# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

UPE622A
REV. 1

# Sumário

## 1. OBJETIVOS

- Estabelecer o compromisso da **Aethra Sistema Automotivos S.A.** em resguardar e proteger as informações, sejam elas pessoais ou não, que estão sob sua guarda, além de definir a governança de **segurança da informação na Organização.**

- Apresentar diretrizes gerais de conduta, bem como obrigações a serem seguidas na Aethra a fim de mitigar eventuais riscos e danos relacionados a ameaças externas ou internas, deliberadas ou acidentais que possam impactar na **confidencialidade**, **integridade** e **disponibilidade** das informações de qualquer natureza, objetivando garantir sua preservação. Esta Política está alinhada ao cumprimento da Lei 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), bem como aos padrões e medidas técnicas visando a Segurança da Informação.

- Promover uma cultura de segurança da informação, integrar as práticas de segurança da informação em todas as atividades e processos organizacionais, garantindo que os colaboradores estejam conscientes de seus papéis e responsabilidades.

- Facilitar a continuidade dos negócios, implementar controles e práticas que minimizem interrupções operacionais decorrentes de incidentes de segurança, assegurando a resiliência e continuidade das operações.

- Estabelecer um ciclo de melhoria contínua, garantir a evolução constante do sistema de gestão, monitorando e ajustando os controles e processos de acordo com as novas ameaças e vulnerabilidades.

## 2. ABRANGÊNCIA

Este documento se aplica a todos os colaboradores Aethra, seus fornecedores, terceiros e prestadores de serviços.

Deverão ser observadas as presentes regras e recomendações em quaisquer operações que possam impactar na Segurança da Informação na Aethra.

## 3. DISTRIBUIÇÃO:

Intranet // Normas Organizacionais // UPE // UPE 622A.

## 4. APROVAÇÃO / VALIDADE:

DocuSigned by:
D9BEEDA3D382472...
Rafael Giovanni Gomes Sportelli
CEO

A Política de Segurança da Informação foi aprovada e entra em vigor a partir de 14/11/2024.

## 5. CONCEITOS E DESCRIÇÕES

**5.1** **ATIVOS DE INFORMAÇÃO:** são os meios de produção, armazenamento, transmissão e processamento de informações, os sistemas de informação, os locais onde se encontram esses meios, as pessoas que têm acesso a informações, assim como as próprias informações coletadas, produzidas, processadas, armazenadas, custodiadas, descartadas e transmitidas pela Aethra.

**5.2** **ATIVOS DE SUPORTE:** Um ativo de suporte refere-se aos recursos que sustentam a operação e a proteção dos ativos de informação. Isso inclui: **Hardware:** Equipamentos físicos, como servidores, computadores, roteadores e dispositivos de armazenamento. **Infraestrutura:** Redes e sistemas de telecomunicações que facilitam o acesso e a transmissão de informações. **Ambiente:** Físico e lógico onde os ativos de informação são armazenados e processados, incluindo salas de servidores e ambientes de nuvem. **Pessoas:** Colaboradores e suas competências, essenciais para a gestão e proteção dos ativos.

**5.3** **CONFIDENCIALIDADE:** propriedade de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizados e credenciados.

**5.4** **INTEGRIDADE:** propriedade de que a informação não foi modificada, suprimida ou destruída de maneira não autorizada ou acidental.

**5.5** **DISPONIBILIDADE:** propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física por determinado sistema ou setor da Aethra no momento requerido.

**5.6** **CRIPTOGRAFIA:** método de codificação da informação que visa evitar que ela seja compreendida ou alterada por pessoas não autorizadas.

**5.7** **CUSTÓDIA DO ATIVO DE INFORMAÇÃO:** é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia.

**5.8** **DADOS PESSOAIS:** todo e qualquer dado relacionado a pessoa natural identificada ou identificável (art. 5º, I, da Lei nº 13.709/2018-Lei Geral de Proteção de Dados Pessoais).

**5.9** **EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM SEGURANÇA DA INFORMAÇÃO:** grupo de pessoas com responsabilidade de receber analisar e responder as notificações relacionadas a incidentes com ativos de informação da Aethra.

**5.10** **GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO:** conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação.

**5.11** **RESPONSÁVEL DE ATIVOS DE INFORMAÇÃO:** responsável por gerenciar determinado segmento de informação e todos os ativos relacionados.

**5.12** **LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD):** Lei Nº 13.709/2018, que dispõe sobre o tratamento de dados pessoais, em meios físicos ou digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado.

**5.13** **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI):** é um conjunto de regras, diretrizes e procedimentos que visam proteger a integridade, confidencialidade e disponibilidade de informações e sistemas de informação. Ela é parte importante da governança da informação de uma empresa.

**5.14** **QUEBRA DE SEGURANÇA:** ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações.

## 6. PROCEDIMENTOS/RESPONSABILIDADES

### 6.1. Política de Segurança da Informação Aethra - PSI

Esta Política de Segurança da Informação exige o cumprimento do **Código de Conduta e Ética Aethra** e de todas as leis e regulamentações aplicáveis e em vigor relacionadas à Proteção de Dados incluindo, sem limitação, a Lei Geral de Proteção de Dados Pessoais (LGPD).

### 6.2. Diretrizes da Política de Segurança da Informação (PSI)

Estabelecer as orientações que assegurem e reforcem o compromisso da Aethra com as práticas e medidas preventivas garantidoras de segurança da informação.

Definir o referencial para a normatização das questões de segurança da informação na Aethra.

Criar condições para que a Aethra eleve continuamente a sua maturidade em segurança da informação, por meio da adoção de diretrizes, normas e procedimentos destinados a proteger os **ativos de informação** da Aethra visando a promoção da integridade, confidencialidade, autenticidade e disponibilidade dos ativos de Informação da Aethra.

