csptech.com.br
+55 21 2263 7660
+55 11 97376 1007

Sistema de Gestão

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO EXTERNA

SG-PO-001.1

1. Objetivos

A Política de Segurança da Informação Externa tem como objetivo o cumprimento da transparência em relação às partes interessadas sobre as atividades relacionadas à Segurança da Informação executadas pela CSP Tech, bem como orientar aos fornecedores, prestadores de serviços, parceiros comerciais e quaisquer terceiros que tenham acesso a dados, sistemas, instalações ou informações da CSP TECH, quanto ao mínimo de Segurança da Informação requerido deles no tratamento das informações referentes à CSP Tech, assegurando a confidencialidade, integridade, disponibilidade e conformidade legal.

2. Referência

- ABNT NBR ISO/IEC 27001:2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação – Requisitos;
- ABNT NBR ISO/IEC 27002:2022 - Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação.

3. Abrangência

Esta Política se aplica a todos os ativos de informação da CSP Tech, incluindo dados, sistemas, aplicativos, dispositivos e redes. A esta Política estão obrigados todos os contratados, parceiros e terceiros que:

- Acessem informações da CSP Tech, em meio físico ou digital;
- Tenham acesso a sistemas corporativos, redes ou recursos tecnológicos;
- Prestem serviços que possam impactar a segurança da informação e proteção de dados.

csptech.com.br
+55 21 2263 7660
+55 11 97376 1007

4. Termos e Definições

CONFIDENCIALIDADE: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável;

DADO PESSOAL SENSÍVEL: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

DISPONIBILIDADE: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

INTEGRIDADE: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

SEGURANÇA DA INFORMAÇÃO: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

INCIDENTE DE SEGURANÇA DA INFORMAÇÃO: É um evento de segurança ou conjunto de eventos confirmados que impactem a disponibilidade, confidencialidade e integridade de um ativo de informação, assim como qualquer violação desta política.

BACKUP: É a cópia de segurança de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais.

TITULAR DO DADO: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

PROVEDOR EXTERNO: empresa ou entidade que fornece produtos, serviços ou funções para outra empresa, mas que é legalmente e operacionalmente separada dela.

5. PRINCÍPIOS

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para a CSP Tech ou seus clientes. Ela pode estar guardada para uso restrito ou exposta ao cliente para consulta ou manuseio. Pode estar impressa ou escrita, pode ser falada, transmitidas por e-mails ou meios eletrônicos. Independentemente da forma apresentada ou o meio pelo qual a informação é compartilhada ou armazenada, a informação é o maior ativo da CSP Tech e de seus clientes, e, por isso, essencial ao negócio. Sendo assim, deverá ser devidamente protegida e utilizada de modo ético e seguro, garantindo confiabilidade através da proteção da:

- Confidencialidade: garantir que a informação não seja revelada ou esteja disponível para indivíduos, entidades e processos não autorizados;
- Integridade: garantir a salvaguarda da exatidão e totalidade da informação e dos métodos de processamento;
- Disponibilidade: garantir que a informação esteja sempre acessível e disponível quando necessário e somente quando autorizado.
- Legalidade: garantir o cumprimento da legislação aplicável, incluindo a LGPD (Lei nº 13.709/2018).

6. Diretrizes

6.1.1 Para fornecedores Externo:

As diretrizes contempladas na Norma de DUE DILIGENCE complementam esta política.

O Acordo de Responsabilidade e Confidencialidade da Informação firmado com o provedor externo deve contemplar todas as diretrizes desta política que são aplicáveis ao prestador de serviço.

Para os serviços terceirizados de Tecnologia da Informação, este Acordo de Responsabilidade e Confidencialidade da Informação deve ser estendido por toda a cadeia de suprimento do provedor externo.

O Procedimento Gestão de Provedor Externo, os questionários de avaliação e reavaliação de fornecedor, apresentam o processo que viabilizam esta política.

Esta PSI deverá ser compartilhada com todos os fornecedores da CSP Tech.

6.1.2 Para uso dos ativos

Para que prestadores de serviços possam acessar informações da CSP Tech por meio das ferramentas da organização, é necessário que seus dispositivos móveis estejam em conformidade com os requisitos de segurança, incluindo antivírus, anti-malware e demais softwares de proteção, quando aplicável.

Cada usuário é responsável pela proteção dos dispositivos físicos contendo informação da CSP Tech que estão sob sua guarda.

Mídias removíveis de qualquer tipo que contenha dados e informações confidenciais da CSP Tech, quando não forem mais utilizadas, devem ser apagadas ou destruídas por procedimentos que garantam que essas informações não possam ser recuperadas.

Quando materiais impressos forem destruídos, eles devem ser destruídos de forma segura, utilizando mecanismos como trituração.

