Política de Segurança da Informação do **smarters** - Externa

Este documento apresenta os princípios e as diretrizes de segurança da informação adotados pelo smarters. É classificado como público e pode ser livremente consultado e compartilhado.

Sumário

1. Informações do documento 2
2. Objetivo 4
3. Abrangência 4
4. Princípios 4
5. Governança E Responsabilidades 5
6. Classificação E Proteção Das Informações 6
7. Controle De Acesso 6
8. Segurança No Desenvolvimento E Nas Aplicações 7
9. Segurança De Inteligência Artificial 7
10. Segurança De Apis E Integrações 7
11. Segurança Em Nuvem 8
12. Proteção De Dados Pessoais 8
13. Criptografia 9
14. Logs, Monitoramento E Rastreabilidade 9
15. Gestão De Vulnerabilidades 9
16. Gestão De Incidentes 10
17. Backup, Restauração E Continuidade 10
18. Segurança De Fornecedores 10
19. Conscientização E Responsabilidade Dos Usuários 11
20. Gestão De Riscos 11
21. Auditoria, Conformidade E Melhoria Contínua 12
22. Exceções 12
23. Descumprimento 12
24. Indicadores De Segurança 12
25. Revisão da Política 13
26. Aprovações 13

1. Informações do documento

DATA ELABORAÇÃO:	31/08/2026		
DOCUMENTO:	Política de Segurança da Informação – Externa		
ELABORADO POR:	Aline Larroza Nery		
CÓDIGO	POL015		
APROVADO POR:	César Henrique Gnecchi Álvares de Moura		
ASSUNTO:	Política Pública		
CLASSIFICAÇÃO DO DOCUMENTO			
Público: X	**Interno**:	**Confidencial**:	**Crítica**:
HISTÓRICO DE VERSÕES			
V1	31/08/2026	Aline Larroza Nery	Criação do documento

2. Objetivo

A presente Política de Segurança da Informação estabelece os princípios, diretrizes e responsabilidades adotados pelo **smarters** para proteger as informações sob sua responsabilidade e as informações definidas no site do **smarters** (https://smarters.ai/)**.**

O **smarters** reconhece a informação como um ativo essencial para a continuidade de suas operações e para a confiança de seus clientes, parceiros e demais partes interessadas. Por essa razão, a segurança da informação deve estar incorporada às atividades de negócio, ao desenvolvimento e à evolução de suas soluções tecnológicas, incluindo plataformas de inteligência artificial, agentes conversacionais, APIs, integrações, sistemas corporativos e ambientes de computação em nuvem.

Esta Política tem como finalidade preservar a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações, bem como reduzir os riscos relacionados ao acesso, utilização, processamento, armazenamento, transmissão ou descarte inadequado dessas informações, nos termos da ISO 27.001:2022.

3. Abrangência

Esta Política aplica-se a todos os colaboradores, administradores, prestadores de serviços, parceiros e terceiros que, de alguma forma, tenham acesso às informações do site do , sistemas, aplicações, ambientes tecnológicos ou demais ativos presentes no site do **smarters**.

Sua aplicação abrange os ambientes de desenvolvimento, homologação e produção, as plataformas e agentes de inteligência artificial, APIs, integrações, ferramentas de observabilidade, bancos de dados, códigos-fonte, sistemas corporativos, dispositivos utilizados nas atividades profissionais e os ambientes de nuvem contratados pela organização.

Também estão abrangidas as informações relacionadas aos clientes, usuários, colaboradores, fornecedores e parceiros que interajam com os serviços e canais do smarters, independentemente do meio utilizado para seu armazenamento ou transmissão.

4. Princípios

O smarters estabelece que a segurança da informação deve ser conduzida de acordo com princípios que orientem tanto as decisões estratégicas quanto as atividades operacionais.

A confidencialidade deve ser preservada por meio da restrição de acesso às informações somente às pessoas, sistemas ou processos devidamente autorizados. A integridade deve ser protegida mediante mecanismos capazes de evitar alterações, exclusões ou manipulações indevidas. A disponibilidade deve ser assegurada de acordo com os requisitos de negócio e os níveis de serviço estabelecidos para os serviços críticos.