Prover a Aethra de mecanismos de atendimento e conformidade às leis de segurança da informação, nacionais e internacionais.

Descrever regras comportamentais e diretrizes a serem seguidas na condução das atividades desenvolvidas pela Aethra que garantam a prevenção de incidentes de segurança da informação e a proteção de dados pessoais.

Os documentos que se relacionam com esta Política são:

- “Código de Conduta e Ética Aethra” - UPE 279A;
- Documentos normativos do sistema de gestão integrado (SGQ e SGA);
- Requisitos e satisfação das partes interessadas, tais como fornecedores e clientes;
- Requisitos legais aplicáveis;
- “Código de Conduta TI” – UPE 190A;
- Outras políticas e procedimentos auxiliares de segurança da informação.

Esses documentos reforçam o compromisso da Aethra com a Segurança da Informação.

### 6.3. Compromisso com a Segurança da Informação

O compromisso da Aethra com a Segurança da Informação é garantido pela preservação de quatro aspectos:

**Autenticidade** - todos os esforços serão feitos para que as informações sejam confiáveis e

corretas, ou seja, as informações não serão alteradas de forma não autorizada ou indevida.

**Confidencialidade -** O acesso à informação é permitido somente para pessoas autorizadas e quando ele for de fato necessário.

**Disponibilidade** - somente as pessoas autorizadas têm acesso à informação, sempre que necessário.

**Integridade –** todos os esforços serão feitos para que as informações sejam exatas e completas bem como seu processamento.

## 7. GESTÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Gestão de Segurança da informação na Aethra é de responsabilidade do "Comitê de Segurança da Informação e Privacidade de Dados", cujos membros estão definidos no **"Regimento do Comitê de Segurança da Informação e Privacidade**" - **UPE623A.**

O cumprimento desta Política, PO - Procedimentos Operacionais, IOA - Instruções Operacionais e Manuais complementares devem ser avaliados periodicamente por meio de verificações de conformidade, realizadas pelo "Comitê de Segurança da Informação e Privacidade de Dados".

A Aethra se orienta pelos melhores frameworks recomendados por entidades especializadas responsáveis pelo estabelecimento de padrões relacionados à segurança de informação.

### 7.1 Informações Complementares do Comitê de Gestão da PSI

#### 7.1.1 Escopo do Sistema de Gestão de Segurança da Informação (SGSI)

- **Abrangência geográfica** - O SGSI da Aethra cobrirá todas as Unidades da empresa, considerando os sites de: Contagem, Betim, Pouso Alegre e Taubaté, além dos fornecedores e parceiros externos envolvidos.
- **Ambiente de TI e dados cobertos** - O escopo incluirá toda a infraestrutura de TI, dados em trânsito e em repouso, além de informações confidenciais dos clientes, colaboradores e parceiros.
- **Fornecedores e parceiros** - Os controles deverão ser aplicáveis aos fornecedores externos, especialmente aqueles envolvidos em projetos críticos e desenvolvimento de veículos ou componentes.
- **Aplicação de controles do TISAX** – Todos os controles exigidos para áreas específicas, como segurança física, proteção de protótipos, segurança nas comunicações, proteção contra-ataques cibernéticos e gerenciamento de vulnerabilidades fazem parte do escopo. O objetivo é garantir conformidade com os requisitos do TISAX, atendendo todos os controles de Segurança da Informação e Proteção de Protótipos conforme escopo "***TISAX Standard Scope 2.0.1*** *- A avaliação inclui todos os processos, procedimentos e recursos sob responsabilidade da organização avaliada que são relevantes para a segurança dos Objetos de Proteção e suas Metas de Proteção definidas nos Objetivos de Avaliação TISAX selecionados para todos os locais listados. A avaliação é conduzida no Nível de Avaliação TISAX mais alto definido em qualquer um dos*

*Objetivos de Avaliação TISAX selecionados. Todos os critérios listados nos Objetivos de Avaliação TISAX estão sujeitos à avaliação*" e as exigências específicas da versão em vigor, assegurando a certificação e a manutenção da conformidade com os requisitos de segurança da informação do setor automotivo.

- **Integração com outros sistemas de gestão** – A **Aethra** possui outros sistemas de gestão, como ISO 9001, ISO 14000, IATF e o SGSI está integrado para otimizar a gestão dos recursos e controles.

### 7.1.2 Classificação da Informação

Para garantir o correto tratamento e proteção dos dados, as informações da **Aethra** devem ser classificadas de acordo com seu nível de sensibilidade. A classificação da informação nos ajuda a definir quem pode acessá-la e como ela deve ser protegida.

As categorias de classificação são as seguintes:

**Confidencial -** Informações que, se divulgadas sem autorização, podem causar danos significativos à empresa, seus clientes ou parceiros. Somente pessoas autorizadas devem ter acesso, e sua distribuição deve ser extremamente restrita. Exemplos: informações financeiras, segredos comerciais, projetos confidenciais e dados pessoais sensíveis.

**Restrita -** Informações que devem ser acessadas apenas por determinados grupos ou setores dentro da empresa. O acesso é limitado e controlado, pois a divulgação não autorizada pode causar impacto à operação ou comprometer a competitividade da empresa. Exemplos: planos estratégicos, contratos com fornecedores e dados de projetos em desenvolvimento.

**Interna -** Informações destinadas ao uso exclusivo da empresa, acessíveis apenas por funcionários ou prestadores de serviço. Não deve ser compartilhada publicamente, mas o impacto da divulgação não autorizada é moderado. Exemplos: políticas internas, documentos de planejamento e relatórios operacionais.

