PLANO DE RESPOSTA A INCIDENTES DE *DATA BREACH* - IPARATYH EMPREENDIMENTOS IMOBILIARIOS LTDA (FIX URBNISMO)

Código:	
Versão:	1.0
Data da versão:	30/11/2021
Criado por:	RMSA
Aprovado por:	Comitê de Privacidade
Nível de confidencialidade:	Interno

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
30/11/2021	1.0	RMSA	Elaboração documento

PLANO DE RESPOSTA A INCIDENTES DE *DATA BREACH*

1. ESCOPO:

O presente Plano de Resposta a Incidentes estabelece princípios, conceitos, diretrizes, responsabilidades e procedimentos a serem seguidos para gestão de incidentes de segurança da informação caso a FIX URBANISMO sofra algum tipo de incidente que resulte em violação dos dados pessoais tratados pela empresa na qualidade de Controladora. Com isso, objetiva-se a minimização dos danos decorrentes de um possível incidente e a operacionalização dos respectivos processos de resposta, de forma que estes sejam tratados adequadamente reduzindo ao máximo os impactos para o negócio.

A intenção da FIX URBANISMO ao publicar o presente documento é priorizar e incentivar sua cultura de privacidade e segurança da informação, de modo que a confiança e integridade da empresa sejam consolidadas, bem como o compromisso com a proteção dos dados pessoais e informações de seus clientes, funcionários e parceiros.

2. DEFINIÇÕES:

- Dados pessoais: é qualquer informação, de qualquer natureza e independentemente do suporte (incluindo imagem e som), relativa à pessoa natural identificada ou identificável, inclusive dado pessoal de crianças e adolescentes;
- Dados pessoais sensíveis: 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;
- Controladora: pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Em outras palavras, o controlador determina as finalidades e as maneiras de tratamento dos

dados pessoais, ou seja, controla tanto os motivos quanto os métodos da atividade de tratamento;

- Incidente de segurança: violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento. Alguns exemplos são: (i) perda/roubo de dispositivos físicos, tais como *notebooks*; (ii) acesso aos dados pessoais por terceiros não autorizados; (iii) divulgação inadvertida de dados pessoais "por erro humano";
- Data Breach (vazamento de dados): incidente de segurança que representa risco relevante aos direitos e liberdades do indivíduo, cuja notificação aos titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD) é obrigatória, dando início ao processo de Resposta a Incidentes;
- Encarregado (data protection officer – dpo): Pessoa indicada pelo controlador ou operador para atuar como canal de comunicação com os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- TRI – Time de Resposta a Incidentes: Uma equipe de colaboradores internos responsáveis e preparados para agir rapidamente no caso de uma situação de incidente de segurança e/ou violação de dados pessoais. Este é um grupo de colaboradores com acesso, habilidades, responsabilidade, treinamento e conhecimento-chave para responder os mais variados tipos de incidente.

3. COMPOSIÇÃO E ATRIBUIÇÕES DO TIME DE RESPOSTA A INCIDENTES (TRI)

3.1. Para uma boa execução do presente Plano de Resposta a Incidentes, os processos devem ser claros e os colaboradores envolvidos devem ser previamente estipulados.

3.2. O TRI deve ter reuniões periódicas para definir melhorias neste plano, verificação de pré-requisitos, mecanismos, atribuições, necessidade de preparo,

bem como divulgação e treinamento para os membros e demais colaboradores. Além disso, o Encarregado e ao menos um representante da equipe da Tecnologia da Informação estará envolvido em sua formação.

3.3. O COMITÊ DE PRIVACIDADE deverá cuidar para que as informações de contato do TRI sejam de fácil acesso para todos os colaboradores, criando, se possível, canais de comunicação ágeis e seguros especificamente direcionados ao relato de incidentes de segurança da informação.

3.4. O Time de Resposta a Incidentes - TRI, deverá ter em sua composição, no mínimo:

i. Membro do Comitê de Privacidade;

ii. Colaborador responsável pela Comunicação interna e externa da **FIX URBANISMO**;

iii. Gestor responsável pelo Departamento Jurídico;

iv. Encarregado de Dados Pessoais nomeado ou seu Representante, quando contratada pessoa jurídica.

v. Contratado responsável pelo TI.