A organização também busca garantir a autenticidade das informações e das transações realizadas em seus ambientes, bem como a rastreabilidade das atividades relevantes, permitindo identificar, quando necessário, quem realizou determinada ação, quando ela ocorreu e em qual ambiente.

A segurança deve ser considerada desde a concepção das soluções, adotando-se, sempre que possível, o princípio de Security by Design. As medidas de proteção devem ser proporcionais aos riscos identificados e baseadas em uma abordagem de melhoria contínua.

5. Governança E Responsabilidades

A segurança da informação é responsabilidade de toda a organização.

A Diretoria é responsável por demonstrar comprometimento com a segurança da informação, aprovar esta Política, disponibilizar recursos adequados e assegurar que os riscos relevantes sejam considerados nas decisões estratégicas da organização.

A área responsável pela Segurança da Informação, GRC ou função equivalente deve coordenar a implementação e manutenção do Sistema de Gestão de Segurança da Informação – SGSI, acompanhar os riscos, monitorar os controles, apoiar auditorias, acompanhar incidentes e promover a melhoria contínua do sistema.

As áreas de Tecnologia e Desenvolvimento são responsáveis pela implementação e manutenção dos controles técnicos necessários à proteção dos ambientes, sistemas, aplicações, infraestrutura, códigos, integrações e informações.

Os gestores de cada área devem assegurar que seus processos estejam de acordo com esta Política, aprovando ou solicitando os acessos necessários, comunicando alterações de função e desligamentos e apoiando a identificação e tratamento dos riscos relacionados às suas atividades.

Todos os usuários são responsáveis pela utilização adequada dos recursos disponibilizados pelo **smarters** e pela proteção das informações às quais tenham acesso.

6. Classificação E Proteção Das Informações

As informações do **smarters** devem ser classificadas de acordo com sua importância, sensibilidade e impacto potencial decorrente de acesso ou divulgação indevida.

As informações poderão ser classificadas como Públicas, Internas, Confidenciais ou Críticas, cabendo aos responsáveis pela informação determinar o nível adequado de proteção.

Informações classificadas como confidenciais ou críticas devem possuir controles adicionais de acesso, armazenamento, compartilhamento e transmissão.

Credenciais, senhas, tokens, chaves de API, segredos, códigos-fonte, configurações de segurança, informações estratégicas, dados pessoais e informações protegidas contratualmente devem receber tratamento compatível com seu nível de sensibilidade.

7. Controle De Acesso

O acesso aos sistemas e informações do **smarters** deve ocorrer exclusivamente mediante autorização e de acordo com a necessidade de execução das atividades profissionais.

A organização adota os princípios de menor privilégio, necessidade de conhecimento e segregação de funções, buscando garantir que cada usuário tenha somente os acessos necessários para desempenhar suas responsabilidades.

A autenticação multifator é obrigatória para o acesso aos sistemas corporativos. Sempre que tecnicamente disponível e compatível com o risco, são utilizados também gerenciamento centralizado de identidades, autenticação federada, controle de acesso baseado em funções e mecanismos adicionais de autenticação para acessos privilegiados.

As credenciais são individuais e não devem ser compartilhadas. A concessão, alteração, revisão e revogação de acessos devem ocorrer mediante processo formal, especialmente nos casos de mudança de função ou desligamento.

Acessos privilegiados devem receber tratamento diferenciado, incluindo controles adicionais de proteção, monitoramento e rastreabilidade.

8. Segurança No Desenvolvimento E Nas Aplicações

A segurança deve fazer parte do ciclo de desenvolvimento e manutenção das soluções do **smarters**.

Os ambientes de desenvolvimento, homologação e produção devem ser segregados sempre que tecnicamente aplicável, evitando-se que alterações realizadas durante o desenvolvimento sejam disponibilizadas diretamente em produção sem os controles necessários.

As mudanças devem ser submetidas a processo de avaliação, aprovação, teste e implantação controlada. Sempre que aplicável, devem ser realizadas revisões de código, análise de dependências, testes de segurança e avaliação de vulnerabilidades.

Informações reais de produção não devem ser utilizadas em ambientes de desenvolvimento ou testes sem autorização e sem a adoção das medidas de proteção necessárias.

