1. OBJETIVO

Este documento define todas as regras e princípios básicos para garantir a qualidade e a proteção das informações das organizações Logiks e LGK. Estas instruções são elaboradas e mantidas levando em conta a Qualidade e Segurança de Informação dos fornecedores e suas infraestruturas que se relacionam com a realização dos serviços prestados.

2. ABRANGÊNCIA

Este documento aplica-se a todos os fornecedores e parceiros que fornecem produtos ou serviços, ou acessam informações das organizações Logiks e LGK.

3. VIGÊNCIA

Esta Política passa a vigorar a partir da data da sua publicação.

4. DEFINIÇÕES

SI – Segurança da Informação.

5. DOCUMENTOS RELACIONADOS

DO.002 – Manual do Sistema de Gestão Integrado
PO.001 – Política de Segurança da Informação
PR.TI.005 – Controle de acesso

6. DIRETRIZES

Todos os fornecedores deverão passar por um processo de homologação, registrado no FR.008 – Lista de fornecedores.

Nesta homologação serão avaliados os riscos relacionados a qualidade e a segurança da informação e as formas de mitigação dos riscos relacionados aos produtos ou serviços fornecidos. Os riscos poderão ser mitigados com base em cláusulas contratuais que garantam a qualidade e segurança da informação, ou certificações.

O processo de homologação deverá ser registrado no FR.008 – Lista de fornecedores.

Os fornecedores serão monitorados mensalmente, e o resultado deste monitoramento é avaliado anualmente, o registro do monitoramento e avaliação deverá ser mantido no FR.020 - Avaliação de fornecedores e quando o fornecedor não estiver atendendo satisfatoriamente, ações deverão ser tomadas.

A seguir são apresentadas as orientações relacionadas à segurança da informação que devem ser avaliadas pelos fornecedores.

6.1. Conscientização Sobre Segurança da Informação

É importante que a educação em segurança da informação seja um processo contínuo e praticado regularmente, a fim de reduzir riscos. É recomendado que todos os colaboradores do fornecedor de serviços que tenham acesso aos sistemas de informação promovam programas de conscientização em segurança da informação.

6.2. Acordos de confidencialidade

Contratos de não-divulgação firmados pelos funcionários e contratados devem permanecer em vigor após a rescisão ou mudança na relação trabalhista.

6.3 Classificação de Integridade de Dados

É recomendado que os dados tratados sejam classificados com base nas exigências de confidencialidade e que um conjunto de medidas para a identificação de tratamento de dados seja definido, evitando vazamentos e acessos indesejados.

6.4 Tratamento de Mídia

É recomendado que o fornecedor estabeleça um procedimento para o tratamento das mídias (discos rígidos internos/externos, drives de memória etc.), considerando o descarte de forma a fim de prevenir a divulgação não autorizada de dados, quando aplicável.

6.5 Controle de Acesso

O acesso dos Prestadores de Serviço às informações internas e confidencias poderá ser feita mediante assinatura do Acordo de Confidencialidade.

É recomendado que normas de controle de acesso sejam estabelecidas e documentadas. O acesso aos dados, sistemas e aplicativos deve ser controlado por um procedimento seguro de autenticação. Os processos de gestão de acesso de usuário devem ser definidos e formalizados, incluindo as etapas de provisionamento, alteração e exclusão. O acesso de usuário deve ser atribuído conforme necessário.

O processo deve garantir a responsabilização pelas ações de gestão de acesso de usuário. Revisões formais de direitos de acesso de usuário devem ser realizadas em intervalos regulares, dependendo da criticidade do ativo, no mínimo uma vez por ano, a fim de identificar qualquer acesso não autorizado e garantir a devida segregação de atribuições.

6.6 Política mesa e tela limpa

É recomendado que seja estabelecida uma política de mesa e tela limpa nas instalações de processamento de informações, levando com conta as classificações de dados, exigências legais e contratuais e riscos.

6.7 Segurança de Serviços de Rede

Cada serviço de rede, seja local ou terceirizado, deve incluir mecanismos de segurança (proteção, detecção e reação) adaptados à sensibilidade dos dados sendo transmitidos. Esses mecanismos de segurança devem ser implementados na rede ou diretamente nos sistemas, aplicativos, estações de trabalho ou banco de dados.

6.8 Trabalho Remoto

É recomendado estabelecer uma Política de Trabalho Remoto, visando assegurar as informações tratadas fora do ambiente de trabalho.

6.9 Backup de Informações e Sistemas

As políticas de backup e restore devem ser definidas para os dados, software e sistemas tratam dados das organizações.

6.10 Relações com Terceiros

Os projetos entregues por terceiros devem seguir as diretrizes estabelecidas nesta Política, sendo de total responsabilidade do fornecedor de serviços a garantia dos serviços e de todas as obrigações legais.

6.11 Aquisição, Desenvolvimento e Manutenção de Sistemas

Todos os fornecedores de softwares, desenvolvimento ou manutenção de sistemas devem seguir está política. Sempre que o fornecedor de serviços iniciar um novo projeto de TI ou mudança substancial em sistema de informação existente, recomendamos que os itens de segurança sejam documentados.

6.12 Gestão de Incidentes

Os incidentes de Segurança da Informação devem ser identificados e gerenciados de forma consistentes, disciplinados e compartilhados.

Assim que identificados e, o mais rápido possível, todos os incidentes de segurança que possam impactar as organizações Logiks e LGK devem ser notificados e comunicados imediatamente.

6.13 Observância de Leis e Normas

As atividades da empresa devem garantir a observância das obrigações contratuais para assegurar que as devidas exigências de qualidade e segurança do trabalho sejam levadas em conta em seus processos.

Os Fornecedores que tratam dados pessoais, devem garantir que eles sejam gerenciados de acordo a Lei 13709 de 14 de agosto de 2019 – Lei Geral de Proteção de Dados Pessoais, quando nenhuma outra orientação for passada.

As atividades do fornecedor de serviços devem garantir a observância das obrigações estatutárias e regulatórias para assegurar que as devidas exigências de qualidade e segurança da informação sejam levadas em conta em seus processos. Todas as exigências legais, estatutárias e regulatórias relevantes devem ser explicitamente definidas.

6.14 Violações

Qualquer evento que resultar em problemas de qualidade ou de segurança da Informação, deverão ser comunicados

No caso de violação desta política ou das demais políticas o fornecedor poderá ser advertido, podendo até reincidir o contrato.

7. HISTÓRICO DE ALTERAÇÃO

Ver.	Data	Histórico	Responsável
00	28/12/2021	Elaboração	Tuanne Sousa
01	01/02/2022	Inclusão do método de minimizar os riscos no item. DIRETRIZES.	Tuanne Sousa
02	14/06/2023	Revisado sem alteração	Elsimar Barros
03	29/11/2023	Incluído a Logiks, pois esta política também irá incorporá-la. Identificado nas diretrizes quais são obrigatórias e quais são recomendadas.	Maria Eduarda