3.5. Suas atribuições num contexto de Data Breach, a princípio, serão as seguintes:

Membro do TRI	Planejamento	Durante o Incidente
Contratado responsável pelo TI	Fornecer orientação sobre detecção, isolamento, remoção e preservação de sistemas e arquivos afetados	Endereçar os dados comprometidos para a condução de investigações internas
Comitê de Privacidade	Demonstrar valor na prevenção de incidentes por meio de ações	Alocar recursos financeiros e pessoal para auxiliar no controle e minimização dos danos ocasionados
Jurídico	Limitar responsabilidades e consequências	Orientar os colaboradores internos em respostas às autoridades e interessados,

	econômicas (revisão de cláusulas contratuais)	em conjunto às orientações do Encarregado
Comunicação	Planejar comunicação estratégica para informar, influenciar e manter um bom relacionamento com o público em situação de crise	Assumir posição de porta-voz interno e externo, mantendo uma mensagem positiva e informativa, devendo manifestar-se apenas após a análise da extensão do dano e definição do plano definitivo de atuação do TRI
Encarregado - DPO	Informar e aconselhar sobre as respectivas obrigações nos termos da LGPD, bem como prestar consultoria relativa a temas de Proteção de Dados	Será o responsável por comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular dos dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares dos dados pessoais

4. A FIX URBANISMO SOFREU UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO. O QUE FAZER AGORA?

PASSO 01: IDENTIFICAÇÃO, COLETA E PRESERVAÇÃO DAS EVIDÊNCIAS

RELATÓRIO DA TI PARA O TIME DE RESPOSTA A INCIDENTES

a) Na verificação de alerta ou detecção de possíveis ataques, ocorrências ou incidentes de segurança da informação, visualizados ou provocados por qualquer usuário/colaborador da empresa, o colaborador que os verificar deverá imediatamente informar os responsáveis pela Tecnologia da Informação (TI) via e-mail, via sistema usual de abertura de chamados de suporte técnico ou pelo canal disponibilizado pela FIX URBANISMO para comunicação de incidentes de segurança da informação;

b) A equipe de TI, por sua vez, avaliará os eventos de segurança da informação relatados e aqueles que presenciar via sistema (logs, alertas, etc) e identificará se o que foi informado consiste de fato em um incidente de segurança;

c) A equipe de TI neste processo deverá cuidar para preservar as evidências, mantendo todos os registros a salvo em ambiente que atenda à segurança da informação, com Confidencialidade, Integridade e Disponibilidade;

d) Caso haja conclusão positiva quanto a ocorrência do incidente, a equipe de TI deverá providenciar um Reporte Inicial a ser encaminhado para o Time de Resposta a Incidentes (TRI), no qual deve constar:

i. Data e hora da ocorrência;
ii. Nome do usuário/colaborador que reportou o incidente;
iii. Problema (por exemplo: incidente de vírus, sequestro de dados, criptografia, etc);
iv. Efeito que o problema causou;
v. Tipo de sistema (por exemplo: desktop, hardware, software);
vi. Nome do sistema (se houver).
vii. Informar se é possível ou não constatar violação de dados pessoais.

PASSO 02: COORDENAÇÃO DE DIAGNÓSTICO E ELABORAÇÃO DO RELATÓRIO FINAL

a) Caso não seja possível constatar que a partir do incidente de segurança houve também um comprometimento de dados pessoais (Violação de Dados Pessoais), deverá o TRI acionar imediatamente empresa ou prestador de serviço indicado para perícia técnica e repassar o Reporte Inicial do incidente para que seja avaliado se houve também comprometimento de dados pessoais.

a. *Exemplo: perícia é necessária quando um incidente do tipo "invasão de sistemas" não puder constatar se houve acesso ou retirada de dados do ambiente do cliente. É o que acontece em um ataque de sequestro de dados (ramsonware), pelo qual não se pode atestar imediatamente se houve retirada de dados do ambiente.*

b) Não haverá necessidade de perícia quando o incidente de segurança reportado no capítulo anterior já puder concluir pela violação de dados pessoais.

c) Realizada a perícia, esta deve ser concluída com um Laudo Pericial, no qual a informação de existência ou não de violação de dados deverá ser obrigatoriamente identificada pelo perito.

d) Verificada a violação de dados pessoais na ocorrência de incidente, deve-se também verificar quais as categorias de dados envolvidas para que possa ser analisado o tipo e grau de risco.