A CSP Tech poderá, a qualquer tempo, revogar credenciais de acesso concedidas em virtude do descumprimento desta política ou a seu exclusivo critério, a fim de proteger os dados com acesso concedido.

6.1.3 Para o Controle de Acesso

O acesso às informações da CSP Tech será concedido apenas mediante necessidade comprovada e autorização formal.

Manter e utilizar senhas fortes (no mínimo 8 caracteres), e duplo fator de autenticação nos softwares, caso esteja disponível.

As contas de acesso devem ser individuais e intransferíveis e é proibido compartilhar credenciais (senhas, tokens, certificados).

Os colaboradores sob controle do fornecedor com acesso aos dados da CSP Tech, incluindo qualquer terceiro contratado por ele, devem estar sujeitos a uma obrigação de confidencialidade.

Deve existir um registro atualizado dos usuários ou perfis de usuários que tenham acesso privilegiado ao sistema de informações.

Os dados pessoais armazenados no fornecedor ou fora de suas dependências devem estar sujeitos a um procedimento de autorização e não devem ser acessíveis a qualquer pessoa que não seja o pessoal autorizado. Que este conteúdo, por exemplo, esteja criptografado.

6.1.4 Para Backups

Backups, cópias ou extrações de dados da CSP Tech só podem ocorrer mediante autorização expressa.
Todo fornecedor contratado pela CSP Tech deve possuir a devida proteção de dados, assegurar a continuidade das operações assim como possibilitar a restauração após um sinistro.
O registro dos esforços de restauração de dados deve conter no mínimo: a pessoa responsável, uma descrição dos dados restaurados e os dados que foram restaurados manualmente.

A CSP Tech deve estar ciente do local onde essas cópias de segurança são mantidas pelo fornecedor, o tempo de retenção, bem como cada fornecedor permite a exclusão dessas informações retidas.

6.1.5 Para Gestão de Evento

O fornecedor contratado pela CSP Tech deve deixar claro os critérios sobre se, quando e como as informações de registros podem ser disponibilizadas ou utilizadas, além de informar como garante a proteção desses registros para evitar a visibilidade dessas informações por pessoas não autorizadas, bem como inibir a exclusão desses registros antes do tempo.

O fornecedor deve determinar um tempo de retenção dos registros de eventos (logs) para garantir que a informação é devidamente apagada depois de um certo tempo.

6.1.6 Para Gestão de Incidentes

Qualquer incidente de segurança ou suspeita de violação deve ser comunicado imediatamente à área de Governança da CSP Tech, por meio do canal de denúncias: https://csptech.clickcompliance.com/reporting-channel.

Em todo incidente de segurança da informação ou suspeita, o fornecedor deve cooperar com a CSP Tech nas investigações e medidas corretivas.

Todo incidente de segurança da informação deve provocar uma análise crítica pelo fornecedor como parte de seu processo de gestão de incidentes de segurança da informação, para determinar se ocorreu uma violação de dados que envolvam dados pessoais.

6.1.7 Para conformidade com requisitos legais e contratuais

Deve-se ter certeza que os dados, incluindo todas as suas cópias e backups, estejam armazenados somente em localizações geográficas permitidas por contrato, SLA e/ou regulação.

Os fornecedores devem permitir que a CSP Tech monitore o desempenho do(s) serviço(s) contratado(s).

É de propriedade da CSP Tech, todos os “designs”, criações ou procedimentos desenvolvidos por qualquer funcionário ou prestador de serviço da CSP Tech cujo contrato de trabalho ou de prestação de serviços tenha por objeto a pesquisa ou atividade inventiva, ou resulte esta da natureza dos serviços para os quais foi contratado (Lei de Propriedade Intelectual – Lei nº 9.279/96 – Art. 88).

Os fornecedores e colaboradores da CSP Tech devem assegurar que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

6.1.8 Para Análise Crítica da Segurança da Informação

Todo fornecedor contratado pela CSP Tech deve comprovar que a segurança da informação é implementada e operada de acordo com as principais normas de segurança da informação, garantindo o mínimo exigido pelo contrato.

O fornecedor deve permitir, quando solicitado, que a CSP Tech realize auditorias de Segurança da Informação.

Nos casos em que auditorias individuais pela CSP Tech forem impraticáveis ou possam aumentar os riscos à segurança, convém que o fornecedor disponibilize, antes da assinatura ou durante um contrato, evidência independente de que a segurança da informação é implementada e operada de acordo com as políticas e procedimentos do mesmo.

Convém que uma auditoria independente relevante, selecionada pelo fornecedor, seja normalmente um método aceitável para atender ao interesse da CSP Tech na análise crítica de suas operações, desde que uma transparência suficiente seja provida.

