetos, de interesse da **UNIO**, tanto para conscietização desta **Política**, quanto para a relevância da Segurança da Informação para o negócio da **UNIO**, mediante campanhas, treinamentos, palestras, etc.;
d. Editar esta **Política** e demais procedimentos de Segurança da Informação, quando necessário;
e. Propor metodologias e os processos específicos para a Segurança da Informação, colaborando com a Equipe de Operação, com medidas de segurança para ameaças e vulnerabilidades identificadas;
f. Propor investimentos relacionados à Segurança da Informação com o intuito de minimizar riscos;
g. Propor e apoiar iniciativas que visem a segurança dos ativos de informação;
h. Classificar os níveis de acesso, sempre que necessário;
i. Avaliar Incidentes de Segurança e propor ações corretivas e, analisar criticamente em conjunto com a Alta Administração;
j. O Comitê poderá utilizar-se de especialistas, internos ou externos, para apoiar em assuntos que exijam conhecimentos técnico específico.

6. Acessos e utilização

6.1 O uso responsável e correto dos recursos de tecnologia da informação se aplica a todos os Colaboradores e Parceiros que utilizam a infraestrutura e demais recursos da **UNIO**.

6.2 Somente atividades éticas, lícitas e administrativamente admitidas devem ser realizadas, por todos no âmbito da infraestrutura de TI, ficando os transgressores sujeitos à Lei Penal, Civil e Administrativa, na medida da conduta, dolosa ou culposa, que praticarem.

6.3 As informações pertencentes à **UNIO** devem ser usadas para, e somente para, os propósitos definidos em sua missão.

6.4 Os *softwares* deverão ser utilizados sem violação dos direitos de propriedade intelectual, bem como é vedada a utilização de marcas, patentes, nomes, domínios, ou qualquer outro material que não tenha sido obtida a expressa autorização do proprietário dos direitos.

6.5 Recomendações e práticas para uso seguro dos recursos de TI:

6.5.1. Quanto a senha:

a. Ao criar senhas evitar o uso de nome, sobrenome, placas de carros, telefone, data de nascimento ou casamento, ou números de documentos ou qualquer outro termo que possa ser facilmente descoberto ou que identifique o usuário;
b. Alterar suas senhas periodicamente;
c. Ao alterar a senha evitar o uso da senha anterior (senhas de acesso cíclicas), utilizar novas senhas, reduzindo o impacto de um possível vazamento da senha;
d. Buscar escolher senhas de fácil memorização, e ao mesmo tempo difíceis de serem previstas por outras pessoas.

6.5.2. Quanto ao acesso à *internet*:

a. Analisar a procedência dos *sites* e a utilização de criptografia (conexão segura) ao realizar transações via *web*;
b. Conferir se o certificado do *site* que deseja acessar, está ativo, dentro do prazo de validade e se corresponde a ele mesmo;
c. Certificar que o endereço apresentado no navegador é do *site* que quer acessar, antes de realizar qualquer transação;
d. Priorizar a digitação do endereço no navegador a utilizar *links* como recurso para acessar um endereço;
e. Omitir-se em utilizar o acesso da *internet* para a prática de atividades particulares não ligadas ao trabalho que lhe foi atribuído.

6.5.3. Quanto aos arquivos:

a. Não guardar documentos com dados pessoais de terceiros em disco local. Utilizar o *Sharepoint* disponibilizado pela **UNIO** para esse fim, e ainda, não armazenar no diretório pessoal e sim no corporativo;
b. Utilizar criptografia sempre que enviar ou receber dados com informações sensíveis. Optar por compartilhar o arquivo em seu disco virtual, ao invés de mandá-lo por *e-mail*, ou em um *pendrive*, por exemplo;
c. Não executar programas, ou abrir arquivos anexados a *e-mails* sem antes verificá-los com um antivírus;
d. Não utilizar de executáveis em arquivos compactados, pois são propensos à propagação de vírus;
e. Guardar em segurança, em local adequado, os arquivos em meio físico que detenham por conta da atividade que estejam executando, evitando o acesso de pessoas não autorizadas.

