Declaração de Privacidade e Segurança para Terceiros

AILOS
SISTEMA DE COOPERATIVAS

Publicado em 08/2023

Nesse documento você encontrará informações sobre:

Se preferir buscar alguma informação específica, utilize o atalho de busca apertando CTRL+F no teclado e digitando a palavra de interesse. Para acessar os títulos, basta clicar no número da página.

Declaração de Privacidade e Segurança para Terceiros

AILOS
SISTEMA DE COOPERATIVAS

1 Objetivos?

Este documento tem por objetivo estabelecer as principais diretrizes e controles de Segurança da Informação, Segurança Cibernética e Privacidade e Proteção de Dados Pessoais a serem implementados pelos fornecedores e parceiros da Cooperativa e suas Filiadas para o correto acesso e manuseio de informações de forma a assegurar a confidencialidade, integridade e disponibilidade destas em seu ambiente físico e lógico durante o manuseio das informações que são processadas por prestadores de serviços.

Nota: É importante observar que, o estabelecimento de diretrizes e controles na relação com os fornecedores e parceiros da Cooperativa e Filiadas, não se limita a esta esse documento, podendo ser definidos novos itens e a revisão destes ao longo de toda a relação contratual.

Nota: Os requisitos neste documento apresentados poderão ser utilizados como critérios para aprovação de contratação de terceiro.

2 Abrangência?

Aplica-se a todos os fornecedores e parceiros da Central Ailos e suas afiliadas.

3 Referências?

ABNT NBR ISO/IEC 27001
ABNT NBR ISO/IEC 27002
ABNT NBR ISO/IEC 27701
Política de Segurança da Informação do Sistema Ailos
Política Cibernética do Sistema Ailos
Resolução CMN nº 4.893, de 26 de Fevereiro de 2021
Lei nº 13.709/2018 Lei Geral de Proteção de Dados Pessoais

4 Diretrizes?

Todo fornecedor ou parceiro deve ter o conhecimento e ser capaz de demonstrar aderência a esta declaração e suas diretrizes, e dessa forma assegurando a confidencialidade, integridade e disponibilidade das informações, com a implantação e manutenção dos controles e princípios que serão descritos Neste documento, as quais devem ser seguidas e consideradas em todas as atividades realizadas dentro ou fora das dependências do Sistema Ailos, sempre que exista a necessidade de manipulação de suas informações.

5 Segurança na Organização e Política de Segurança da Informação - PSI?

O terceiro deve possuir governança de Segurança da Informação responsável por controlar, implementar e operar a Segurança da Informação dentro da organização.
Os colaboradores e terceiros, do terceiro contratado, devem ser treinados periodicamente de acordo com os procedimentos de segurança e uso correto das instalações de processamento da informação. O fornecedor se compromete, por si e por seus funcionários, a aceitar e aplicar as diretrizes definidas nesta Declaração de Privacidade e Segurança para Terceiros.

6 Gestão de Ativos de Informação?

O terceiro deve realizar a gestão dos ativos de informação, no que tange à sua identificação, e definição de papéis e responsabilidades de seus colaboradores para assegurar que as informações recebam um nível adequado de proteção, e estando sempre alinhado à classificação das informações atribuída pelo Sistema Ailos.
No caso dos ativos de informação do Sistema Ailos, o terceiro entende e concorda que acessos privilegiados, como administradores de domínios, recursos de rede, aplicações, banco de dados e outros recursos de infraestrutura crítica são concedidos exclusivamente pelo Sistema Ailos aos colaboradores do terceiro.
Todos os acessos mencionados acima deverão possuir, revisão periódica, monitoramento, dupla custódia sendo que os respectivos registros deverão ser mantidos como evidência da realização desses processos a ser fornecida ao Sistema Ailos, mediante solicitação formal.