**Pública –** Informações que podem ser divulgadas sem causar impacto à empresa. Estes dados são de acesso livre e não precisam de medidas rigorosas de proteção. Exemplos: materiais promocionais, comunicados de imprensa e conteúdo publicado em sites públicos.

**Regras de Tratamento**

- **Confidencial:** Requer proteção máxima, como criptografia e controle rigoroso de acesso. Não deve ser transmitida sem segurança adequada.
- **Restrita:** Deve ser acessada apenas por grupos específicos, com controles de acesso e monitoramento. Não pode ser compartilhada fora desses grupos sem autorização.
- **Interna:** Protegida por senhas e acessível apenas por funcionários autorizados. Não deve ser compartilhada fora da empresa.

- **Pública:** Pode ser compartilhada livremente, sem necessidade de medidas especiais de proteção.

É responsabilidade de todos os colaboradores garantir que as informações sejam corretamente classificadas e protegidas conforme seu nível de sensibilidade.

### 7.1.3 Gestão de Ativos de Informação e Suporte

O objetivo principal da gestão de ativos é garantir a proteção e a integridade dos ativos da Organização, que incluem tanto os **ativos de informação** quanto os **ativos de suporte**. Isso é alcançado por meio de:

- **Identificação de Ativos:** Catalogar todos os ativos de informação e de suporte, incluindo hardware, software, dados e documentação, assegurando que cada ativo tenha um responsável designado.
- **Classificação de Ativos:** Classificar os ativos com base em sua importância e sensibilidade, estabelecendo critérios claros para determinar o nível de proteção necessário para cada categoria.
- **Controle de Acesso:** Implementar controles de acesso adequados para garantir que apenas pessoas autorizadas possam acessar e manipular os ativos, protegendo informações sensíveis contra acessos não autorizados.
- **Manutenção e Atualização:** Estabelecer rotinas para a manutenção e atualização dos ativos de informação e de suporte, garantindo que estejam sempre em conformidade com as melhores práticas de segurança e desempenho.
- **Proteção de Dados:** Aplicar medidas de segurança, como criptografia e backups regulares, para proteger os ativos de informação contra perda, corrupção ou acesso indevido.
- **Descarte Seguro:** Desenvolver procedimentos para o descarte seguro de ativos obsoletos, assegurando que dados sensíveis sejam completamente eliminados e não possam ser recuperados.
- **Monitoramento e Auditoria:** Implementar um processo de monitoramento e auditoria regular dos ativos, avaliando a eficácia das medidas de segurança e identificando áreas para melhoria contínua.
- **Treinamento e Conscientização:** Promover a conscientização sobre a importância da gestão de ativos entre todos os colaboradores, oferecendo treinamentos regulares sobre práticas seguras e responsáveis de uso e manejo dos ativos.

### 7.1.4 Gestão de Riscos de Segurança da Informação

A Gestão de Riscos e de Segurança da Informação-GRSI é um processo contínuo e deve ser aplicado na implementação e operação da gestão de segurança da informação, levando em consideração o planejamento, execução crítica e melhoria da segurança da informação. Visa identificar ameaças e reduzir as vulnerabilidades dos ativos de informação, assim como reduzir os impactos de eventuais incidentes com eles. Etapas a serem seguidas:

- **Identificação de Riscos:** Realizar regularmente a identificação de riscos que

possam impactar a segurança da informação, abrangendo ativos, vulnerabilidades e ameaças potenciais.

- **Avaliação de Riscos:** Analisar e classificar os riscos identificados com base em sua probabilidade de ocorrência e impacto potencial, priorizando aqueles que representam maior ameaça à organização.
- **Tratamento de Riscos:** Desenvolver e implementar estratégias para mitigar, transferir, aceitar ou evitar riscos, assegurando que as medidas adotadas sejam proporcionais à criticidade do risco.
- **Monitoramento Contínuo:** Estabelecer um processo contínuo de monitoramento e revisão dos riscos e das medidas de controle, garantindo que as mudanças no ambiente interno e externo sejam consideradas.
- **Comunicação e Treinamento:** Promover a conscientização sobre a gestão de riscos entre todos os colaboradores, oferecendo treinamentos regulares para garantir que todos compreendam suas responsabilidades e o papel da segurança da informação.
- **Documentação e Relatórios:** Manter documentação adequada sobre a gestão de riscos (no mínimo anual), incluindo registros de avaliações, decisões tomadas e ações implementadas, e garantir que relatórios periódicos sejam elaborados para a alta direção.
- **Conformidade Legal e Normativa:** Assegurar que a gestão de riscos esteja alinhada com as legislações e normas aplicáveis, garantindo a conformidade e a proteção dos dados e ativos da organização.

### 7.1.5 Segurança da Informação em Recursos Humanos

A gestão de recursos humanos desempenha um papel importante na segurança da informação, assegurando que todos os colaboradores entendam suas responsabilidades e adotem práticas seguras em suas atividades. O ciclo de vida dos colaboradores, desde a contratação até o desligamento, é gerido com foco na proteção da informação, congo. Etapas do ciclo de vida:

- **Contratação:** Durante o processo de contratação, serão realizadas verificações adequadas das documentações e comprovantes de experiência dos candidatos, de acordo com o nível de acesso às informações da empresa que será exigido pela função.
- **Confidencialidade:** Todos os colaboradores devem assinar um acordo de confidencialidade e estarem cientes das suas responsabilidades na proteção dos dados e informações da empresa.
- **Monitoramento do desempenho:** O comportamento e o desempenho dos colaboradores em relação às práticas de segurança da informação serão avaliados regularmente, incentivando o cumprimento das políticas de segurança.
- **Desligamento ou mudança de função:** Quando um colaborador for desligado ou mudar de função, todos os seus acessos lógicos (sistemas) e físicos serão revogados imediatamente, e o retorno de equipamentos e outros ativos será realizado de forma controlada.