6.5.4. Recomendações sobre atividades permitidas:

a. Criar, distribuir, disponibilizar, armazenar ou transmitir documentos, desde que respeite às leis e regulamentações, em especial àquelas que se referem aos crimes informáticos e a pornografia envolvendo crianças, presando pela decência, ética e honra à imagem de pessoas ou empresas, a vida privada e a intimidade;
b. Fazer cópia de documentos e ou programas de computador a fim de salvaguardá-los, respeitando a legislação que rege a salvaguarda de dados, informações, documentos e materiais sigilosos;
c. Ao desenvolver, respeite as diretrizes de segurança presentes no *green book* de arquitetura nas várias camadas da aplicação, repositório de dados, *backend*, *frontend*, *webjobs*, etc.

6.5.5. Recomendações sobre atividades **não** permitidas:

a. Introduzir código malicioso nos sistemas;
b. Compartilhar ou divulgar códigos de autenticação, identificação e autorização de uso pessoal (conta, senhas, chaves de integração, etc.), ou permitir a terceiros o uso de recursos que são autorizados por intermédio desses códigos utilizando a sua conta;
c. Tentar interferir em um sistema ou serviço sem autorização expressa, desativá-lo, sobrecarregá-lo, ou ainda, cooperar com ataques de negação de serviços internos ou externos;
d. Alterar registro de evento dos sistemas;
e. Obter acesso a sistemas, a dados, ou redes indevidamente, ou sem autorização;
f. Interceptar ou monitorar o tráfego de dados nos sistemas, sem a autorização;

g. Violar medida de segurança, sem autorização de autoridade competente;
h. Fornecer informações a terceiros, de pessoas física ou jurídica, ou serviços disponíveis nos sistemas da **UNIO**, ou presentes em dados referentes a suporte técnico, em especial àqueles classificados como sensíveis pela legislação (dado referente à saúde ou à vida sexual, dado genético ou biométrico e informações de crianças e adolescentes, além de origem étnica, convicção religiosa, opinião política, filiação a sindicato, organização de caráter religioso, filosófico ou político), exceto mediante autorização expressa.

6.6 Recomendações específicas:

6.6.1. Utilização de *e-mail*:

a. É vedado o acesso às caixas postais de terceiros sem autorização expressa;
b. É vedado o envio de informações estratégicas, críticas ou sensíveis para organizações, ou pessoas não autorizadas;
c. É vedado o envio de material obsceno, não ético, ilegal, mensagem do tipo corrente e de entretenimento, relacionadas com convicção política, raça ou nacionalidade, religião, orientação sexual, ou qualquer outro assunto que possa difamar a qualquer pessoa;
d. É vedada a participação em listas de discussão, utilizando o correio eletrônico corporativo, exceto para assuntos relacionados às atividades da **UNIO**;
e. O uso do correio eletrônico deve sempre ser baseado no bom senso e de acordo com os preceitos legais.

