A Direção da Fast Solutions, organização formada pelas divisões Digital Fast & Ltda, entende que qualidade é uma questão holística, onde o todo depende de cada parte. Assim sendo, esta Direção considera de fundamental importância o papel de cada colaborador com o resultado global pretendido, expresso em nossa Política da Qualidade, e reafirma o seu compromisso com a melhoria contínua e com o Sistema de Gestão Integrado descrito neste manual.

Missão

Desenvolver soluções inovadoras de tecnologia com uma abordagem exclusiva que nos permita combinar competências-chave em todos os setores da nossa organização, entregando inovação de tecnologia digitais e processos escaláveis aos clientes.

Visão

Ser reconhecida como líder mundial em soluções e inovações tecnológicas, aproximando, cada vez mais, as empresas e seus clientes finais, onde entregamos resultados transformadores para um exigente novo mundo digital.

Valores

- **Cliente em primeiro lugar:** a confiança dos nossos clientes é um bem valioso.
- **Qualidade acima de tudo:** não fazemos qualquer coisa, fazemos o melhor.
- **Comprometimento é nosso forte:** prazo é prazo, é compromisso assumido.
- **Temos Integridade:** Somos éticos e temos bom senso em nossas decisões.
- **Respeito ao próximo:** Isso faz toda a diferença.
- **Inovação:** fazer diferente e melhor.

1. OBJETIVO

Definir as diretrizes para o gerenciamento da LGPD em nossos processos de negócio e elucidar todas as condições que minimizam exposições com dados e outras questões pertinentes à Privacidade dos Dados dos nossos clientes.

2. CAMPO DE APLICAÇÃO

Este manual se aplica a todas as atividades executadas pela FAST SOLUTIONS que influenciam direta ou indiretamente na entrega de segurança da informação em nossos produtos.

3. NORMAS E DOCUMENTOS APLICÁVEIS

NBR ISO 9000:2015 – Sistemas de Gestão da Qualidade – Fundamentos e Vocabulário.
NBR ISO 9001:2015 – Sistema de Gestão da Qualidade – Requisitos.
ISO IEC 27000:2014-Information Technology –Security Techniques-Information Security Management Systems –Overview and vocabulary.
ABNT NBR ISO IEC 27001:2013-Tecnologia da informação –Técnicas de segurança- Sistemas de Gestão da segurança da informação –Requisitos.
ABNT NBR ISO IEC 27002:2013- Tecnologia da informação –Técnicas de segurança- Código de Prática para controles de segurança da informação.
FSC-STD-40-004 V3-0.

4. A IMPORTÂNCIA DA PRIVACIDADE DE DADOS

A proteção dos dados pessoais é essencial no cenário empresarial atual. O respeito à privacidade dos indivíduos e o cumprimento de regulamentações, como o LGPD e outras leis de privacidade, são fundamentais para construir confiança com os clientes e evitar perdas relacionadas com a violação dos direitos dos consumidores dos nossos clientes.

5. NOSSA ABORDAGEM

Na Fast Solutions compreendemos a complexidade da minimização de dados pessoais. Oferecemos uma abordagem abrangente e eficaz para garantir que suas operações de processamento de dados estejam em conformidade com as regulamentações aplicáveis.

Principais Recursos e Serviços

- **Identificação de Dados Sensíveis:** Nossa tecnologia avançada identifica automaticamente os dados pessoais sensíveis em seu banco de dados, incluindo informações como CPF, endereços e nomes.

- **Anonimização e Pseudonimização:** Implementamos técnicas robustas de anonimização e pseudonimização, permitindo que você proteja os dados pessoais dos titulares enquanto mantém a utilidade das informações para seus processos de negócios.

- **Registro de Minimização:** Mantemos um registro detalhado de todas as ações de minimização de dados, garantindo total transparência e conformidade.

- **Gestão de Consentimento:** Facilitamos o gerenciamento de consentimento dos titulares de dados, ajudando você a manter registros precisos de opt-ins e opt-outs.

- **Blacklist e Lista de Rejeição:** Nós trabalhamos em conjunto com o cliente de forma a trocar informações sobre quais e-mails são válidos para disparo e quais não são. Trata-se de uma gestão de e-mails com condições para serem recebidos na ponta pelos consumidores, com a finalidade de recebimento da fatura e de medição dos índices de abertura dos e-mails.

- **Conformidade Legal:** Nossa solução garante que sua empresa esteja em conformidade com regulamentações globais de privacidade de dados, minimizando o risco de multas e sanções.

- **Confiança do Cliente:** Proteger os dados pessoais dos clientes é essencial para construir confiança. Nossa solução reforça sua reputação de cuidado com a privacidade.

- **Eficiência Operacional:** Automatizamos processos de minimização de dados, economizando tempo e recursos valiosos.