e) Com ou sem o laudo, quando não cabível, o Time de Resposta a Incidentes em conjunto, deverá analisar o caso e discutir as ações a serem tomadas, para compor o Relatório Final de Incidente onde constará:

i. Detalhes do incidente de segurança constantes do Relatório Inicial;

ii. Laudo pericial, quando houver;

iii. Quais providências de preservação das evidências foram adotadas;

iv. Quais os colaboradores integraram o Time de Resposta a Incidentes e as ações desempenhadas;

v. Se houve operadores de dados ou parceiros envolvidos no incidente e qual o motivo de seu envolvimento;

vi. Medidas técnicas que serão tomadas para reduzir ou mitigar o risco (troca de senha, anominização, etc);

vii. Forma de comunicação com o público externo e alinhamento da comunicação com o público interno;

viii. Se é caso que demanda notificação obrigatória à ANPD ou aos titulares de dados, conforme orientação do Encarregado;

ix. Previsão para ações judiciais ou sanções administrativas, com provisionamento para fins de auditoria e/ou transações amigáveis de eventuais indenizações ou sanções pecuniárias;

x. Plano prévio e prazo para apresentação do plano final para evitar incidentes da mesma natureza;

PASSO 03: COMUNICAÇÃO DO INCIDENTE – AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

a) Elaborado o Relatório Final e sendo caso de comunicação à ANPD e aos titulares de dados pessoais, a notificação deverá seguir as seguintes orientações básicas:

b) O Encarregado indicado deverá ser responsável pela elaboração de notificação que terá como base o Relatório Final do Time de Resposta a Incidentes.

c) A notificação à ANPD deverá conter, minimamente:

i. a descrição da natureza dos dados pessoais afetados;
ii. as informações sobre os titulares envolvidos;
iii. a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
iv. os riscos relacionados ao incidente;
v. os motivos da demora, no caso de a comunicação não ter sido imediata;
vi. As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

PASSO 04: COMUNICAÇÃO DE INCIDENTE – TITULARES DE DADOS PESSOAIS

a) O titular dos dados deverá ser informado de forma clara, efetiva e transparente, pela equipe de comunicação, com suporte nas informações aprovadas e encaminhadas pelo Encarregado, informando os titulares dos dados:

i. do incidente;
ii. dos riscos relacionados a este incidente;
iii. dos elementos de dados atingidos;
iv. das medidas de segurança adotadas previamente ao incidente;

v. das ações que foram ou serão adotadas para reverter ou mitigar os efeitos;

vi. canal de atendimento para esclarecimentos.

As comunicações à ANPD ou aos titulares não deverão ser realizadas diretamente nos casos em que os dados pessoais sejam controlados pelos clientes da FIX. Nessas situações, caberá à FIX comunicar a seus contratantes, controladores dos dados pessoais, salvo se o contrato entre as partes dispor de forma diversa.

5. COMUNICANDO O INCIDENTE PARA IMPRENSA E PELOS CANAIS INSTITUCIONAIS

O Time de Resposta a Incidentes, por meio de seu colaborador responsável pela área de Comunicação, deverá, apoiada nas orientações do Encarregado, cuidar para que não haja desencontros na comunicação interna e externa. Para tanto, recomenda-se:

i. Não realizar qualquer tipo de nota à imprensa ou aos titulares antes da análise do incidente pela equipe responsável.

ii. A equipe interna da **FIX URBANISMO** responsável por atender telefonemas e/ou canais de atendimentos via e-mail de clientes ou fornecedores deverá ser treinada para alinhar a comunicação, evitando desencontros;

iii. Assegurar ao titular de dados que a situação está sob análise da **FIX URBANISMO**;

iv. Indicar a Política de privacidade disponível no site da empresa;

v. Repassar o contato e a dúvida do titular de dados para um dos membros da equipe de resposta à incidentes, para que esta possa contatar o respectivo titular.

vi. Evitar comunicação com imprensa antes de ciência completa do caso, salvo mencionar que está apurando com o zelo e cuidados necessários

A ***FIX URBANISMO*** deverá manter uma relação fixa e de confiança com prestadores de serviço que serão responsáveis pela área de tecnologia da informação, bem como perícia técnica.

Goiânia/GO, 30 de novembro de 2021.

VISTO COMITÊ DE PRIVACIDADE: