POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA FORNECEDORES

Versão 1.0
Florianópolis-SC
Dezembro 2022

SMÁRIO

1. INTRODUÇÃO

1.1. Apresentação

Este documento descreve a PSIF - Política de Segurança da Informação para Fornecedores - da empresa ipTrust Tecnologia.

Esta política regula o comportamento dos fornecedores, o acesso, a geração, a manipulação e o descarte dos ativos de informação, visando preservar a integridade, confidencialidade e disponibilidade destes ativos.

Quaisquer condutas em desacordo com as diretrizes aqui descritas são consideradas “incidentes de segurança da informação”.

1.2. Objetivos

Esta política possui os seguintes objetivos:

a. Definir diretrizes organizacionais relativas à segurança da informação para fornecedores;
b. Balizar o comportamento dos fornecedores sobre os ativos da informação da empresa;
c. Conscientizar os fornecedores sobre o correto uso dos recursos de informação da empresa;
d. Definir responsabilidades e ações a serem tomadas quando do não cumprimento desta política.

1.3. Autores

Esta Política de Segurança da Informação para Fornecedores é de autoria do Comitê de Segurança da Informação e Privacidade da ipTrust Tecnologia, assim como a aplicação desta política, sua revisão e sua manutenção.

Dúvidas sobre a aplicação desta política ou sugestões de alteração e melhoria devem ser encaminhadas para os canais atendimento oficiais da ipTrust Tecnologia.

1.4. Divulgação e Distribuição

Esta política de segurança da informação para fornecedores deve ser parte integrante do contrato de prestação de serviço de todos os fornecedores da ipTrust Tecnologia.

As diretrizes contidas neste documento devem ser de conhecimento de todos os fornecedores, inclusive no ato da assinatura dos contratos estabelecidos com a ipTrust Tecnologia.

Ao assinar um contrato que mencione a Política de Segurança da Informação para Fornecedores, o terceiro assume total conhecimento e concordância das diretrizes mencionadas neste documento.

1.5. Versão e Revisão

As versões e revisões realizadas nesta Política são apresentadas na Tabela 1 abaixo:

Tabela 1 – Controle de versões a PSIF.

Data	Versão	Descrição
24/11/2022	0.1	Elaboração da PSIF
02/12/2022	0.2	Ajustes no documento
15/12/2022	0.3	Revisão do documento
13/02/2023	1.0	Revisão final do documento

Este documento deve ser revisado e uma nova versão deve ser elaborada, homologada, divulgada e distribuída nos seguintes casos:

a. Quando existir alteração significativa em um ativo de informação coberto por esta política;

b. Quando existir a criação de novos ativos de informação relevantes a esta política;

c. Quando uma nova diretriz necessitar ser criada de maneira emergencial;

d. No período máximo de 12 meses a partir da última versão de publicação.

A responsabilidade por iniciar a revisão da política de segurança é do Comitê de Segurança da Informação e Privacidade.

2. DIRETRIZES DE SEGURANÇA

2.1 Diretrizes Gerais

a) O gestor do contrato deve ser comunicado de forma imediata quando houver a identificação de quaisquer riscos ou incidentes que possam causar impacto à segurança das informações da ipTrust Tecnologia.

b) Na identificação de riscos, incidentes e não conformidades ações corretivas e preventivas devem ser adotadas, de modo a eliminar a causa raiz e prover o tratamento adequado dos riscos associados.

c) Quando necessário, inspeções e avaliações podem ser realizadas pela ipTrust Tecnologia para garantir que todos os requisitos para a segurança da informação estão sendo atendidos. Os resultados das inspeções e avaliações, bem como recomendações de melhorias serão registradas e encaminhadas para providências pelo fornecedor.

d) Documentos e registros que demonstrem e evidenciam o atendimento dos requisitos e das diretrizes estabelecidas devem ser apresentadas sempre que necessário.

e) A Política de Segurança da Informação (ou documento equivalente) do prestador de serviço, parceiro e fornecedor pode ser analisada pela ipTrust Tecnologia para verificação de sua conformidade com as normas e políticas internas.

f) Avaliação de risco de segurança da informação e privacidade podem ser realizadas nos contratos dos prestadores de serviço, parceiros e fornecedores no que tange envolvimento de dados pessoais, armazenamento ou processamento de informação sensível, computação em nuvem.