Essas medidas garantem que as boas práticas de segurança da informação sejam

integradas à gestão de recursos humanos, reduzindo riscos e promovendo uma cultura de segurança.

### 7.1.6 Treinamento e Conscientização em Segurança da Informação

Todos os colaboradores, terceiros e prestadores de serviços da **Aethra** devem participar de programas de treinamento e conscientização em segurança da informação. Esses treinamentos são essenciais para garantir que todos conheçam as práticas e políticas de segurança, entendam seus papéis e saibam como proteger os dados da **Aethra**.
Os treinamentos serão realizados periodicamente, no **mínimo anual**, incluindo atualizações sobre novas ameaças e procedimentos de segurança. Além disso, todos os novos colaboradores receberão um treinamento inicial sobre a política de segurança da informação durante o processo de **integração**.
A conscientização contínua é fundamental para criar uma cultura de segurança, onde todos os colaboradores estejam atentos e preparados para agir de acordo com as normas de proteção de dados e evitar incidentes de segurança.

### 7.1.7 Uso Aceitável dos Recursos de TI

Os recursos de TI da empresa, como computadores, e-mails, internet, redes, dispositivos móveis, sistemas de comunicação, armazenamento, acesso remoto e sistemas corporativos, devem ser utilizados exclusivamente para atividades relacionadas ao trabalho. O uso adequado desses recursos é essencial para garantir a segurança das informações e o bom funcionamento das operações.
Regras básicas para o uso aceitável dos recursos de TI incluem:

- **Utilização responsável:** Evitar o uso dos recursos de TI, como computadores, impressoras, redes e dispositivos móveis, para atividades pessoais ou não relacionadas ao trabalho.
- **Proteção das credenciais:** Não compartilhar senhas, tokens de autenticação ou outras informações de acesso com terceiros.
- **Uso da internet e redes:** Navegar apenas em sites confiáveis e relacionados ao trabalho. O acesso a conteúdos impróprios, inseguros ou de alto risco para a rede da empresa é proibido.
- **Instalação de software:** Não instalar programas, aplicativos ou extensões sem autorização prévia do TI, incluindo em dispositivos móveis corporativos.
- **Uso de e-mail:** Evitar o envio de informações confidenciais ou sensíveis por e-mail sem a devida proteção, como criptografia.
- **Dispositivos móveis e BYOD:** Seguir as diretrizes de segurança para o uso de dispositivos móveis, especialmente no caso de BYOD (Bring Your Own Device), incluindo a proteção de dados e o uso de redes seguras.
- **Armazenamento e backup:** Utilizar apenas os sistemas de armazenamento aprovados pela empresa, como servidores corporativos e serviços de nuvem autorizados, e garantir a realização de backups conforme as políticas da organização.
- **Mensagens instantâneas e videoconferências:** Utilizar ferramentas de comunicação e videoconferência da empresa com responsabilidade,

assegurando a privacidade e a proteção dos dados compartilhados.

- **Acesso remoto:** Utilizar o acesso remoto (VPN ou outras soluções autorizadas) de maneira segura e apenas para fins corporativos. Assegurar que as conexões sejam feitas por meio de redes seguras e seguir as diretrizes estabelecidas pela empresa para o trabalho remoto.
- **Uso de sistemas corporativos:** Utilizar os sistemas e plataformas de softwares corporativos apenas para atividades relacionadas ao trabalho e de acordo com as permissões de acesso. Não acessar, alterar ou compartilhar informações sem autorização.

O descumprimento dessas regras pode comprometer a segurança da empresa e levar a sanções disciplinares. Todos os colaboradores devem seguir as orientações para garantir o uso seguro e responsável dos recursos de TI.

### 7.1.8 Gestão de Acessos Lógicos e Físicos

A gestão adequada dos acessos é essencial para proteger as informações da empresa. Atribuir permissões de acesso corretas e monitorar os acessos físicos e lógicos (sistemas) ajudam a evitar violações de segurança.

**Acessos Lógicos (Sistemas)**

- **Controle de acesso:** O acesso aos sistemas, aplicativos e redes da empresa será concedido apenas a colaboradores autorizados, de acordo com suas funções e responsabilidades.
- **Princípio do menor privilégio:** Cada usuário terá acesso apenas às informações e sistemas necessários para realizar suas atividades, evitando permissões excessivas.
- **Revisão de acessos:** Os acessos aos sistemas serão revisados periodicamente para garantir que apenas pessoas autorizadas tenham permissão. A remoção de acessos de colaboradores desligados ou que mudaram de função será feita imediatamente.
- **Autenticação:** O uso de senhas fortes e, quando necessário, autenticação de dois fatores será obrigatório para acessar sistemas críticos.

**Acessos Físicos**

- **Controle de entrada:** O acesso a áreas restritas ou confidenciais, como servidores, salas de dados, salas de protótipos ou instalações críticas será controlado por meio de crachás, biometria ou outras medidas de segurança.
- **Permissões físicas:** Apenas colaboradores com autorização específica terão acesso a áreas confidenciais e as permissões serão concedidas conforme a necessidade operacional.
- **Monitoramento de acessos físicos:** Todos os acessos a áreas confidenciais serão monitorados e registrados e qualquer acesso não autorizado será investigado.
- **Revisão de permissões:** O acesso físico também será revisado regularmente para garantir que apenas colaboradores autorizados possam entrar em áreas confidenciais.

O cumprimento dessas diretrizes é fundamental para proteger os dados e ativos da empresa. Qualquer violação de acesso, lógico ou físico, será tratada como um incidente de segurança e poderá resultar em medidas corretivas.