7 Segurança nas Comunicações?

Os terceiros devem se comprometer a segregar logicamente e fisicamente os dados do Sistema Ailos dos demais clientes.
Também devem assegurar a implementação de procedimentos de filtragem dos acessos à Internet para proteger as estações de trabalho do usuário final de sites mal-intencionados e transferências de arquivos não autorizados. As informações do Sistema Ailos devem ser criptografadas quando em repouso.
As atividades de compartilhamento e transmissão da informação, devem ser realizadas através dos meios seguros e homologados pela Segurança da Informação do Sistema Ailos (API ou SFTP).

8 Uso de Internet?

Para casos em que a atuação *in loco* seja necessária, o uso de conexões aos sistemas de internet é permitido para atender apenas os propósitos de negócios do Sistema Ailos, tendo a cooperativa o direito, a qualquer momento, de:

- ✓ Suspender o acesso do terceiro;
- ✓ Restringir o download e upload de arquivos ou acesso a conteúdo que não sejam de interesse da cooperativa;
- ✓ Monitorar e auditar os acessos;
- ✓ Solicitar aos terceiros justificativas por acessos efetuados.

É expressamente vetado o uso dos recursos do Sistema Ailos para:

- ✓ Acesso ou veiculação de conteúdo relacionado à pedofilia;
- ✓ Veiculação de conteúdos de cunho: político, religioso, racial, orientação sexual, pornográfico e ilegal (pirataria de software, comércio de ilícitos etc.);
- ✓ Quaisquer outras atividades consideradas inapropriadas, indevidas ou desvinculadas às atividades desempenhadas na cooperativa;
- ✓ Publicar, postar, carregar, distribuir ou divulgar quaisquer tópicos, nomes, materiais ou informações que incentivem a discriminação, ódio ou violência com relação a uma pessoa ou a um grupo;
- ✓ Uso de falsa identidade ou assumir, sem autorização, a identidade de outro usuário;
- ✓ Utilizar-se da internet e outros serviços disponibilizados com o intuito de cometer fraude;
- ✓ Utilizar os serviços, para de qualquer modo reproduzir ou infringir direitos de terceiros, sejam imagens, áudio, fotografias, vídeos, softwares ou qualquer material protegido por lei de propriedade intelectual, incluindo, lei de direitos autorais, marcas ou patentes;
- ✓ Fins ilícitos, tais como: atividades hackers, crackers, bombas, falsidade ideológica, entre outros;
- ✓ A utilização da rede Wi-Fi por dispositivos não homologadas pelo Sistema Ailos. Em caso de exceção para prestadores de serviço e terceiros que desenvolverão projetos de longo prazo, é necessário abrir uma solicitação junto à CSTI, devendo passar pela aprovação do gestor imediato.

Declaração de Privacidade e Segurança para Terceiros

9 Backup e Restore?

Os terceiros devem possuir as políticas de backup e restore bem definidas para os dados, software e sistemas que tratam dados do Sistema Ailos, e devem realizar periodicamente o procedimento de execução destes backups e testes de restore nesses ativos envolvidos, de forma a evitar ou minimizar a perda de dados, diante da ocorrência de incidentes, quando aplicável.

Os testes de backup e restore devem ser registrados e monitorados a fim de observar e corrigir possíveis falhas no decorrer do processo.

As cópias de backup devem estar guardadas em local apropriado e seguro, e devem ser mantidas medidas técnicas para proteger contra o acesso por pessoas não autorizadas. Para toda mídia armazenada fora da infraestrutura do Sistema Ailos, estas devem ser mantidas criptografadas e as chaves de segurança, armazenadas em um cofre corporativo.

O terceiro deverá manter uma cópia do plano de Backup/Restore juntamente com o backup contingencial.

10 Controle de Acesso?

Os terceiros devem possuir controles de acessos à informação a fim de se proteger contra possíveis danos, acessos não autorizados ou perdas. Sendo assim, os terceiros devem possuir uma Política de Controle de Acesso que descreva as diretrizes para a criação, alteração, revisão exclusão de contas de usuários para sistemas ou aplicativos.