2.2 Propriedade Intelectual

a) O fornecedor é responsável por garantir a conformidade legal de todo e qualquer sistema ou conteúdo utilizado durante a realização de seu serviço;

b) O fornecedor é responsável pela propriedade intelectual do conteúdo dos equipamentos que trouxer para dentro das dependências da ipTrust Tecnologia;

c) O fornecedor é responsável por garantir que os softwares por ele instalados não ferem qualquer tipo de lei de direitos autorais.

2.3 Acesso à Internet

a) O acesso à internet realizado pelo fornecedor em qualquer uma das redes disponibilizadas pela ipTrust Tecnologia, somente poderá ocorrer após autorização e com acompanhamento de um colaborador da ipTrust Tecnologia responsável;

b) A ipTrust Tecnologia se reserva o direito de monitorar o acesso à internet do fornecedor a fim de garantir o uso adequado;

c) O ipTrust Tecnologia se reserva no direito de bloquear os sites que considerar inadequados para a empresa, sem aviso prévio;

d) O acesso à internet realizado pelo fornecedor deverá ter como único objetivo o cumprimento de seu serviço, seja este acesso fornecido pela ipTrust Tecnologia ou por terceiros.

2.4 Equipamentos e Mídias Removíveis

a) A ipTrust Tecnologia reserva-se no direito de realizar auditoria nos equipamentos do fornecedor, antes de autorizar o uso dentro da instituição;

b) O fornecedor se compromete inteiramente pela segurança dos dados de seus equipamentos dentro das dependências da ipTrust Tecnologia;

c) O fornecedor é responsável por garantir que os equipamentos ou mídias que utiliza estão com todos os softwares atualizados, legalizados, com antivírus e livres de qualquer tipo de software que possa prejudicar a rede interna da ipTrust Tecnologia.

2.5 E-Mails

a) A ipTrust Tecnologia reserva-se o direito de monitorar os e-mails enviados e recebidos pelo fornecedor, quando este utilizar a plataforma de gerenciamento de e-mails fornecida pela ipTrust Tecnologia;

b) O fornecedor assume que todos os e-mails enviados durante a execução de serviço, utilizando conta fornecida pela ipTrust Tecnologia, são e-mails corporativos e podem ser monitorados;

c) Nas dependências da ipTrust Tecnologia o fornecedor deve ler e enviar e-mails apenas relacionados com seu trabalho;

d) A qualquer tempo e de qualquer local o fornecedor não deve encaminhar e-mails para colaboradores da ipTrust Tecnologia cujo conteúdo não tenha relação com o trabalho.

2.6 Armazenamento e Manuseio Lógico de Informações

a) O acesso aos ativos de informação da ipTrust Tecnologia só pode ser feito em condições controladas e monitoradas. A concessão dos acessos físicos e lógicos seguirá as premissas das políticas de segurança estabelecidas não sendo permitido que terceiros acessem informações sensíveis sem a devida autorização.

b) Todos os acordos para a preservação da confidencialidade e o sigilo das informações acessadas antes, durante e após a prestação dos serviços devem ser respeitados e cumpridos.

c) Os prestadores de serviços devem respeitar e cumprir todas as medidas, procedimentos e instruções para o registro e controle de acessos físicos e lógicos estabelecidas pela ipTrust Tecnologia.

d) O fornecedor se compromete com a total confidencialidade, integridade e disponibilidade das informações da ipTrust Tecnologia que lhe forem concedidas;

e) O fornecedor se compromete a não transmitir informações da ipTrust Tecnologia por canais de comunicação não seguros, que possam ocasionar vazamento destas informações;

f) O fornecedor se compromete com o descarte adequado e seguro das informações da ipTrust Tecnologia ao final do serviço ou quando elas não forem mais utilizadas (o que ocorrer primeiro);

g) O ipTrust Tecnologia se reserva no direito de realizar auditorias de segurança da informação em seus fornecedores;

h) O armazenamento de informações do ipTrust Tecnologia pelo fornecedor deve ser realizado de modo seguro, ou seja, com controle de acesso restrito aos envolvidos com o serviço dentro da empresa e com criptografia quando a informação for confidencial;

i) Caso o fornecedor esteja com uma mídia em trânsito contendo informações do ipTrust Tecnologia, este é responsável por garantir que a perda ou roubo desta mídia não implique no acesso a estas informações;

j) O fornecedor também se compromete com a garantia de que as informações da ipTrust Tecnologia não serão adulteradas durante o armazenamento em qualquer tipo de mídia sob sua responsabilidade.