### 7.1.9 Aquisição, Desenvolvimento e Manutenção de Sistemas

O objetivo de **Aquisição, Desenvolvimento e Manutenção de Sistemas** dentro da segurança da informação é garantir que os sistemas utilizados pela Organização sejam seguros, eficazes e alinhados às necessidades de negócio, ao mesmo tempo em que protegem os ativos de informação. Etapas a serem seguidas:

- **Avaliação de Segurança:** Realizar avaliações de segurança em todas as fases de aquisição, desenvolvimento e manutenção de sistemas para garantir que os requisitos de segurança sejam atendidos.
- **Requisitos de Segurança:** Definir e documentar requisitos de segurança específicos antes da aquisição ou desenvolvimento de sistemas, assegurando que as funcionalidades atendam às necessidades de proteção dos ativos de informação.
- **Fornecedores Confiáveis:** Selecionar fornecedores com boas práticas de segurança e conformidade, avaliando sua capacidade de atender aos requisitos de segurança da informação.
- **Controle de Acesso:** Implementar controles de acesso adequados durante o desenvolvimento e a manutenção de sistemas, garantindo que apenas usuários autorizados possam realizar alterações ou acessar informações sensíveis.
- **Teste de Segurança:** Conduzir testes de segurança, incluindo avaliações de vulnerabilidade e testes de penetração, para identificar e corrigir falhas.
- **Documentação Completa:** Manter documentação detalhada sobre o desenvolvimento e a manutenção de sistemas, incluindo configurações de segurança, para facilitar a gestão e a auditoria.
- **Treinamento de Usuários:** Fornecer treinamento adequado aos usuários sobre a utilização segura dos sistemas, promovendo a conscientização sobre boas práticas de segurança.
- **Manutenção e Atualizações:** Estabelecer um cronograma regular para manutenção e atualização de sistemas, incluindo a aplicação de patches de segurança, para proteger contra novas ameaças.
- **Monitoramento e Revisão:** Implementar mecanismos de monitoramento contínuo dos sistemas para detectar e responder a incidentes de segurança, revisando as políticas e procedimentos conforme necessário.

### 7.1.10 Relacionamento com Fornecedores

A gestão da relação com fornecedores é fundamental para garantir que as práticas de segurança da informação sejam mantidas ao longo de toda a cadeia de suprimentos. As diretrizes a seguir ajudam a estabelecer uma abordagem robusta:

- Os acordos com terceiros que possuam algum relacionamento com ativos de informação da Aethra devem observar as disposições e normas dessa “Política

de Segurança da Informação".

- **Avaliação de Segurança do Fornecedor:** Realizar avaliações rigorosas de segurança dos fornecedores antes da contratação, considerando suas práticas de segurança, conformidade regulatória e histórico de incidentes.
- **Requisitos Contratuais:** Incluir cláusulas de segurança da informação nos contratos, especificando obrigações, responsabilidades e requisitos de proteção de dados. Monitoramento Contínuo: Implementar um processo de monitoramento contínuo da segurança dos fornecedores, avaliando periodicamente seu desempenho e conformidade com os requisitos de segurança.
- **Comunicação Eficiente:** Estabelecer canais de comunicação claros para relatar incidentes de segurança e compartilhar informações relevantes sobre ameaças e vulnerabilidades.
- **Treinamento e Conscientização:** Promover a conscientização e o treinamento dos fornecedores sobre as políticas de segurança da informação da Organização e melhores práticas.
- **Gestão de Incidentes:** Garantir que os fornecedores tenham planos de resposta a incidentes que incluam a notificação à Organização em caso de comprometimento de dados ou segurança.
- **Avaliação de Riscos:** Realizar análises de risco para identificar e mitigar riscos associados à relação com fornecedores, considerando o acesso a informações sensíveis e sistemas críticos.
- **Descarte Seguro:** Estabelecer procedimentos para o descarte seguro de informações e ativos ao final do relacionamento com o fornecedor, assegurando que dados confidenciais sejam adequadamente eliminados. Um Plano de Contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.

### 7.1.11 Gestão de Incidentes e Crises

O objetivo do processo de gestão de incidentes e crises é garantir uma resposta rápida e eficaz a eventos que possam comprometer a segurança da informação e as operações da Organização. É um processo essencial para proteger a Organização contra ameaças, garantir a continuidade das operações e fortalecer a confiança de stakeholders. Etapas a serem seguidas:

- **Identificação de Incidentes:** Estabelecer processos claros para a detecção e identificação de incidentes de segurança, garantindo que todos os colaboradores saibam como reportar situações suspeitas.
- **Classificação e Priorização:** Classificar e priorizar incidentes com base em sua gravidade e impacto potencial na organização, facilitando uma resposta adequada e oportuna.
- **Resposta a Incidentes:** Implementar um plano de resposta que inclua procedimentos para contenção, erradicação e recuperação, assegurando que as ações sejam coordenadas e documentadas.
- **Comunicação Eficiente:** Definir canais de comunicação para manter todos os stakeholders informados durante um incidente, incluindo equipes internas e partes externas, quando necessário.

- **Avaliação Pós-Incidente:** Conduzir uma análise pós-incidente para avaliar a eficácia da resposta, identificando lições aprendidas e oportunidades de melhoria para prevenir recorrências.
- **Treinamento e Simulações:** Realizar treinamentos regulares e simulações de incidentes para preparar as equipes para a resposta efetiva e rápida em situações reais.
- **Documentação e Relatórios**: Manter registros detalhados de todos os incidentes e respostas, garantindo que informações relevantes sejam compiladas para relatórios periódicos à Alta Direção.
- **Planejamento de Crises:** Desenvolver um plano de gestão de crises que aborde cenários de maior impacto, incluindo estratégias de comunicação e coordenação durante crises.