Os privilégios da conta do usuário devem ser realizados com base no princípio do privilégio mínimo necessário e devem ser formalmente autorizados e registrados.

Os direcionadores sobre uso de senha segura e duplo fator de autenticação devem ser formalmente registrado, contendo todas as precauções necessárias para cuidar das credenciais de acesso e se proteger contra acesso não autorizado.

Quando aplicável para a prestação do serviço, o terceiro deve credenciar nos domínios do Sistema Ailos seus profissionais autorizados a operar presencialmente e remotamente, aqueles que terão acesso aos sistemas corporativos, inclusive com a assinatura de termo apropriado de sigilo e responsabilidade.

O terceiro se responsabiliza a comunicar ao Sistema Ailos, com antecedência de no mínimo 1 dia útil, qualquer término ou mudança de responsabilidades de emprego de funcionários envolvidos diretamente na execução dos serviços de suporte à infraestrutura, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos do Sistema Ailos, caso aplicável a esta contratação.

Declaração de Privacidade e Segurança para Terceiros

AILOS
SISTEMA DE COOPERATIVAS

11 **Gestão de Vulnerabilidades?**

O terceiro deve possuir processo formal para a realização de testes de vulnerabilidades e intrusão em seus dispositivos de rede, telecomunicações, aplicações, estações de trabalho e servidores. Os testes devem ser realizados periodicamente. Devem ser mantidos os relatórios, assim como resultados e respectivos planos de ação para mitigação e gestão dos riscos, e estarem disponíveis para apresentação ao Sistema Ailos sempre que solicitado.

12 **Gestão de incidentes?**

O terceiro deve efetuar a gestão de incidentes para assegurar um processo efetivo na atuação de pessoal treinado e equipado para detectar, relatar e tratar fragilidades e eventos de segurança da informação.
É necessário a presença de monitoramento e resposta tempestiva para retomada da disponibilidade do serviço com menor impacto ao negócio, como por exemplo, o uso de serviços de segurança gerenciados.
Caso o terceiro tome conhecimento ou possua suspeita da ocorrência de um evento ou incidente envolvendo informações ou ativos de informação do Sistema Ailos, o fornecedor deverá comunicar imediatamente à área Segurança da Informação pelo e-mail encarregado.lgpd@ailos.coop.br e manter a área gestora do contrato informada. Além disso, o fornecedor deve possuir procedimentos para identificação, tratamento, monitoramento e reporte do incidente.

13 **Gestão de mudanças?**

O terceiro deve possuir um processo de gestão de mudanças, com o intuito de controlar as alterações nos sistemas de produção, rede de produção, aplicativos, arquivos de dados estruturais, outros componentes do sistema e mudanças físicas/ambientais, através de um registro formal de controle de mudança, minimizando os impactos e riscos associados à manutenção do serviço fornecido ao Sistema Ailos.

Declaração de Privacidade e Segurança para Terceiros

AILOS
SISTEMA DE COOPERATIVAS

14

Gestão da Continuidade do Negócio e Recuperação de Desastres ?

O terceiro deve se comprometer a manter a continuidade das operações de Segurança da Informação a fim de minimizar as perdas e manter a operacionalidade dos sistemas em situações adversas, como, por exemplo, situações de crise ou desastre.

16

Auditoria?

O terceiro deve permitir que o Sistema Ailos monitore e avalie os serviços contratados por meio de diligências, desde que avisada previamente com mínimo de 10 (dez) dias úteis, a aderência aos requisitos contratuais, incluindo os controles de Segurança da Informação. Sendo assim, comprometem-se a disponibilizar sua documentação, relatórios e/ou informação comprobatória durante a diligência.
Os terceiros devidamente certificados pela ISO 27001 não precisarão realizar esse processo de auditorias, desde que apresente a comprovação da vigência da certificação para o escopo contratado e o mesmo seja validado pela área de Segurança da Informação do Sistema Ailos.