6. APLICAÇÃO TÉCNICA

As informações dos clientes são tratadas da seguinte forma:

- **Identificar Dados Pessoais Relevantes:** Primeiro, identifique quais campos contêm informações pessoais sensíveis ou identificáveis. Isso pode incluir campos como cpf, nomeDestinatario, emailDestinatario, foneDestinatario, entre outros dados pessoais.

- **Anonimização e Pseudonimização:** Dependendo dos requisitos de privacidade, que o cliente solicitar, podemos aplicar técnicas de anonimização ou pseudonimização a esses campos. Anonimização envolve a remoção completa de informações pessoais, enquanto pseudonimização substitui os dados pessoais por valores não identificáveis.

    - **Exemplo de pseudonimização em PseudoLang que utilizamos em nossas aplicações** (substituição do CPF por um código pseudônimo):

```
UPDATE Tabela SET cpfDestinatario = SHA256(cpfDestinatario);
```

- **Exposição dos dados pessoais:** Temos duas formas de expor os dados pessoais, sem comprometer a segurança da informação e sua integridade.

    - **Criptografia da camada Rest:** a abordagem abaixo é amplamente utilizada em nossas implementações.

```
import ...

@Path("/crypto")
public class CryptoResource {

 // Definição da chave criptografada (mantenha isso seguro em um
ambiente de produção)
    private static final String SECRET_KEY = "chave-secreta";

    @POST
    @Path("/encrypt")
    @Consumes(MediaType.TEXT_PLAIN)
    @Produces(MediaType.TEXT_PLAIN)
    public Response encryptText(String plainText) {
        try {
            // Crie uma chave secreta
```

```
            SecretKey secretKey = new
SecretKeySpec(SECRET_KEY.getBytes(), "AES");

            // Crie uma instância de cifra AES
            Cipher cipher = Cipher.getInstance("AES");
            cipher.init(Cipher.ENCRYPT_MODE, secretKey);

            // Criptografe o texto
            byte[] encryptedBytes =
cipher.doFinal(plainText.getBytes());

            // Codifique os bytes criptografados para Base64
            String encryptedText =
Base64.getEncoder().encodeToString(encryptedBytes);

            return Response.ok(encryptedText).build();
        } catch (Exception e) {
            e.printStackTrace();
            return
Response.status(Response.Status.INTERNAL_SERVER_ERROR).entity("Erro
ao criptografar o texto.").build();
        }
    }
```

- **Exposição por isolamento de infra**, como por exemplo, link ponta a ponta, vpn e outras abordagens de arquitetura que visem a proteção e o bloqueio a dados sensíveis.

  - **Principais Soluções homologadas:**
    - **Connect:** utilizado para recepcionar arquivos por meio de um link ponta a ponta, via camada segura.
    - **SFTP:** poucos clientes utilizam, mas é uma proposta adequada para quem não quer fechar uma VPN ou um link dedicado.
    - **API Rest:** utilizado em ambientes de trocas online, como por exemplo a solução Oi URA ou as camadas de comunicação apresentadas no OmniTIM e no OmniChannel.

- **Exclusão de Dados Irrelevantes:** Remova dados que não são mais necessários para a finalidade de processamento. Certifique-se de que está retendo apenas os dados estritamente necessários.

  - **Caso TIM:** os dados já disparados por nosso processo, são descartados, sendo retidos apenas os arquivos criptografados, enviados inicialmente pelo cliente. O período de retenção pode variar de cliente para cliente, de acordo com o contrato vigente.

- **Consentimento do Titular dos Dados:** Certifique-se de que possui consentimento adequado dos titulares dos dados para processar as informações. Isso pode ser representado pelos campos dataOptin e dataOptout.
- **Criptografia:** Para campos sensíveis que precisam ser mantidos em seu formato original, como endereços de e-mail, deve se aplicar técnicas de criptografia para proteger essas informações.

  Utilizamos duas principais tecnologias de criptografia para alcanvßar nossos objetivos:

  - **Transparent Data Encryption (TDE):** Implementamos o TDE no nível do banco de dados SQL Server. Essa técnica criptografa todo o banco de dados, incluindo os campos que contêm dados sensíveis. Isso garante que os dados estejam protegidos em repouso e que qualquer acesso não autorizado aos arquivos de banco de dados seja inútil sem a chave de descriptografia apropriada.

  - **Always Encrypted:** Para um nível adicional de segurança, utilizamos o Always Encrypted para criptografar colunas específicas que contêm dados sensíveis, como endereços de e-mail. Isso garante que mesmo nossos administradores de banco de dados não possam acessar os dados sem a chave de descriptografia adequada.

- **Acesso Restrito:** Controle o acesso aos dados pessoais, permitindo que apenas pessoas autorizadas acessem essas informações.