### 7.1.12 Aspectos de segurança da informação em continuidades das atividades

A continuidade das atividades é crucial para garantir que a Organização possa operar de maneira eficaz, mesmo diante de incidentes ou crises. Os aspectos de segurança da informação que devem ser considerados incluem:

- 
- **Análise de Riscos:** Realizar avaliações regulares de riscos para identificar ameaças e vulnerabilidades que possam impactar a continuidade das operações, permitindo a implementação de medidas preventivas.
- **Planos de Continuidade e Recuperação de Desastres**: Desenvolver e manter planos de continuidade de negócios (PCN) e de Recuperação de Desastres (DRP) que incluam procedimentos específicos para proteger os ativos de informação e garantir a recuperação rápida em caso de incidentes.
- **Redundância de Sistemas:** Implementar soluções de redundância, como backups de dados e sistemas alternativos, para assegurar que informações críticas possam ser recuperadas e acessadas durante interrupções.
- **Treinamento e Conscientização:** Promover a capacitação contínua dos colaboradores sobre a importância da segurança da informação e os procedimentos a serem seguidos em situações de continuidade.
- **Teste e Validação:** Realizar testes regulares dos planos de continuidade para verificar sua eficácia e a capacidade da Organização de responder a incidentes, ajustando estratégias conforme necessário.
- **Comunicação em Crises:** Estabelecer protocolos de comunicação claros para garantir que todos os stakeholders sejam informados sobre o status das operações e as medidas adotadas para manter a continuidade.
- **Monitoramento e Revisão:** Implementar mecanismos de monitoramento contínuo das operações e revisar periodicamente os planos de continuidade para adaptá-los a mudanças no ambiente de negócios e nas ameaças.
- **Integração com Gestão de Incidentes:** Garantir que os planos de continuidade estejam integrados ao processo de gestão de incidentes, permitindo uma resposta coesa e eficaz em situações adversas.

### 7.1.13 Gestão de Compliance e Conformidade Legal

Deve ser realizada, com periodicidade **mínima anual**, verificação de conformidade das práticas de segurança da informação da **Aethra** e de suas divisões administrativas com esta Política e suas normas de procedimentos complementares, bem como com a legislação específica de segurança da informação.

A verificação de conformidade deve também ser realizada nos contratos, convênio, acordos de cooperação e outros instrumentos do mesmo gênero celebrados com a Aethra.

O calendário de ações de verificação de conformidade é elaborado com base na priorização dos riscos identificados ou percebidos.

A verificação de conformidade pode combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (log) e teste de invasão.

Os resultados de cada ação de verificação de conformidade são documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo Coordenador de TI aos responsáveis da Unidade verificada, para ciência e tomada das ações cabíveis.

### 7.1.14 Plano de investimentos em segurança da Informação da Aethra

Os investimentos em segurança da informação serão realizados de forma planejada e consolidados em um plano de investimento plurianual.

O plano de investimento será elaborado na priorização dos riscos a serem tratados e será obtido a partir da aplicação do método que considere, no mínimo, o produto entre a probabilidade de ocorrência e o impacto do risco no negócio ou na imagem da Aethra.

Os planos de investimentos e seus orçamentos são produzidos, apresentados e geridos pelo “Comitê de Segurança da Informação e Privacidade de Dados”.

## 8. PAPÉIS E RESPONSABILIDADES DE SEGURANÇA DA INFORMAÇÃO

**Comitê de Segurança da Informação e Privacidade de Dados**

- Assessorar a implementação das ações de Segurança da Informação;
- Acompanhar periodicamente a evolução das iniciativas de Segurança da Informação;
- Analisar os reportes de infrações ou violações às Normas de Segurança da Informação e Privacidade, e assegurar a devida tratativa aplicável a cada caso;
- Garantir a imparcialidade ao examinar as ocorrências apresentadas e ao endereçar suas decisões/recomendações;
- Deliberar sobre normas internas de Segurança da Informação;
- Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação;

- Discutir e endereçar situações que envolvam atendimento aos direitos dos titulares de dados;
- Decidir sobre Reporte de Incidentes à ANPD e outras partes interessadas, quando aplicável.

**Responsabilidades do ISO (Responsável pela Segurança da Informação)**

- Desenvolver e implementar políticas de segurança: Elaborar e manter atualizadas as políticas e diretrizes de segurança da informação da **Aethra**.
- Gerenciar riscos de segurança: Identificar, avaliar e mitigar riscos de segurança da informação para proteger os ativos da **Aethra**.
- Monitorar e responder a incidentes: Coordenar o monitoramento dos sistemas e a resposta a incidentes de segurança.
- Realizar auditorias e testes de segurança: Garantir que sejam realizadas auditorias e testes regulares para avaliar a eficácia dos controles de segurança.
- Promover a conscientização: Conduzir programas de treinamento e conscientização em segurança da informação para todos os colaboradores.

**Responsabilidades do DPO (Encarregado de Proteção de Dados)**

- Garantir a conformidade com a legislação: Assegurar que a **Aethra** cumpra as leis e regulamentações de proteção de dados (ex.: LGPD).
- Supervisionar o tratamento de dados pessoais: Monitorar as atividades que envolvem a coleta, armazenamento, uso e compartilhamento de dados pessoais.
- Atuar como ponto de contato: Servir como canal de comunicação entre a **Aethra**, titulares de dados e autoridades regulatórias.
- Conduzir avaliações de impacto: Avaliar e mitigar riscos relacionados à privacidade e proteção de dados.
- Conscientização e treinamento: Promover ações educativas para garantir que os colaboradores entendam suas responsabilidades na proteção de dados.