9. Segurança De Inteligência Artificial

Considerando a natureza dos serviços oferecidos pelo **smarters**, a segurança dos agentes de inteligência artificial constitui elemento essencial da proteção da informação.

Os agentes, modelos, prompts, configurações, bases de conhecimento, integrações e ferramentas utilizadas pelos agentes devem ser protegidos contra acesso, alteração ou utilização não autorizada.

A organização deve considerar, durante o ciclo de vida das soluções de IA, riscos relacionados à manipulação de entradas, exposição indevida de informações, prompt injection, utilização inadequada de dados, acesso indevido a ferramentas e integrações e execução de ações não autorizadas.

Alterações relevantes nos agentes ou em seus componentes devem ser controladas e rastreáveis, devendo ser realizados testes e validações antes da disponibilização em produção, de acordo com o nível de risco.

10. Segurança De Apis E Integrações

As APIs, integrações e conectores utilizados pelas soluções do **smarters** devem possuir mecanismos de autenticação, autorização e proteção compatíveis com sua criticidade.

Tokens, chaves de API, credenciais e demais segredos utilizados nas integrações devem ser armazenados de maneira segura e não devem ser inseridos diretamente no código-fonte ou disponibilizados de forma inadequada.

As integrações devem ser monitoradas e, quando aplicável, possuir mecanismos de controle de requisições, validação de entradas, criptografia, registro de eventos e gerenciamento do ciclo de vida das credenciais.

11. Segurança Em Nuvem

Os serviços de nuvem utilizados pelo **smarters** devem ser selecionados e administrados considerando requisitos de segurança, disponibilidade, continuidade, privacidade, conformidade e desempenho.

A organização deve avaliar os riscos associados aos provedores de nuvem e aos serviços utilizados, estabelecendo critérios para contratação, utilização, monitoramento e encerramento desses serviços.

A infraestrutura em nuvem deve possuir controles adequados de identidade e acesso, configuração segura, proteção de dados, criptografia, registro de eventos, monitoramento, backup e recuperação.

A responsabilidade pela segurança deve observar o modelo de responsabilidade compartilhada aplicável a cada serviço contratado.

12. Proteção De Dados Pessoais

O **smarters** deve tratar dados pessoais de acordo com a legislação aplicável, especialmente a Lei Geral de Proteção de Dados Pessoais – LGPD, além das obrigações contratuais assumidas com clientes e parceiros.

O tratamento de dados deve observar os princípios de finalidade, necessidade, segurança, prevenção, transparência e responsabilização.

Os dados pessoais devem ser protegidos contra acesso, utilização, alteração, divulgação, perda ou destruição não autorizada.

Quando houver tratamento de dados pessoais por fornecedores ou serviços de terceiros, devem ser considerados os requisitos de segurança e privacidade aplicáveis.

13. Criptografia

O **smarters** deve utilizar mecanismos de criptografia sempre que necessários para reduzir os riscos de exposição, interceptação ou acesso indevido às informações.

A criptografia deve ser considerada especialmente para informações confidenciais, dados pessoais, credenciais, chaves, backups e informações transmitidas por redes não confiáveis.

As chaves criptográficas devem ser protegidas durante todo o seu ciclo de vida, incluindo geração, armazenamento, utilização, renovação, revogação e descarte.

14. Logs, Monitoramento E Rastreabilidade

O **smarters** deve manter mecanismos de registro e monitoramento capazes de identificar eventos relevantes relacionados à segurança da informação.

Sempre que aplicável, devem ser registrados eventos de autenticação, falhas de acesso, utilização de privilégios administrativos, alterações de configuração, atividades relevantes em APIs, eventos de segurança e demais operações consideradas críticas.

Os registros devem possuir proteção contra alteração ou exclusão indevida e devem ser mantidos pelo período definido de acordo com requisitos legais, contratuais, operacionais e de segurança.

Os mecanismos de observabilidade também devem apoiar a identificação de comportamentos anômalos, falhas e possíveis incidentes de segurança.

15. Gestão De Vulnerabilidades

O **smarters** deve manter processo para identificar, avaliar, priorizar e tratar vulnerabilidades existentes em seus sistemas, aplicações, infraestrutura e componentes tecnológicos.