6.6.2. Controle de acesso:

a. O acesso às informações restritas será permitido quando houver uma necessidade e tal acesso for aprovado pela equipe responsável pelo dado. Da mesma forma, o acesso a servidores e outros ativos do ecossistema virtual;
b. O processo de liberação de acesso a dados, sistemas e *hardwares* considerados restritos deve ser registrado e ter prazo de revogação definido;
c. O acesso aos serviços inerentes ao trabalho de todos os colaboradores, como correio eletrônico, *browser*, *Microsoft Office*, *Sharepoint*, disco virtual, entre outros, será dado a todos os usuários;
d. O acesso a outras ferramentas, como por exemplo o *Azure DevOps*, usado pela equipe de operação, analistas, desenvolvedores e *stakeholders*, será concedida de acordo com a função desempenhada. No caso de dúvidas sobre o acesso aos sistemas, essas perguntas devem ser direcionadas ao líder de equipe ou líder da equipe de operação;
e. As solicitações de acesso para os novos usuários e eventuais alterações de privilégios, devem ser enviadas por meio do formulário de automação ou da ferramenta de abertura de chamado, e aprovadas pelo líder da equipe que o recurso está alocado. O pedido deve deixar claro, o motivo pelo qual é necessário ter acesso e por qual período esse acesso se faz necessário;
f. Recursos alocados em projeto, devem ter seus privilégios revogados imediatamente em caso de desligamento antecipado, ou quando da finalização do contrato (cliente) e/ou do projeto;
g. Os privilégios para todos os usuários da **UNIO** deverão ser revisados periodicamente;
h. Todos os usuários (Colaboradores e Parceiros) que utilizam os recursos de tecnologia da **UNIO** devem assinar o Termo de Confidencialidade antes da criação de sua identificação de usuário. Casos em que o usuário já possuía acesso, antes da instauração dessa norma, a assinatura do termo deve ser obtida em caráter de urgência. O termo assinado aponta que o usuário entende e concorda com as políticas, normas,

procedimentos e padrões, bem como entende as implicações legais decorrentes do não cumprimento do disposto no termo.

6.6.3. Ambiente de trabalho:

a. Nenhum dado pessoal, ou informação confidencial deve ser deixada sobre a mesa, à vista, seja em papel ou em um dispositivo eletrônicos, ou outro meio;
b. Ao deixar sua estação de trabalho o computador deve ser bloqueado, evitando a exposição dos dados na tela;
c. Ao imprimir esse tipo de informação na impressora coletiva, a cópia deve ser recolhida imediatamente, evitando a exposição do dado.

6.6.4. Computadores e sistemas:

a. Os equipamentos disponíveis aos Colaboradores são de propriedade da **UNIO**, cabendo a cada um utilizá-los de modo correto para as atividades de interesse da empresa, cumprindo as recomendações fornecidas por esse documento e pelas gerências responsáveis;
b. É proibido todo procedimento de manutenção física, sem autorização expressa;
c. Os equipamentos fornecidos pela **UNIO** deverão ser utilizados de modo seguro, preservando sua integridade e segurança.

6.7 Recomendações sobre os ativos de informação:

6.7.1. Quanto ao manuseio:

a. Todos ativos devem ser protegidos, cuidados e gerenciados adequadamente com o objetivo de garantir a sua disponibilidade, integridade e confidencialidade, independentemente do meio de armazenamento, processamento ou transmissão que esteja sendo utilizado;
b. Toda informação de responsabilidade das nossas equipes deve ser protegida para que não seja alterada, acessada e destruída indevidamente;
c. Termos de Compromisso específicos para os nossos Colaboradores e Parceiros, que devem ser assinados ao iniciarem a sua atuação na empresa, com restrições relacionadas à cópia e à divulgação de informações sendo monitorados durante a vigência do respectivo vínculo com a empresa;
d. Todos os Colaboradores e Parceiros da **UNIO** que manuseiam dados sensíveis de outros Colaboradores ou clientes devem ser treinados de acordo com os procedimentos de Segurança da Informação, presentes nesse documento, e instruções complementares de sua área de atuação;
e. Todos os Colaboradores e Parceiros que desejam acessar informações que não sejam pertinentes ao seu acesso e/ou função desempenhada na **UNIO**, devem solicitar via *e-mail* ao líder de equipe ou ao líder de operação, detalhando a justificativa para o acesso à essas informações.

6.7.2. Quanto ao monitoramento:

a. Todo o uso das informações geradas, armazenadas ou veiculadas na **UNIO** pode ser monitorado e registrado. Dado isto, os usuários dos ativos de tecnologia da informação da **UNIO** não devem ter qualquer expectativa de privacidade com relação à utilização que fizerem dos respectivos ativos, utilização esta que pode ser monitorada a qualquer momento sem aviso prévio;
b. Todo ativo de informação deve ser armazenado no seu respectivo repositório, *Sharepoint* ou *Azure Devops*, garantido o monitoramento, proteção e auditoria.