6.1.9 **Para a Proteção de Dados**

6.1.9.1 Consentimento e Escolha

Que o fornecedor forneça à CSP Tech os meios para capacitá-la a atender à sua obrigação de facilitar o exercício dos direitos dos titulares de dados pessoais a acessar, corrigir e/ou apagar seus respectivos dados.

6.1.9.2 Legitimidade e Especificação da Finalidade

Informações classificadas como confidenciais só podem ser utilizadas para a finalidade contratual.

Os dados pessoais tratados sob um contrato não devem ser utilizados para qualquer outra finalidade que não para o cumprimento do objeto do contrato e restrito ao seu propósito.

Os dados pessoais não devem ser utilizados para fins de marketing e publicidade pelo fornecedor sem o consentimento expresso.

Convém que este consentimento não seja uma condição de recebimento do serviço.

6.1.9.3 Limitação da Coleta

Não devem ser coletados dados pessoais indiscriminadamente. Tanto a quantidade quanto o tipo de dados pessoais coletados devem estar limitados ao necessário para cumprir o(s) objetivo(s) especificado(s) pela CSP Tech e/ou objeto contratado.

6.1.9.4 Minimização

Os arquivos e documentos temporários devem ser apagados ou destruídos dentro de um período especificado e documentado.

6.1.9.5 Limitação de Uso, Retenção e Divulgação

O fornecedor deve notificar a CSP Tech, no prazo de 24 horas, de qualquer solicitação recebida de autoridade competente para divulgação dos dados

pessoais para cumprimento de lei ou intimação judicial, a menos que esta notificação seja proibida.
As divulgações dos dados pessoais a terceiros devem ser registradas, incluindo qual dado pessoal foi divulgado, a quem e em qual momento.

6.1.9.6 Precisão e Qualidade

O fornecedor deve possibilitar meios para a CSP Tech assegurar aos titulares dos dados pessoais:

- tratamento preciso, completo, atualizado, adequado e pertinente para o objetivo de uso;
- a confiabilidade dos dados pessoais recolhidos a partir de uma fonte que não seja o titular de dados pessoais antes de ser tratado;
- por meios apropriados, a validade e a exatidão das reivindicações feitas pelo titular de dados pessoais antes de fazer qualquer alteração nos dados pessoais (a fim de assegurar que as alterações sejam devidamente autorizadas, quando for apropriado fazê-lo;
- procedimentos de coleta de dados pessoais para ajudar a garantir a precisão e a sua qualidade;
- mecanismos de controle para verificar periodicamente a precisão e a qualidade dos dados pessoais coletados e armazenados.

6.1.9.7 Abertura, Transparência e Notificação

Dados pessoais tratados em nome da CSP Tech devem observar a LGPD e demais normas vigentes. O uso de subcontratados pelo fornecedor para tratar os dados pessoais deve ser informado e autorizado à CSP Tech antes da sua utilização.
Também é necessário que seja informado, em tempo hábil, sobre quaisquer alterações pretendidas a este respeito, de modo que a CSP Tech tenha a possibilidade de contestar estas alterações ou encerrar o contrato.

Os contratos entre o fornecedor e quaisquer subcontratados que tratam dados pessoais devem especificar as medidas técnicas e organizacionais mínimas que atendam à segurança da informação e às obrigações de proteção dos dados pessoais do fornecedor.
É obrigatório que estas medidas não sejam sujeitas à redução unilateral pelo subcontratado.
É necessário que as informações divulgadas também incluam os países em que os subcontratados podem tratar os dados pessoais e os meios pelos quais os subcontratados são obrigados a atender ou exceder às obrigações do fornecedor. Em caso de não inclusão, entende-se que só são tratadas no Brasil.

6.1.9.8 Acesso e Participação Individual

O fornecedor deve possibilitar meios para a CSP Tech permitir aos titulares de dados pessoais:

- a capacidade de acessar e analisar criticamente os seus dados pessoais, desde que a sua identidade seja primeiramente autenticada com um nível apropriado de garantia e tal acesso não seja proibido pela lei aplicável;
- questionar a exatidão e a integridade dos dados pessoais e que sejam aperfeiçoados, corrigidos ou removidos conforme apropriado e possível no contexto específico;
- fornecer qualquer emenda, correção ou remoção sempre que solicitados;
- exercer seus respectivos direitos de forma simples, rápida e eficiente, o que não implica atrasos ou custos indevidos.

6.1.9.9 Responsabilização

É necessário que os colaboradores sob controle do provedor externo com acesso aos dados pessoais da CSP Tech estejam sujeitos a uma obrigação de confidencialidade.

csptech.com.br
+55 21 2263 7660
+55 11 97376 1007

O provedor externo deve cumprir integralmente esta Política e cláusulas contratuais relacionadas e, também, garantir que seus colaboradores, subcontratados e parceiros também cumpram estas diretrizes.

O provedor externo assumirá a toda a responsabilidade civil e criminal por violações de segurança decorrentes de sua atuação.