- **Registro de Minimização:** Mantemos um registro de todas as ações de minimização realizadas em um campo específico, incluindo data e hora da minimização, tipo de minimização e quaisquer detalhes relevantes. Essas informações são gerenciadas a partir de nosso log e não são registradas em banco de dados para fins de preservação da segurança e performance da infraestrutura.

- **Limpeza Regular (housekeeping):** Temos implementada uma política de limpeza regular para excluir dados pessoais quando não forem mais necessários para a finalidade original do processamento. **Exemplo:** no caso da TIM mantemos dados de processamento em registro por 3 meses (3 cortes) para apuração de resultados e validação do processo do disparo.

- **Máscara de Dados:** Em certos casos, como exibição de dados em interfaces de usuário, é essencial usar máscaras para ocultar partes dos dados pessoais, como mascarar parte do número de telefone ou endereço de e-mail.

7. PLANO DE AÇÃO

Este documento detalha as diretrizes e procedimentos para lidar com incidentes de vazamento de dados, assegurando que a organização possa responder eficazmente a essas situações, minimizar impactos e cumprir com obrigações legais e regulamentares relacionadas à privacidade de dados, conforme cada contrato vigente.

Assim, em caso de ataque cibernético e vazamento de dados, os seguintes procedimentos serão executados imediatamente.

a) Identificação e Isolamento da Brecha:

a. A equipe de segurança de dados deve ser notificada imediatamente após a identificação de um incidente de vazamento de dados.

b. Analisar as fontes e a extensão do vazamento para que sejam identificadas, podendo envolver investigação para determinar como os dados foram comprometidos.

b) Contenção:

a. Devem ser tomadas medidas imediatas para conter o vazamento de dados e evitar que ele se propague ainda mais.

b. Isso pode incluir a desativação de contas comprometidas, o bloqueio de acesso não autorizado e a correção de vulnerabilidades.

c) Notificação das Autoridades Competentes (se houver necessidade):

a. A organização deve garantir que esteja ciente das obrigações legais em relação à notificação de vazamentos de dados na jurisdição que for competente.

b. Em muitas regiões, é obrigatório que as autoridades reguladoras de privacidade e proteção de dados sejam notificadas sobre vazamentos de dados dentro de um prazo específico após a descoberta.

d) Notificação dos Afetados:

a. Devemos comunicar de maneira rápida e transparente com os stakeholders (clientes) afetados sobre o vazamento de dados e sua extensão.

b. As informações devem ser fornecidas sobre o que ocorreu, que tipo de dados foi comprometido e quais medidas foram tomadas na Fast e quais medidas os afetados podem tomar para proteger suas informações.

e) Avaliação de Riscos:

a. A Fast deve **r**ealizar uma avaliação dos riscos associados ao vazamento de dados, incluindo o potencial impacto na privacidade dos indivíduos afetados e nas operações da organização.

b. Após a avaliação dos riscos, devem ser categorizados os potenciais problemas que estão em andamento e as medidas de mitigação e remoção devem ser tomadas.

f) Correção e Mitigação:

a. A causa raiz do vazamento de dados deve ser identificada e corrigida.

b. Medidas devem ser implementadas para evitar futuros vazamentos semelhantes.

g) Produzir Relatório de Incidente:

a. Todas as informações relevantes sobre o vazamento de dados, incluindo ações tomadas, comunicações e correções, devem ser devidamente documentadas.

b. Essa documentação será útil para relatórios futuros e para demonstrar conformidade com regulamentações de privacidade.

h) Revisão das Políticas de Segurança:

a. As políticas e procedimentos de segurança de dados devem ser revisados e atualizados para evitar futuros incidentes.

b. Se houver a necessidade, a equipe deve ser treinada para seguir as melhores práticas de segurança.

i) Monitoramento Contínuo:

a. O monitoramento constante de possíveis atividades suspeitas deve ser mantidos para evitar recorrências.

8. OBSERVAÇÕES SOBRE A NOSSA INFRAESTRUTURA

A infraestrutura da Fast Solutions atualmente é privada, dentro de um datacenter próprio, com políticas de restrição de acessos, backup, criptografia, firewall e demais regras que são cimplementares a este padrão técnico para controle de privacidade dos dados de todos os consumidades processados dentro da nossa infraestrutura.

Todos os pontos de acesso são controlados por meio de nossas políticas de firewall configuradas exclusivamente para cada cliente, cada qual com acesso restrito.

Mais informações sobre nossa política de segurança está em nosso MANUAL DE GESTÃO INTEGRADA, conforme certificação ISO 27001.

REVISÃO	DATA	DESCRIÇÃO	RESPONSÁVEL
1	02/08/2023	Criação do procedimento técnico para tratamento e implementação de políticas para privacidade das informações de consumidores processados em nossos servidores.	Eduardo Bortolotti