POL 0005 – SEGURANÇA DA INFORMAÇÃO
Número do documento: POL 0005
Versão do Documento: 005

FOLHA DE APROVAÇÃO

Elaborado por	Função	Assinatura
Renato Rodrigues	Gerente de Infraestrutura e Suporte	Documento assinado digitalmente gov.br RENATO DE JESUS RODRIGUES Data: 26/02/2026 12:12:24-0300 Verifique em https://validar.iti.gov.br
Revisado por	**Função**	**Assinatura**
Eraldo Canuto	Diretor de Tecnologia	Documento assinado digitalmente gov.br ERALDO CANUTO DE SOUSA Data: 27/02/2026 15:13:04-0300 Verifique em https://validar.iti.gov.br
Aprovado por	**Função**	**Assinatura**
Marcello Martins	Diretor de Assuntos Internos	Documento assinado digitalmente gov.br MARCELLO ARAUJO MARTINS Data: 27/02/2026 16:14:37-0300 Verifique em https://validar.iti.gov.br

Sumário

1. Objetivos

A política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da CH MASTER DATA | ASTREIN para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Este documento formaliza o compromisso da empresa com a segurança da informação por meio do SGSI. Os objetivos de segurança da informação são os abaixo informados:

a) Assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações nos processos da organização, alinhando-os aos objetivos estratégicos do negócio.

b) Buscar continuamente o alinhamento com as melhores práticas de segurança da informação do mercado, garantindo conformidade com a legislação, regulamentação, normas e padrões aplicáveis a organização.

c) Promover e desenvolver o comportamento seguro entre colaboradores e parceiros, reforçando a importância da segurança da informação em todos os processos da organização.

d) Estabelecer controles eficazes no tratamento de dados dos clientes, preservando os princípios da segurança da informação;

e) Adotar um modelo de desenvolvimento de sistemas que incorpore princípios de segurança da informação desde a concepção até a implementação.

f) Desenvolver e manter soluções que assegurem que os sistemas e as informações utilizadas por nossos processos estejam devidamente protegidos contra ameaças externas.

g) Responder de forma eficaz e ágil a crises que comprometam os princípios de segurança da informação, garantindo a continuidade dos nossos negócios.

h) Fomentar a melhoria contínua dos processos de segurança da informação, adaptando-os proativamente às novas ameaças e demandas do mercado.

É fundamental reforçar que os regramentos estabelecidos devem ser seguidos por colaboradores, prestadores de serviço e parceiros, garantindo a proteção da informação, a conformidade com normas e legislações e a integridade dos processos organizacionais.

2. Histórico e versões do documento

Versão	Descrição	Data
001	Emissão Inicial do documento	12/01/2023
002	Ajustes no cabeçalho, troca das logomarcas, aumento de espaço para assinatura eletrônica	15/11/2024
003	Foi ajustada a discrepância entre os objetivos do SGSI declarados no documento do contexto organizacional e na PSI Segregação de documentos, deixando apenas os tópicos envolvidos na PSI	24/03/2025
004	Revisão geral e ajustes de estrutura do documento, substituição do procedimento 8000129 – INFRA – PSI – POLÍTICA DA SEGURANÇA DA INFORMAÇÃO pelas políticas POL 0005 – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, POL 0006 - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA USUÁRIO e POL 0007 - POLÍTICA DA SEGURANÇA DE OPERAÇÕES DE INFRAESTRUTURA.	13/05/2025
005	Correção no tópico 3 Escopo, retirando o trecho sobre obrigatoriedade de ciência do time de implantação, uma vez que essa obrigatoriedade é para todos os colaboradores.	12/02/2026

3. Escopo

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

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

É também obrigação de cada colaborador se manter atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação do seu Gestor, Coordenador ou da equipe de Infraestrutura e Segurança da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

4. Referências

- Norma ISO/IEC 27001:2022, requisito 5.2 e cláusula 5.1.

5. Princípios

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela CH MASTER DATA | ASTREIN pertence à referida instituição. As exceções devem ser explicitadas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais.

A CH MASTER DATA | ASTREIN, por meio da equipe de Infraestrutura e Segurança da Informação, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

6. Requisitos

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores da CH MASTER DATA | ASTREIN a fim de que a política seja cumprida dentro e fora da empresa.

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

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

Deverá constar em todos os contratos da CH MASTER DATA | ASTREIN o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

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

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente ao departamento de infraestrutura e este deverá encaminhar posteriormente ao Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê, de outros membros da diretoria e de terceiros (ex.: titulares de dados, órgãos governamentais, clientes etc.).

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

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

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

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

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

Esta PSI será implementada na CH MASTER DATA | ASTREIN por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

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

7. Das responsabilidades específicas

7.1 Dos colaboradores em geral

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

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à CH MASTER DATA | ASTREIN e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

7.2 Dos gestores de pessoas e/ou processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da CH MASTER DATA | ASTREIN.

Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da CH MASTER DATA | ASTREIN.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

7.3 Comitê de Segurança da Informação

O comitê de segurança da informação, denominado CSI, é responsável pelo Sistema de Gestão de Segurança da Informação (SGSI) e deve ser formalmente constituído por colaboradores nomeados para participar do grupo pelo período de um ano.

A composição mínima deve incluir um colaborador de cada uma das áreas:

Área
ADM
TEC-INFRA
TEC-P&D
TEC-SUP
TEC-IMPL

A liderança do CSI caberá à Diretoria de Assuntos Internos, que deverá nomear seus membros, coordenar as atividades e fazer as convocações para reuniões.

O CSI se reunirá sempre que for necessária a deliberação de mudanças que impactem a segurança da informação, incidente de segurança da informação, definições relevantes ou sob demais demandas específicas globais de segurança da informação relevantes para a CH MASTER DATA | ASTREIN.

O CSI poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

Cabe ao CSI:

- Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
- Propor e apoiar iniciativas que visem à segurança dos ativos de informação da CH MASTER DATA | ASTREIN.
- Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Comitê de Segurança da Informação.
- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.
- Apresentar as atas e os resumos das reuniões do Comitê de Segurança da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.
- Manter comunicação efetiva com a Alta Gestão sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a CH MASTER DATA | ASTREIN.
- Buscar alinhamento com as diretrizes corporativas da instituição.
- Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
- Propor alterações nas versões da PSI e a inclusão, a eliminação ou a mudança de normas complementares;
- Avaliar os incidentes de segurança e propor ações corretivas;
- Definir as medidas cabíveis nos casos de descumprimento da PSI e/ou das Normas de Segurança da Informação complementares.

8. Das disposições finais

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da CH MASTER DATA | ASTREIN, ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

A violação desta política de segurança pode acarretar medidas disciplinares ou outras medidas cabíveis na lei.

9. Auditoria regular

Todas as práticas aqui observadas devem ser avaliadas regularmente, a fim de verificar a execução das regras estabelecidas.