6.7.3. Quanto ao descarte:

a. As informações, quando perderem sua utilidade ou valor, devem ser eliminadas de maneira adequada;
b. Os documentos impressos que contenham informações sensíveis devem ser fragmentados impossibilitando a sua leitura;
c. Os discos e/ou outras mídias de armazenamento digital de dados devem ser entregues ao líder da operação para serem examinados antes do descarte, para assegurar que todos os dados sensíveis e *softwares* licenciados tenham sido removidos ou sobrescritos com segurança;
d. Os dispositivos que contêm informações confidenciais devem ser fisicamente destruídos ou as informações devem ser destruídas, excluídas ou substituídas usando técnicas para tornar as informações originais não recuperáveis em vez de usar a função excluir ou formatar padrão;
e. Todos os documentos que contenham dados pessoais, independente da forma de armazenamento, precisam ser deletados ou destruídos depois de atingirem sua finalidade e tempo de retenção previsto para cada um, mantendo um cuidado extra com documentos ou bancos de dados que contenham dados pessoais sensíveis;
f. As mídias de armazenamento devem ser descartadas de forma adequada, conforme os requisitos e melhores práticas de Segurança da Informação;
g. Para toda e qualquer informação sensível somente é considerado o descarte de forma segura e irreversível, eliminando todo o conteúdo de mídias e recursos tecnológicos;
h. Toda informação produzida ou recebida pelos Colaboradores e Parceiros da **UNIO** em razão de sua atividade contratada, pertencem à **UNIO**, assim o processo de descarte se aplica a todos os custodiantes de informações.

6.7.4. Notificação de coleta de dados pessoais:

a. A **UNIO** deve fornecer uma notificação adequada aos titulares dos dados quando a informação pessoal é recolhida, por exemplo, na contratação de novos Colaboradores;
b. O aviso fornecerá informações completas, conforme seja razoável nas circunstâncias, para informar um indivíduo sobre como suas informações pessoais serão usadas para que o uso da **UNIO** seja dentro das finalidades informadas pelo titular, necessário à execução dos processos do negócio.

6.7.5. Processo de gestão de consentimento:

a. O consentimento deve ser obtido dos titulares dos dados no momento do recolhimento de informações pessoais, antes de suas informações pessoais serem utilizadas e/ou transferidas para, ou de, seus sistemas de processamento de informações. Além disso, será obtido de forma explícita para a coleta, uso e divulgação de informações pessoais confidenciais, a menos que uma lei ou regulamento especificamente exija ou permita de outra forma;
b. O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico, dado por pelo menos um dos pais ou pelo responsável legal;
c. A coleta de informações pessoais de crianças sem o consentimento de um dos pais ou do responsável legal somente poderá ocorrer quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem o armazenamento, ou para sua proteção e em nenhum caso poderão ser repassados para terceiros sem o consentimento dos pais ou responsável legal.

6.7.6. Limitação de uso, divulgação e retenção de dados:

a. As informações pessoais não devem ser usadas ou divulgadas para fins diferentes daqueles para os quais foram coletadas, exceto com o consentimento do indivíduo ou conforme exigido por lei;
b. A retenção de informações pessoais será apenas durante o tempo necessário para cumprir os fins comerciais e legais identificados;
c. Após o término dos objetivos legítimos identificados ou da retirada do consentimento, a **UNIO** deve apagar ou anonimizar com segurança as informações pessoais dos titulares de dados. Os dados são anonimizados para impedir a identificação exclusiva de um indivíduo e por isso, não serão considerados dados pessoais, salvo quando o processo de anonimização puder ser revertido, com esforços razoáveis.