A priorização deve considerar a criticidade do ativo, a gravidade da vulnerabilidade, a possibilidade de exploração, a exposição do ambiente e o impacto potencial para o negócio.

Vulnerabilidades críticas e de alto risco devem ser tratadas prioritariamente, de acordo com os prazos e critérios definidos pela organização.

16. Gestão De Incidentes

Eventos que possam comprometer a confidencialidade, integridade ou disponibilidade das informações devem ser avaliados e, quando caracterizados como incidentes, tratados de acordo com o processo de resposta a incidentes do **smarters**.

O tratamento deve contemplar, conforme aplicável, identificação, registro, classificação, contenção, investigação, erradicação, recuperação e encerramento.

Quando necessário, evidências relacionadas ao incidente devem ser preservadas de forma a garantir sua integridade e rastreabilidade.

Incidentes que envolvam dados pessoais devem também ser avaliados sob a perspectiva da legislação de proteção de dados e das obrigações contratuais aplicáveis.

Após incidentes relevantes, devem ser identificadas causas, oportunidades de melhoria e medidas preventivas para evitar recorrências.

17. Backup, Restauração E Continuidade

O **smarters** deve manter mecanismos de backup e recuperação compatíveis com a criticidade de seus sistemas e informações.

Os backups devem ser protegidos contra acesso ou alteração não autorizada e devem possuir critérios definidos de frequência, retenção e proteção.

Testes periódicos de restauração devem ser realizados para verificar se os mecanismos de recuperação são efetivos.
Os serviços críticos devem possuir requisitos de continuidade definidos de acordo com os impactos potenciais ao negócio, considerando infraestrutura, aplicações, integrações, serviços de terceiros e recursos necessários à operação.

Quando aplicável, devem ser definidos e monitorados objetivos de recuperação, incluindo RTO e RPO.

18. Segurança De Fornecedores

Fornecedores e parceiros que possam acessar informações, sistemas ou ambientes do **smarters** devem ser avaliados de acordo com o risco associado ao serviço contratado.

A avaliação poderá considerar aspectos relacionados à segurança da informação, proteção de dados, disponibilidade, continuidade, histórico de incidentes, certificações, localização do processamento e controles técnicos e administrativos.

Os contratos com fornecedores críticos devem estabelecer requisitos de segurança e proteção de informações compatíveis com os riscos identificados.

19. Conscientização E Responsabilidade Dos Usuários

A segurança da informação depende também da atuação consciente das pessoas.

O **smarters** deve promover ações periódicas de conscientização e treinamento sobre segurança, proteção de dados, engenharia social, phishing, utilização adequada dos recursos tecnológicos, proteção de credenciais e utilização segura de ferramentas de inteligência artificial.

Todos os usuários devem comunicar imediatamente situações que possam representar risco ou incidente de segurança.

É proibido utilizar recursos corporativos para atividades que possam comprometer a segurança, a reputação ou a continuidade das operações da organização.

20. Gestão De Riscos

O **smarters** deve manter processo formal de identificação, análise, avaliação e tratamento dos riscos de segurança da informação.

Os riscos devem ser avaliados considerando sua probabilidade de ocorrência e seu impacto potencial sobre os objetivos da organização.

De acordo com o resultado da avaliação, os riscos poderão ser evitados, reduzidos, transferidos ou aceitos, observando-se os critérios e níveis de autoridade estabelecidos pela organização.

Riscos relevantes devem possuir tratamento, responsável definido e acompanhamento até sua conclusão ou aceitação formal.

21. Auditoria, Conformidade E Melhoria Contínua

A conformidade com esta Política e com os controles estabelecidos pelo SGSI deve ser acompanhada periodicamente por meio de indicadores, auditorias, avaliações, testes e análises de riscos.

Não conformidades identificadas devem ser registradas, analisadas e tratadas de acordo com o processo de melhoria contínua.

O **smarters** deve utilizar os resultados de auditorias, incidentes, avaliações de riscos, testes e demais fontes de informação para aprimorar continuamente seus controles de segurança.