2.7 Acesso à Rede Interna (local ou remoto)

a) O fornecedor somente poderá acessar a rede interna da ipTrust Tecnologia após autorização da equipe responsável;

b) O acesso do fornecedor à rede interna poderá ser monitorado pelo setor de Tecnologia da Informação da ipTrust Tecnologia quando este julgar necessário;

c) A ipTrust Tecnologia se reserva no direito de liberar o acesso local ou remoto a sua rede interna, somente após a autorização formal e com o devido acompanhamento por um colaborador;

d) Os acessos remotos de todos os fornecedores devem ser criados e autorizados pela equipe de Tecnologia da Informação da ipTrust Tecnologia.

e) A ipTrust Tecnologia se reserva no direito de monitorar ou acompanhar todos os acessos realizados na sua rede interna.

2.8 Uso de Senhas

a) O fornecedor não deve solicitar, aceitar ou utilizar senha de acesso dos colaboradores da ipTrust Tecnologia em nenhum caso;

b) Toda credencial utilizada pelo fornecedor deve ser criada especificamente para este fim e identificá-lo de modo inequívoco;

c) A ipTrust Tecnologia é responsável por realizar a inativação da senha do fornecedor. Caso o fornecedor identifique que a credencial ainda está ativa, após finalização de contrato, este deve solicitar imediatamente a sua desativação;

d) O fornecedor não deve compartilhar senhas utilizadas para acesso a sistemas da ipTrust Tecnologia entre seus colaboradores ou com terceiros, ou seja, cada credencial e senha deve ter um identificador único;

e) O fornecedor é responsável pela segurança das senhas que lhe são entregues e deve comunicar imediatamente a ipTrust Tecnologia a sua perda ou vazamento.

2.9 Colaboradores do Fornecedor

a) O fornecedor deve garantir que seus colaboradores alocados para a realização de determinado serviço possuam a formação e qualificação necessária para tal;

b) O fornecedor deve informar a ipTrust Tecnologia o nome, formação e tempo de serviço de seus colaboradores quando for solicitado;

c) A ipTrust Tecnologia reserva-se no direito de estabelecer requisitos de qualificação, formação e tempo de serviço, para autorizar o acesso de colaboradores do fornecedor a suas informações, sistemas ou dependências físicas;

d) O fornecedor é responsável por comunicar imediatamente a ipTrust Tecnologia o desligamento de seus colaboradores, quando estes estejam prestando algum serviço interno ou possuam credenciais de acesso aos sistemas da ipTrust Tecnologia;

e) O fornecedor deve comunicar imediatamente qualquer mudança na lista de seus colaboradores autorizados a prestar o serviço interno a ipTrust Tecnologia;

f) Todos os colaboradores do fornecedor que prestam serviço a ipTrust Tecnologia assumem total conhecimento e concordância com o conteúdo deste documento.

2.10 Segurança Física

a) O fornecedor é responsável pela informação física concedida a ele pela ipTrust Tecnologia, devendo assegurar a confidencialidade, integridade e disponibilidade destas quando estiverem em seu poder;

b) O fornecedor é responsável pela devolução a ipTrust Tecnologia ou pelo descarte adequado das informações físicas quando estas não forem mais necessárias ou ao final de seu serviço;

c) O fornecedor se compromete a acessar as dependências físicas da ipTrust Tecnologia somente quando devidamente autorizado e acompanhado por um colaborador;

d) Para a retirada de equipamentos da ipTrust Tecnologia, por qualquer motivo, o fornecedor deverá receber autorização formalizada por um dos colaboradores da organização, podendo esta ser por documento físico, e-mail ou registro de chamado interno.

3. INCIDENTES E MEDIDAS DISCIPLINARES

Qualquer violação das diretrizes constantes nesta política constitui-se em incidentes de segurança da informação e será devidamente registrado e analisado pelo Comitê de Segurança da Informação da ipTrust Tecnologia.

Após análise do Comitê de Segurança, serão deliberadas medidas disciplinares ao fornecedor, que podem incluir:

- Advertência formal ou informal;
- Cancelamento do contrato de prestação de serviço;
- Multas previstas em contrato;
- Ações judiciais ou abertura de boletim de ocorrência.