6.7.7. Criptografia

O uso efetivo e adequado de sistemas de criptografia deve ser estabelecido com o intuito de se assegurar a proteção da confidencialidade, autenticidade e integridade das informações, conforme nuvem de sistemas da *Microsoft 365* (para Skype for Business, OneDrive for Business, SharePoint Online, *Microsoft Teams* e *Exchange*).

7. Avaliação e gerenciamento de riscos e incidentes

7.1 Riscos internos de Segurança da Informação:

7.1.1. Os riscos de Segurança da Informação devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os processos nos aspectos da Segurança da Informação (Confidencialidade, Integridade e Disponibilidade);

7.1.2. Todos os riscos no que tange a Segurança das Informações da **UNIO** devem ser reportados para o Comitê de Segurança da Informação, para que eles sejam analisados, avaliados e tratados de acordo com os critérios e diretrizes estabelecidas com a metodologia de riscos cibernéticos escolhida pela Alta Administração.

7.2 Parceiros:

7.2.1. Os riscos de Segurança da Informação devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os processos nos aspectos da Segurança da Informação (Confidencialidade, Integridade e Disponibilidade);

7.2.2. Todos os riscos no que tange a Segurança das Informações da **UNIO** devem ser reportados para o Comitê de Segurança da Informação, para que eles sejam analisados, avaliados e tratados de acordo com os critérios e diretrizes estabelecidas com a metodologia de riscos cibernéticos escolhida pela Alta Administração.

7.3 Gestão de incidentes:

7.3.1 Todos os usuários (Colaboradores e Parceiros) devem relatar eventos que possam comprometer a Confidencialidade, Integridade e Disponibilidade das informações, tanto quando se tratar de eventos relacionados a tecnologia, como questões jurídicas ou qualquer outra demanda, logo que tenham conhecimento, enviando e-mail para o encarregado de dados (D.P.O).

7.3.2 Incidentes graves, onde haja a necessidade de se manter anonimidade, que estejam vinculados à descumprimento de leis, normas ou relacionadas a condutas antiéticas devem ter o seu registro realizado através do Canal de Integridade da **UNIO**.

7.3.3 Nenhum usuário deverá tomar ação própria sobre os eventos de Segurança da Informação sem o conhecimento do Comitê de Segurança da Informação.

7.4 Backup:

7.4.1 Como os recursos computacionais da **UNIO** são integralmente hospedados em nuvem, o serviço de *backup* do *Microsoft Azure* e *Amazon Web Services* (AWS) fornecem soluções simples, seguras e para fazer *backup* de seus dados e recuperá-los da nuvem do *Microsoft Azure* e da *Amazon Web Services* (AWS), e a empresa utiliza as ferramentas conforme recomendação da *Microsoft* e da *Amazon.com*, garantindo a segurança e privacidade da informação.

8. Canais de contato

8.1 A **UNIO** conta com canais de contato para reportar o não cumprimento dessa **Política**, irregularidades na sua aplicação, ou quaisquer outros desvios de conduta disponíveis da seguinte forma:

a. Canal de Integridade, disponível atráves do link: aloetica.com.br/uniodigital.
b. E-mail: aloetica.com.br/uniodigital
c. Telefone: 0800 67 26 867

8.2 Em todos os canais de contato disponíveis, o manifestante poderá se identificar ou efetuar relato anônimo. Ressalta-se que sigilo e a confidencialidade serão garantidos e não haverá qualquer retaliação ao denunciante de boa-fé.

9. Penalidades

9.1 Configura infração grave a transgressão às disposições contidas nesta **Política**.

9.2 Sem prejuízo das demais penalidades previstas na legislação e regulamentação aplicável, em caso de infração às disposições previstas nesta **Política** o infrator ficará sujeito a sanções de acordo com as normas internas da **UNIO**.

10. Vigência

10.1 Esta **Política** entra em vigor na data de sua aprovação, vigorando por prazo indeterminado, enquanto não alterada por nova deliberação do Comitê de Segurança da Informação da **UNIO.**