22. Exceções

Qualquer exceção aos requisitos estabelecidos nesta Política deve ser formalmente justificada, avaliada quanto aos riscos envolvidos e aprovada pela autoridade competente.

A exceção deve possuir prazo de validade, responsável definido e, quando necessário, controles compensatórios.

Exceções não devem ser utilizadas como mecanismo permanente para evitar a implementação de controles necessários à proteção das informações.

23. Descumprimento

O descumprimento desta Política poderá resultar na suspensão ou revogação de acessos, aplicação de medidas administrativas ou disciplinares, medidas contratuais e, quando aplicável, adoção das providências legais cabíveis.

A aplicação das medidas deverá considerar a natureza e gravidade da ocorrência, seus impactos, a existência de dolo ou negligência e eventual reincidência.

24. Indicadores De Segurança

O smarters mantém indicadores de desempenho de segurança da informação, com meta, periodicidade de apuração e responsável definidos para cada um.

A eficácia desta Política é acompanhada por esses indicadores, cujos resultados são analisados pelo Comitê de Segurança da Informação, consolidados na análise crítica pela direção e utilizados para orientar ações de melhoria.

25. Revisão da Política

Esta Política é revisada anualmente ou sempre que houver mudança material, como parte do ciclo de análise crítica do SGSI (ISO/IEC 27001:2022).

26. Aprovações

O presente Documento foi aprovado pelo CISO, pela área de tecnologia e pela Diretoria (Board) da empresa, tendo sido analisado em todos os seus termos e fundamentos.

São Paulo, 31 de agosto de 2026.

Aprovação dos membros do Board:

Pietro Buquera Bujaldon

César Henrique Gnecchi Álvares de Moura

Aprovação Gestão de Segurança e Desenvolvimento:

César Henrique Gnecchi Álvares de Moura
CISO

Felipe Aguiar

POL015 - Política de Segurança da Informação - Externa_V1 - Google Docs

Relatório de auditoria final 2026-09-01

Criado em:	2026-08-31
Por:	Contratos smarters (contratos@smarte.rs)
Status:	Assinado
ID da transação:	CBJCHBCAABAABUMHsDm9bKJcVsJ6DPCx2DSFKNxExnrX

Histórico

Documento criado por Contratos smarters (contratos@smarte.rs)
2026-08-31 - 23:16:15 GMT

Documento enviado por email para pietro@smarters.ai para assinatura
2026-08-31 - 23:16:21 GMT

Documento enviado por email para cesar@smarters.ai para assinatura
2026-08-31 - 23:16:22 GMT

Documento enviado por email para felipe@smarters.ai para assinatura
2026-08-31 - 23:16:22 GMT

Email visualizado por cesar@smarters.ai
2026-08-31 - 23:17:53 GMT

O signatário cesar@smarters.ai inseriu o nome Cesar Henrique Gnecchi Alvares de Moura ao assinar
2026-08-31 - 23:18:17 GMT

Documento assinado eletronicamente por Cesar Henrique Gnecchi Alvares de Moura (cesar@smarters.ai)
Data da assinatura: 2026-08-31 - 23:18:19 GMT - Fonte da hora: servidor - Aparência da assinatura selecionada: TIPO

Email visualizado por pietro@smarters.ai
2026-08-31 - 23:23:36 GMT

O signatário pietro@smarters.ai inseriu o nome Pietro Bujaldon ao assinar
2026-08-31 - 23:24:10 GMT

Documento assinado eletronicamente por Pietro Bujaldon (pietro@smarters.ai)
Data da assinatura: 2026-08-31 - 23:24:12 GMT - Fonte da hora: servidor - Aparência da assinatura selecionada: IMAGEM

Email visualizado por felipe@smarters.ai

2026-09-01 - 1:08:43 GMT

O signatário felipe@smarters.ai inseriu o nome Felipe Aguiar ao assinar

2026-09-01 - 1:09:01 GMT

Documento assinado eletronicamente por Felipe Aguiar (felipe@smarters.ai)

Data da assinatura: 2026-09-01 - 1:09:03 GMT - Fonte da hora: servidor - Aparência da assinatura selecionada: TIPO

Contrato finalizado.

2026-09-01 - 1:09:03 GMT