SG-PL-007- Política de Segurança da Informação Externa

:hiperstream

Nome:	SG-PL-007- Política de Segurança da Informação Externa	**Data de vigência da primeira versão:**	**18/05/2022**
Versão:	**1.1**	**Data da última revisão:**	16/05/2024
Responsável:	Daniel de Mello Scarparo		
Área Responsável:	Segurança da Informação		
Descrição:	A Política de Segurança da Informação Externa tem como objetivo o cumprimento da transparência em relação aos clientes sobre as atividades relacionadas à Segurança da Informação executadas pela Hiperstream, bem como orientar aos fornecedores quanto ao mínimo de Segurança da Informação requerido deles no tratamento das informações referentes à Hiperstream.		
Aplicabilidade:	Esta política aplica-se a todos os colaboradores, clientes e fornecedores externos à Hiperstream.		

Sumário

1. Objetivo, Abrangência e Definições

1.1. Objetivo

A Política de Segurança da Informação Externa tem como objetivo o cumprimento da transparência em relação aos clientes sobre as atividades relacionadas à Segurança da Informação executadas pela Hiperstream, bem como orientar aos fornecedores quanto ao mínimo de Segurança da Informação requerido deles no tratamento das informações referentes à Hiperstream.

1.2. Abrangência

Esta política aplica-se a todos os colaboradores, clientes e fornecedores externos à Hiperstream.

1.3. Definições

Termo	Definição
Colaborador (es)	Qualquer pessoa física ou jurídica que, por relação contratual tácita ou expressa, colabora com a consecução dos objetivos sociais da empresa ou que tenha tido ou não acesso franqueado à Informação, independentemente de sua classificação. Nesta categoria de pessoas incluem-se, sem se limitar a estes, os empregados, gestores, acionistas, fornecedores e prestadores de serviços da Hiperstream.
Gestor da Informação	O colaborador designado para realizar a gestão da Informação, sendo responsável pela validação, liberação e cancelamento dos acessos à Informação
Informação	Conjunto de conhecimentos e dados relacionados aos negócios da empresa, seus clientes, fornecedores, colaboradores e demais stakeholders, incluindo, sem limitação, de natureza comercial, técnica, financeira, pessoal, de marketing ou produto, independente do repositório da informação. A Informação pode ser classificada como Confidencial, de Uso Interno ou Pública.
Repositórios da Informação	Qualquer recurso físico ou lógico utilizado no armazenamento ou manuseio da informação. Enquadram-se nesse conceito documentos em papel, arquivos físicos, computadores, servidores, programas de computador, bases de dados, linhas telefônicas, discos, dvd´s, cd´s, disquetes, *pen-drives*, dentre outros.
Usuário	Qualquer pessoa autorizada a acessar, ler, responder, inserir, alterar ou eliminar determinada informação.
Ativo	Tudo aquilo que possui algum valor para a Hiperstream. Ativos podem ser humanos, de tecnologia da informação, físicos, dentre outros, como a própria informação.

Confidencialidade	Garantia de que o acesso à informação esteja disponível somente para pessoas, entidades ou processos autorizados
Integridade	Garantia de que a informação seja mantida em seu estado original, exata e completa
Disponibilidade	Garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
Autenticidade	Garantia de que, no processo de comunicação da informação, os criadores ou remetentes não possam ser forjado ou se passem por terceiros.
Legalidade	Garantia de que a informação seja produzida, mantida e divulgada de acordo com a legislação vigente.

2. Princípios fundamentais da Segurança da Informação

A Gestão da Segurança da Informação da Hiperstream é embasada nos seguintes princípios fundamentais:

- Dever de estrito cumprimento do disposto na política de segurança da informação interna por todos os colaboradores e usuários que porventura tiverem acesso à Informação;
- Adoção de política de melhoria contínua, baseada no monitoramento constante (planejamento vs. checagem de resultados) e aperfeiçoamento das políticas de segurança da informação interna e externa e dos controles associados sempre que julgado necessário;
- Avaliação sistemática e periódica dos riscos de Segurança da Informação de modo a acompanhar sua constante evolução e aperfeiçoar os controles existentes;
- Resguardo dos procedimentos relativos à política de segurança da informação interna através da segregação de funções, de forma que as atividades associadas à implementação não sejam executadas e controladas pelo mesmo colaborador, ou pela mesma equipe de colaboradores;
- Dever de cumprimento da legislação aplicável de conduta pautada na adoção dos mais altos preceitos morais e éticos relativos ao tratamento das Informações, da Hiperstream ou de terceiros;
- Compatibilidade desta Política e da Política de Segurança da Informação interna com os demais sistemas de gestão da empresa.

3. Diretrizes

Descrição das diretrizes das políticas que compõe esta política de segurança da informação externa.

3.1. Política para Uso dos Ativos

A criação de material impresso exibindo dados pessoais da Hiperstream deve ser evitada e, quando necessária, restrita e previamente consentida pela Hiperstream.

Quando materiais impressos forem destruídos, eles devem ser destruídos de forma segura, utilizando mecanismos como corte transversal, trituração, incineração ou desfibramento por exemplo.

3.2. Política para Transferência de Informações

Os dados pessoais transmitidos por redes públicas de transmissão de dados devem ser criptografados antes da transmissão.

Os dados pessoais transmitidos utilizando uma rede de transmissão de dados devem estar sujeitos a controles apropriados, projetados para assegurar que os dados alcancem o seu destino pretendido.

3.3. Política de Controle de Acesso

Os colaboradores sob controle do fornecedor com acesso aos dados da Hiperstream, incluindo qualquer terceiro contratado pelo mesmo, devem estar sujeitos a uma obrigação de confidencialidade.