17

Segurança em Recursos Humanos?

O terceiro declara que os funcionários e terceiros compreendem suas responsabilidades e estão em conformidade com os papéis para os quais foram selecionados.
O terceiro, bem como seus representantes, empregados e colaboradores devem zelar pela manutenção do sigilo absoluto de dados, informações, documentos e especificações técnicas do Sistema Ailos de que tenham conhecimento em razão dos serviços executados.

15

Conformidade e Governança?

Manter um plano de controle de Segurança da Informação e de Sistemas com o propósito de controlar o nível geral de Segurança da Informação e do ambiente cibernético. As políticas, inclusive a de Segurança da Informação devem ser revisadas regularmente.
As atividades realizadas com dados pessoais devem estar em observância das normas e leis de privacidade de dados, e de acordo com as diretrizes do Sistema Ailos.
Todas as atividades realizadas devem garantir a observância das obrigações contratuais para assegurar que as devidas exigências de segurança sejam levadas em conta em seus processos.
Caso o Sistema Ailos identifique alguma conduta não aderente ou o descumprimento das diretrizes estabelecidas, serão tomadas as medidas administrativas e ou legais cabíveis.

18 Segurança Física e Lógica?

O controle de acesso físico às medidas e tecnologias utilizadas para proteger e limitar o acesso físico a edifícios, instalações, áreas restritas ou recursos físicos. Isso envolve o uso de sistemas e dispositivos de segurança para garantir que apenas pessoas autorizadas possam entrar em locais específicos. Algumas das técnicas comuns de controle de acesso físico incluem:

- ✓ Cartões de acesso: Utilização de cartões ou crachás eletrônicos que contêm informações de identificação do indivíduo autorizado.
- ✓ Biometria: Emprego de características únicas do corpo humano, como impressões digitais, reconhecimento facial ou leitura da íris, para autenticar e permitir o acesso.
- ✓ Portões e catracas: Instalação de portões e catracas que só permitem o acesso após a validação da identificação.
- ✓ Vigilância: Monitoramento com câmeras de segurança e sistemas de alarme para detecção e prevenção de intrusos.

É essencial que o terceiro mantenha um controle de acesso físico para proteger ativos, informações sensíveis e garantir a segurança geral de instalações físicas.

O controle de acesso lógico refere-se a medidas e procedures utilizadas para garantir que somente usuários autorizados tenham acesso a informações ou sistemas específicos. Isso é geralmente alcançado através de autenticação, autorização e auditoria de atividades. Existem várias técnicas e ferramentas para implementar o controle de acesso lógico, como senhas, autenticação de dois fatores, certificados digitais e políticas de controle de acesso baseadas em funções (RBAC), entre outros. É essencial que o terceiro tenha definido seus controles de acesso lógico para a segurança de dados e sistemas em ambientes digitais.

Declaração de Privacidade e Segurança para Terceiros

19

Análise de Riscos?

A gestão de riscos cibernéticos é de responsabilidade do terceiro, bem como da área de Segurança da Informação da Central Ailos. Este processo identifica os requisitos de segurança da informação relacionado com a cadeia de suprimentos. A gestão de riscos cibernéticos é contínua e define contextos internos e externos para avaliação, além de tratar riscos identificados de modo que sejam reduzidos a níveis aceitáveis.

20

Subcontratação de Serviços pelo terceiro?

Em caso de subcontratação de serviço, o terceiro deverá informar a Ailos:

- Qual a localização da sede do subcontratado;
- Descrição do Produto ou Serviço;
- Se haverá trânsito de informações de propriedade do Sistema Ailos com este fornecedor subcontratado;
- Se o subcontratado possui certificação ISO/IEC 27001;
- Se o subcontratado possui outras certificações.