**Equipe de tratamento e resposta a incidentes em Segurança da Informação**

- Coordenar as atividades de tratamento e respostas a incidentes de segurança;
- Promover a recuperação do sistema junto à área de Tecnologia da informação;
- Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de segurança da informação e avaliando condições de segurança de redes por meio de verificações de conformidade;
- Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;
- Analisar ataques e intrusões na rede da Aethra;
- Executar ações necessárias para tratar quebras de segurança;
- Obter informações quantitativas acerca dos acidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;
- Apurar ações que violem esta política ou quaisquer de suas diretrizes e normas de procedimentos. Aos responsáveis, serão aplicadas as sanções penais, administrativas e cíveis em vigor e
- Participar de fóruns, treinamentos relativos à segurança da informação.

**Tecnologia da Informação - TI**

- Seguir as diretrizes dessa política;
- Garantir a segurança dos ativos de Informação sob sua responsabilidade;
- Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade, em conformidade com esta política;
- Conceder e revogar acessos aos ativos de informação;
- Comunicar a equipe de tratamento e resposta a incidentes em segurança da informação a ocorrência de acidentes de segurança da informação;
- Designar os usuários dos ativos de informação, quando aplicável.
- É de responsabilidade do RH e de Tecnologia da Informação a programação de atividades de treinamento e conscientização.

**Colaboradores e Usuários**

- Conformidade com as Políticas - Seguir rigorosamente todas as políticas e diretrizes de segurança da informação da organização.
- Proteção de Credenciais - Manter senhas e informações de acesso em segurança, evitando compartilhamentos e utilizando senhas fortes e únicas.
- Uso Adequado dos Recursos - Utilizar os recursos da **Aethra** (hardware, software, redes) de maneira ética e para fins profissionais, evitando atividades pessoais que possam comprometer a segurança.
- Notificação de Incidentes - Comunicar imediatamente qualquer incidente de segurança, como acessos não autorizados, perda de dispositivos ou vazamentos de dados.
- Proteção de Dados Sensíveis - Manter a confidencialidade e a integridade de dados sensíveis, seguindo os procedimentos de manuseio e armazenamento estabelecidos.
- Descarte Seguro de Informações - Garantir que documentos e dispositivos com informações confidenciais sejam descartados de maneira segura, conforme as diretrizes da organização.
- Participação em Treinamentos - Participar de treinamentos e workshops sobre segurança da informação, mantendo-se atualizado sobre melhores práticas e novas ameaças.
- Segurança em Conexões - Utilizar apenas redes seguras e confiáveis ao acessar sistemas da **Aethra**, evitando conexões públicas ou não seguras.
- Manutenção de Software - Garantir que os sistemas e aplicativos utilizados estejam sempre atualizados e que as correções de segurança sejam aplicadas prontamente.
- Reportar Vulnerabilidades - Informar sobre quaisquer vulnerabilidades ou falhas de segurança detectadas em sistemas e processos, contribuindo para a melhoria contínua.
- Proteção de Dispositivos - Proteger dispositivos móveis e computadores com senhas, criptografia e outras medidas de segurança, especialmente em ambientes não seguros.
- Uso Responsável de E-mail - Ser cauteloso ao abrir e-mails e anexos de fontes desconhecidas, evitando “phishing” e outras ameaças digitais.
- Controle de Acesso - Garantir que o acesso a informações e sistemas seja restrito apenas a colaboradores autorizados e solicitar revisões de acesso quando necessário.
- Colaboração em Auditorias - Cooperar em auditorias e avaliações de segurança, fornecendo informações e acesso conforme necessário.
- Contribuição para a Cultura de Segurança - Promover uma cultura de segurança dentro da equipe, incentivando colegas a seguir práticas seguras e relatar preocupações.

**Gestores**

- Conscientizar equipe sob sua responsabilidade em relação as Políticas, Procedimentos e

Instruções Operacionais;

- Incorporar aos processos de trabalho de sua divisão ou de seu setor boas práticas em segurança da informação;
- Tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação por parte dos usuários sob sua supervisão;
- Garantir a realização de tratamento e classificação da informação definidos nas políticas, procedimentos e instruções operacionais;
- Autorizar, de acordo com a legislação vigente e as diretrizes do "Comitê de Segurança da Informação e Privacidade de Dados", a divulgação das informações em sua divisão administrativa;
- Comunicar ao TI, os casos identificados de quebra de segurança;
- Solicitar à equipe de tratamento e resposta a incidentes de segurança quando perceber riscos ou suspeitas de incidentes em segurança da informação;
- Manter lista atualizada de ativos de informação sob sua responsabilidade.