Devem existir procedimentos para registro e cancelamento do usuário que tratem a situação quando o controle de acesso do usuário estiver comprometido, como a corrupção ou o comprometimento de senhas ou outros dados de registro do usuário (por exemplo, como resultado de uma divulgação involuntária).

Deve existir um registro atualizado dos usuários ou perfis de usuários que tenham acesso autorizado 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.

3.4. Política de Backup

Todo fornecedor contratado pela Hiperstream 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 Hiperstream 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.

3.5. Política de Gestão de Evento

O fornecedor contratado pela Hiperstream 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.

3.6. Política de Gestão de Incidentes

O fornecedor deve cooperar com a Hiperstream em todo incidente de segurança da informação, como por exemplo para determinar se ocorreu uma violação de dados que envolva dados pessoais.

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.

O fornecedor tem a obrigação de informar a Hiperstream no caso de um incidente de segurança relacionado à Dados Pessoais conforme os prazos estabelecidos pela ANPD (Autoridade Nacional de Proteção de Dados).

3.7. Política de 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 Hiperstream monitore o desempenho do(s) serviço(s) contratado(s).

3.8. Política de Análise Crítica da Segurança da Informação

Todo fornecedor contratado pela Hiperstream 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 em contrato.

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

Nos casos onde auditorias individuais pela Hiperstream forem impraticáveis ou possam aumentar os riscos à segurança, convém que o fornecedor disponibilize, antes da assinatura e 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 Hiperstream na análise crítica de suas operações, desde que uma transparência suficiente seja provida.

3.9. Política para Proteção de Informação Pessoal

3.9.1. Consentimento e Escolha

O Fornecedor deve fornecer à Hiperstream 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.

3.9.2. Legitimidade e Especificação da Finalidade

Os dados pessoais tratados sob um contrato não devem ser utilizados para qualquer finalidade independente das instruções da Hiperstream.

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.

3.9.3. 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 Hiperstream.

3.9.4. Minimização

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

3.9.5. Limitação de Uso, Retenção e Divulgação

O fornecedor deve notificar a Hiperstream, de acordo com qualquer procedimento e períodos de tempo acordados no contrato, de qualquer solicitação legalmente vinculativa para divulgação dos dados pessoais por uma autoridade competente para cumprimento da lei, a menos que esta divulgação seja proibida.

As divulgações dos dados pessoais a terceiros devem ser registradas, incluindo qual dado pessoal foi divulgado, a quem e em qual momento.

3.9.6. Precisão e Qualidade

O fornecedor deve possibilitar meios para a Hiperstream 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 qualidade;
- Mecanismos de controle para verificar periodicamente a precisão e a qualidade dos dados pessoais coletados e armazenados.

3.9.7. Abertura, Transparência e Notificação

O uso de subcontratados pelo fornecedor para tratar os dados pessoais deve ser divulgado à Hiperstream antes da sua utilização. Que também seja informado, em tempo hábil, sobre quaisquer alterações pretendidas a este respeito, de modo que a Hiperstream tenha a capacidade 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. Que estas medidas não sejam sujeitas à redução unilateral pelo subcontratado.

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.

3.9.8. Acesso e Participação Individual

O fornecedor deve possibilitar meios para a Hiperstream 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.

3.9.9. Responsabilização

Convém que os colaboradores sob controle do fornecedor com acesso aos dados pessoais da Hiperstream estejam sujeitos a uma obrigação de confidencialidade.

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.

Convém que o fornecedor atribua um ponto de contato para uso da Hiperstream referente ao tratamento de dados pessoais.

O fornecedor deve notificar prontamente a Hiperstream 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 de tempo, 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, que um registro inclua uma descrição dos dados comprometidos, se forem conhecidos; e se notificações foram realizadas, as medidas tomadas para notificar a Hiperstream 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 como tal.

O fornecedor deve disponibilizar as informações necessárias para assegurar a Hiperstream que os dados pessoais tratados sob um contrato sejam apagados (pelo fornecedor 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 da Hiperstream.

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.

3.9.10. Transferência e Compartilhamento

O fornecedor deve especificar e documentar os países em que, possivelmente, os dados pessoais podem ser armazenados.

Convém que as identidades dos países decorrentes do uso de fornecedores subcontratados sejam incluídos. 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 fornecedor deve informar, em tempo hábil, ou sem demora indevida, à Hiperstream sobre quaisquer alterações pretendidas a este respeito, de modo que a Hiperstream tenha a capacidade de contestar estas alterações ou encerrar o contrato.

4. Revisão e Comunicação

Este documento deve ser revisado pelo menos uma vez por ano. A menos que exigido de outra forma por requisitos legais, contratuais ou regulamentares que justifiquem um plano de revisão.

Quando apropriado, funcionários e contratados devem ser notificados sobre alterações realizadas nesse documento. Ele deve estar publicado e devidamente informado a todos para que a qualquer momento os funcionários e contratados tenham acesso de leitura.

As atualizações desse documento são realizadas sob a direção e aprovação do Diretor de Tecnologia da Informação.

5. Histórico de revisões

Data	Revisores	Versão	Alterações Realizadas
18/05/2022	Daniel de Mello Scarparo	1.0	Primeira versão do documento
16/05/2023	Daniel de Mello Scarparo	1.0	Revisão periódica sem alteração do documento
16/05/2024	Daniel de Mello Scarparo	1.1	Revisão dos itens ‘3.6’ e ‘4’

6. Aprovações

Assinatura	Aprovador
	Bruno Moreira