21

Avaliação de segurança da Informação?

A avaliação dos terceiros é realizada através de um questionário disponibilizado no sistema OneTrust. Este questionário contém os critérios de avaliação para classificar o nível de maturidade em Segurança da Informação. O ciclo de revalidação é anual.

22

Requisitos de Privacidade e Proteção de Dados

- Manter Programa de Privacidade e Proteção de Dados, nos termos do art. 50 LGPD;
- Nomeação de Encarregado pelo tratamento de dados pessoais, nos termos do art. 41 da LGPD c/c exceções da Resolução CD/ANPD nº2;
- Manter registro da operação de tratamento de dados pessoais;
- Realizar tratamento de dados pessoais justificado em, ao menos, uma base legal, prevista nos art. 7º ou 11 da LGPD;
- Direcionar o tratamento de dados os princípios estabelecidos pela LGPD em seu art. 5º;
- Sob nenhuma hipótese, tratar dados pessoais para fins diversos aos contratados pelo Sistema Ailos;
- Em caso de contato direto com o titular, o fornecedor deve ter protocolo de comunicação alinhado com as expectativas do Sistema Ailos;
- Auxiliar o Sistema Ailos, por meio de medidas técnicas e operacionais, sempre que possível, e tempestivamente, a cumprir as suas obrigações de resposta às solicitações de titulares de dados que procuram exercer os seus Direitos;
- Salvo instruções em contrário, o fornecedor deverá encaminhar para encarregado.lgpd@ailos.coop.br todos os Titulares dos Dados que contactarem diretamente o fornecedor para exercer os seus Direitos;
- Informar a existência de subcontratação: no ato de preenchimento da Avaliação de Segurança da Informação para Terceiros junto ao Sistema Ailos, ou, se no decorrer de execução da prestação de serviço, antes do compartilhamento de dados do Sistema Ailos com terceiro subcontratado;
- Informar a existência de transferência internacional de dados: no ato de preenchimento da Avaliação de Segurança da Informação para Terceiros junto ao Sistema Ailos, ou, se no decorrer de execução da prestação de serviço, antes do compartilhamento de dados do Sistema Ailos com o país estrangeiro;
- Na hipótese de identificação incidente de privacidade, informar imediatamente a área de privacidade do Sistema Ailos, sempre antes de comunicar a Autoridade Nacional de Proteção de Dados ou titulares de dados.

22 Requisitos de Privacidade e Proteção de Dados

- Caso o terceiro tenha acesso ao nosso ambiente lógico ou físico, deverá tomar conhecimento e aplicar o conteúdo das Normas e Políticas relacionadas a Privacidade e Proteção de Dados e Segurança da Informação;
- Quando aplicável, o terceiro deve coletar e manter registro do consentimento do Titular dos Dados para todas as suas atividades de antes de recolher os Dados Pessoais do Titular dos Dados. O fornecedor deverá manter gestão dos consentimentos coletados a fim de assegurar os requisitos estabelecidos pelos artigos. 7º, 17 e 18 da LGPD;
- Quando aplicável, o terceiro deve coletar e manter registro da autorização de pelo menos um dos pais ou responsável legal da criança antes de recolher os Dados Pessoais do Titular dos Dados, nos temos do art. 14, §1º da LGPD;
- Os terceiros cuja prestação de serviço envolva a gestão de sites e aplicativos devem manter públicas as Declarações de Cookies, bem como forma de gestão transparente de cookies;
- Assegurar que os dados pessoais controlados pelo Sistema Ailos não sejam retidos durante mais tempo do que o necessário para seu tratamento, exceto nos casos previstos pelo art. 16 da LGPD;
- Assegurar que, ao final da prestação de serviço, os dados pessoais e informações internas e restritas do Sistema Ailos sejam devolvidos ou destruídos;
- O terceiro deve manter a integridade de todos os dados pessoais do Sistema Ailos, assegurando que estes se mantêm exatos, completos e relevantes para a finalidade informada;
- Anonimizar, em ambiente de desenvolvimento ou teste, todos os dados pessoais controlados pelo Sistema Ailos;
- O terceiro deve manter suas informações classificadas de forma a apontar e proteger a confidencialidade das informações, com base em sua criticidade.