Os dados pessoais armazenados pelo provedor externo ou fora de suas dependências devem estar sujeitos a um procedimento de autorização e não devem ser acessíveis a qualquer pessoa que não seja o pessoal autorizado. Que este conteúdo, por exemplo, esteja criptografado.

Que o provedor externo atribua um ponto de contato para uso da CSP Tech referente ao tratamento de dados pessoais.

O provedor externo deve notificar prontamente a CSP Tech no caso de qualquer acesso não autorizado aos dados pessoais ou acesso não autorizado aos equipamentos ou instalações que resulte em risco de perda, divulgação ou alteração dos dados pessoais.

No caso de ocorrência de uma violação de dados que envolva dados pessoais, convém que um registro seja mantido com uma descrição do incidente, o período temporal, as consequências do incidente, o nome da pessoa que reportou o incidente, a quem o incidente foi reportado, as medidas tomadas para resolver o incidente (incluindo a pessoa responsável e os dados recuperados) e o fato de que o incidente resultou em perda, divulgação ou alteração dos dados pessoais.

Também, é obrigatório que o provedor externo mantenha registro que inclua uma descrição dos dados comprometidos, se forem conhecidos; e se notificações foram realizadas, quais as medidas tomadas para notificar a CSP Tech e/ou as agências reguladoras.

Para fins de descarte ou reuso seguro, os equipamentos que contêm mídia de armazenamento que possivelmente possam conter dados pessoais devem ser tratados.

O provedor externo deve disponibilizar as informações necessárias para assegurar à CSP Tech que os dados pessoais tratados sob um contrato sejam apagados (pelo provedor externo e por qualquer um dos seus subcontratados) de onde quer que estejam armazenados, inclusive para fins de cópia de segurança (backup) e continuidade do negócio, assim que não sejam mais necessários para as finalidades específicas do contrato firmado pela CSP Tech.
Os dados pessoais devem ser destruídos de forma segura (desvinculação, sobregravação, desmagnetização, destruição ou outras formas de apagamento), inviabilizando a restauração de qualquer possível informação contida neles.

6.1.9.10. Transparência e Compartilhamento

O provedor externo deve especificar e documentar os países em que, possivelmente, os dados pessoais podem ser armazenados.
Os provedores externos devem identificar as identidades dos países decorrentes do uso de fornecedores subcontratados sejam incluídas. Quando acordos contratuais específicos se aplicarem à transferência internacional de dados, como Cláusulas de Contrato-Modelo, Regras Corporativas Vinculativas ou Regras de Privacidade Internacionais, convém que os acordos e os países ou circunstâncias em que estes acordos se aplicam também sejam identificados.
O provedor externo deve informar, em tempo hábil, ou sem demora indevida, à CSP Tech sobre quaisquer alterações pretendidas a este respeito, de modo que a CSP Tech tenha a capacidade de contestar estas alterações ou encerrar o contrato.

6.10. Uso de Recursos Tecnológicos

Os dispositivos próprios (BYOD) dos provedores externos só podem ser utilizados para acesso aos ambientes corporativos da CSP Tech mediante autorização prévia.
Quando autorizado a acessar os ambientes corporativos da CSP Tech, é vedado instalar softwares não autorizados nos ambientes corporativos.

Quando autorizado a acessar os ambientes corporativos da CSP Tech, o provedor externo deve cuidar para que o tráfego de informações deve ocorrer por canais seguros (VPN, criptografia, etc.).

7. Penalidades

A CSP Tech estabeleceu para toda e qualquer infração à Política e demais Normas de Segurança da Informação que a suportam, que deve ser aberto um incidente de segurança da informação com comunicação obrigatória ao Comitê de Segurança da Informação. Por conseguinte, o incidente é apurado através de procedimento interno, que é conduzido pelo CSI com a participação do responsável da área em que se encontra alocado o profissional que cometeu a infração, ou responsável pela contratação do prestador.

Caso o CSI julgue cabível, o colaborador ou terceiro envolvido poderá, enquanto durar o processo de apuração interna, ser afastado da função ou ser suspenso.

Ao colaborador ou terceiro suspeito de cometer violações à Política e/ou Normas de Segurança da Informação, é assegurado tratamento justo e correto, sendo que toda e qualquer medida resultante de sua infração deverá ser aplicada com proporcionalidade à ocorrência com base no Código de Ética e Conduta, Termo de Confidencialidade, Política e Normas de Segurança da Informação da CSP Tech e legislações vigentes.

8. Vigência e Atualização

Esta Política entra em vigor na data de sua publicação e poderá ser revisada periodicamente pela CSP Tech, sem prejuízo das obrigações já assumidas.

Versão	Data da Revisão	Histórico	Editado por
1.0	06/04/2026	Elaboração do Documento	Governança e Jurídico