**Fornecedores, terceiros, parceiros comerciais**

- **Conformidade com Políticas de Segurança** - Os fornecedores devem estar cientes e aderir às políticas de segurança da informação da Organização.
- **Avaliação de Riscos** - Realizar avaliações de risco regulares para identificar e mitigar potenciais vulnerabilidades relacionadas aos serviços ou produtos fornecidos.
- **Proteção de Dados Sensíveis** - Implementar medidas adequadas para proteger dados sensíveis que possam ser acessados ou processados em nome da organização.
- **Controle de Acesso** - Estabelecer controles de acesso rigorosos para garantir que apenas colaboradores autorizados tenham acesso a informações da organização.
- **Treinamento e Conscientização** - Proporcionar treinamento em segurança da informação para todos os colaboradores que terão acesso a dados ou sistemas da Aethra.
- **Notificação de Incidentes** - Notificar a organização imediatamente sobre qualquer incidente de segurança que possa afetar os dados ou sistemas dela.
- **Gerenciamento de Mudanças** - Informar a organização sobre quaisquer mudanças significativas nos serviços ou processos que possam impactar a segurança da informação.
- **Auditorias e Revisões** - Permitir auditorias e revisões de segurança realizadas pela organização ou por terceiros autorizados para garantir a conformidade com as normas de segurança.
- **Segurança Física e Lógica** - Implementar medidas de segurança física e lógica para proteger instalações e sistemas onde dados da organização são armazenados ou processados.
- **Planos de Continuidade** - Desenvolver e manter planos de continuidade de negócios que abordem a continuidade da prestação de serviços em caso de incidentes de segurança.
- **Subcontratação** - Notificar a organização sobre qualquer subcontratação de serviços e garantir que subcontratados também cumpram com as políticas de segurança da informação.
- **Documentação e Registro** - Manter registros e documentação que demonstrem a conformidade com as políticas de segurança e as responsabilidades acordadas.
- **Proteção de Propriedade Intelectual** - Proteger a propriedade intelectual da organização, evitando divulgação ou uso indevido.
- **Revisão de Contratos** - Rever e atualizar contratos regularmente para incluir cláusulas de segurança da informação e garantir a adesão às práticas de segurança.

## 9. APURAÇÃO, SANÇÕES E CONSEQUÊNCIAS

As sanções devem ter como objetivo reforçar a importância da segurança da informação, promover a conformidade e proteger os ativos da organização.

O Comitê de Segurança da Informação será responsável pelo processamento e deliberação acerca das infrações aos princípios e normas descritos nesta Política de Segurança da Informação.

A violação dos princípios e regras descritos nesta Política de segurança da Informação, cometida por qualquer empregado da AETHRA, estará sujeita às seguintes ações disciplinares, de forma proporcional à infração ocorrida:

- Advertência verbal
- Advertência escrita
- Suspensão
- Desligamento sem justa causa
- Desligamento por justa causa
- Abertura de processo cível e/ou criminal

**Direito de Defesa:** Deve ser garantida aos colaboradores a oportunidade de apresentar sua versão dos fatos antes da aplicação de sanções.

**Documentação:** Devem ser mantidos os registros detalhados de todos os procedimentos realizados para apuração das infrações e sanções aplicadas, incluindo a natureza da infração, a investigação realizada e a decisão tomada.

**Reavaliação e Aprendizado:** Após a aplicação de sanções, deve ser realizada uma análise para identificar se as políticas e procedimentos de segurança precisam ser ajustados ou se há necessidade de treinamentos adicionais.

**Confidencialidade:** Deve ser garantido que todo o procedimento realizado para apuração das infrações e aplicação das sanções cabíveis sejam tratadas com confidencialidade, visando proteger a privacidade dos colaboradores.

**Treinamento e Conscientização:** Devem ser realizados treinamentos regulares para reforçar a importância da segurança da informação e esclarecer as consequências de violações.

## 10. CANAL DE DENÚNCIA E DE INCIDENTES

Todos os empregados e terceiros devem reportar imediatamente qualquer suspeita ou possível violação às regras desta Política para o Canal de Denúncias (codigodeconduta@aethra.com.br, ou à sua chefia imediata no caso de empregados.

Caso o incidente seja reportado à chefia imediata, esta deverá imediatamente abrir chamado ao TI na Intranet (https://intranet.aethra.com.br), sob a denominação “Chamado TI //Seguranca da Informacao”.

O “Canal de Denúncia” é estruturado para garantir o sigilo absoluto, protegendo o anonimato do denunciante e preservando todas as informações para que uma apuração justa possa ocorrer.

## 11. MONITORAMENTO E AUDITORIA

Para garantir a proteção das informações, a **Aethra** realiza o monitoramento contínuo de seus sistemas e recursos tecnológicos. Isso inclui o acompanhamento de acessos, atividades e eventuais tentativas de violação de segurança. Qualquer atividade suspeita ou incidente será identificada e tratada de acordo com os procedimentos estabelecidos.
Além do monitoramento, auditorias internas (**anualmente**) e externas (**a cada 3 anos**) serão realizadas para verificar a conformidade com a Política de Segurança da Informação e as regulamentações aplicáveis. Essas auditorias ajudam a identificar vulnerabilidades e oportunidades de melhoria nos controles de segurança.
O monitoramento e a auditorias periódicas são essenciais para garantir que as práticas de segurança estejam funcionando corretamente e para reforçar a proteção dos dados da **Aethra**.

## 12. REVISÃO E ATUALIZAÇÃO DA POLÍTICA

A Política de Segurança da Informação deve ser revisada regularmente para garantir que continue atualizada e eficaz diante de novas ameaças, tecnologias e mudanças nos processos da **Aethra**.

As revisões ocorrerão pelo menos **uma vez por ano** ou sempre que houver alterações significativas nas operações, na legislação aplicável ou no ambiente de segurança. Qualquer atualização relevante será comunicada a todos os colaboradores e partes interessadas relevantes.

É responsabilidade da equipe de Segurança da Informação coordenar o processo de revisão, recebendo sugestões de melhorias e garantindo que a política esteja alinhada às melhores práticas de mercado e aos requisitos legais.

## 13. ANEXOS

N.A.

## 14. REFERÊNCIAS

TISAX – Trusted Information Security Assessment Exchange
ISO 27001 – Sistema de Gestão de Segurança da Informação
ISO 27005 - Gestão de riscos de Segurança da Informação
Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)

## 15. CONTROLE DE REVISÃO

- Revisão 0 – Elaborado por: responsável pela Segurança da Informação – Aprovado por: CEO - Data de vigor: a partir de 01/12/22
- Revisão 1 – Revisado por: responsável pela Segurança da Informação – Aprovado por: CEO - Data de vigor: a partir de 14/11/24.

⇨ **Essa Política foi revisada na íntegra.**