23

Treinamento e Conscientização em Segurança da Informação?

Terceiros, é preciso seguir as disposições a seguir e notificar os seus colaboradores sobre:

- ✓ A fim de cuidar da segurança do nosso ambiente, promovemos ações, eventos, cursos e a participação neles pode ser uma obrigatoriedade;
- ✓ Não compartilhar as credenciais de acesso com outras pessoas, além de utilizar das soluções de cofre de senhas para armazenamento de dados de acesso;
- ✓ Não expor informações do Sistema Ailos a pessoas não autorizadas;
- ✓ Não sair de crachá para fora das dependências da Cooperativa;
- ✓ Não utilizar ou compartilhar contatos corporativos, como e-mail e número de telefone para situações particulares;
- ✓ Obrigatoriedade de que a mão de obra alocada realize os cursos de Segurança da Informação, que poderão sofrer alteração de acordo com a área em que tiverem alocados;
- ✓ No caso de uso de equipamentos Ailos, deverão se ater ao uso exclusivo aos fins da função exercida;
- ✓ Manter poucos itens na mesa de trabalho, principalmente os que se referem ao Sistema Ailos.

24 Desenvolvimento e Manutenção de Sistemas?

Devem ser adotadas práticas de desenvolvimento seguro em sistemas de propriedade do terceiro, bem como na prestação de serviços de desenvolvimento;
Não devem ser usados dentro de um ambiente de teste os dados de produção do Sistema Ailos. Caso seja inevitável, os dados devem ser sanitizados. Dados pessoais devem ser anonimizados, antes de serem usados.

25 Tecnologia em Nuvem?

Os terceiros que possuem serviços em nuvem, é recomendado salvaguardar o gerenciamento, a aquisição e o suporte à Segurança da Informação nesses serviços, de modo a garantir a confidencialidade, integridade e disponibilidade das informações presentes no sistema operacional.
A Central Ailos também orienta assegurar a criptografia dos dados em trânsito e repouso nas camadas de aplicação e de interfaces.
É indicado possuir diretrizes sobre a utilização de serviços em nuvem que contemple as estratégias de adesão desses serviços, visando o cumprimento da legislação e da regulamentação em vigor e descrevendo como se realizará a substituição de prestadores de serviços, em nuvem em caso de descontinuidade ou necessidade.
Sempre informar a Central Ailos o mais rápido possível sobre a contratação de terceiros de armazenamento e processamento de dados em nuvem, indicando qual a empresa selecionada, quais os serviços e, se possível, quais os países e regiões onde os dados serão armazenados, processados e gerenciados.

26

Propriedade Intelectual?

Não é permitida a reprodução ou manutenção de cópias ilegais de propriedade intelectual de qualquer natureza de serviços. O Sistema Ailos preza e resguarda a propriedade intelectual por ela produzida, bem como a dos terceiros.

27

Término de Contrato?

Em caso de encerramento de contrato, a fim de assegurar um término seguro do relacionamento, o terceiro deve garantir que todos os dados do Sistema Ailos em sua posse sejam completamente migrados para o ambiente do Sistema Ailos e, posteriormente expurgados de sua propriedade exclusiva, com o acompanhamento dos representantes a serem devidamente informados pelo Sistema Ailos, utilizando ferramentas que garantam que as informações foram permanentemente deletadas, e caso não for possível realizar o expurgo de dados, o fornecedor deve garantir que os dados estejam protegidos contra vazamento e/ou acesso não autorizado.

AILOS

SISTEMA DE COOPERATIVAS