1. OBJETIVO

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

Essas políticas e diretrizes não se limitam apenas a esta política de segurança da informação externa, por isso o **Target Bank** realiza adoção de políticas, normas e procedimentos que visem garantir a segurança da informação, reduzindo-se os riscos, os danos e/ou os prejuízos que possam comprometer a imagem e os objetivos da organização.

2. DOCUMENTOS DE REFERÊNCIA

- NORMA ABNT NBR ISO 27001:2013 - Tecnologia de informação – Técnica de segurança – Sistemas de gestão de segurança da informação – Requisitos;
- Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes
- Acordo de Responsabilidade e de Confidencialidade da Informação.

3. POLÍTICA PARA RELACIONAMENTO COM PROVEDORES EXTERNOS

Os requisitos de segurança da informação devem ser acordados com o provedor externo e documentados no Acordo de Responsabilidade e Confidencialidade da Informação a fim de mitigar os riscos associados com o acesso dos provedores externos aos ativos do **Target Bank**.

As diretrizes contempladas na Política - Conheça Seu Fornecedor – KYP, complementam esta política.

O Acordo de Responsabilidade e Confidencialidade da Informação firmado com o provedor externo deve contemplar todas as diretrizes desta política que são aplicáveis ao prestador de serviço.

Para os serviços terceirizados de Tecnologia da Informação, este Acordo de Responsabilidade e Confidencialidade da Informação deve ser estendido por toda a cadeia de suprimento do provedor externo.

Um processo formal para gestão de provedor externo deve ser estabelecido.

A aderência a esta política por parte do provedor externo deve ser monitorada sistematicamente pelo **Target Bank**.

O Procedimento Gestão de Provedor Externo, bem como Procedimento Gestão de Nível de Serviço, os questionários de avaliação e reavaliação de fornecedor, apresentam o processo que viabilizam esta política.

Esta PSI deverá ser compartilhada com todos os fornecedores do **Target Bank**, sendo obrigatória a comunicação aos fornecedores sempre que houver atualizações ou alterações nesta PSI.

4. POLÍTICA PARA USO DE ATIVOS

A criação de material impresso exibindo dados pessoais do **Target Bank** deve ser evitada e, quando necessária, restrita e previamente consentida pelo **Target Bank**.

Mídias removíveis de qualquer tipo que contenha dados e informações confidenciais do **Target Bank**, quando não forem mais utilizadas, devem ser apagadas ou destruídas por procedimentos que garantam que essas informações não possam ser recuperadas.

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

Todos os colaboradores deverão ter ciência dos riscos associados à sua condição e cumprir rigorosamente as políticas, normas e procedimentos. O **Target Bank** poderá, a qualquer tempo, revogar credenciais de acesso concedidas em virtude do descumprimento desta política ou a seu exclusivo critério, a fim de proteger os dados com acesso concedido.

5. 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.

6. POLÍTICA DE CONTROLE DE ACESSO

Os colaboradores sob controle do fornecedor com acesso aos dados do **Target Bank**, 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.

7. POLÍTICA DE BACKUP

Todo fornecedor contratado pelo **Target Bank** 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.

O **Target Bank** deve estar ciente do local onde essas cópias de segurança são mantidas pelo fornecedor, o tempo de retenção, bem como como cada fornecedor permite a exclusão dessas informações retidas.

8. POLÍTICA DE GESTÃO DE EVENTO

O fornecedor contratado pelo **Target Bank** 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.

9. POLÍTICA DE GESTÃO DE INCIDENTES

O fornecedor deve cooperar com o **Target Bank** 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.

10. 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 o **Target Bank** monitore o desempenho do(s) serviço(s) contratado(s).

É de propriedade do **Target Bank**, todos os "designs", criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com o **Target Bank** (Lei de Propriedade Intelectual – Lei nº 9.279/96 – Art. 88).

Os fornecedores e colaboradores do **Target Bank** devem assegurar que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

11. POLÍTICA DE ANÁLISE CRÍTICA DA SEGURANÇA DA INFORMAÇÃO

Todo fornecedor contratado pelo **Target Bank** 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 pelo contrato.

O fornecedor deve permitir, quando solicitado, que o **Target Bank** realize auditorias de Segurança da Informação.

Nos casos em que auditorias individuais pelo **Target Bank** forem impraticáveis ou possam aumentar os riscos à segurança, convém que o fornecedor disponibilize, antes da assinatura ou 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 do **Target Bank** na análise crítica de suas operações, desde que uma transparência suficiente seja provida.

12. POLÍTICA PARA PROTEÇÃO DE INFORMAÇÃO PESSOAL

12.1. Consentimento e Escolha

Que o fornecedor forneça ao **Target Bank** 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.

12.2. Legitimidade e Especificação da Finalidade

Os dados pessoais tratados sob um contrato não devem ser utilizados para qualquer finalidade independente do objeto do contrato e restrito ao seu propósito.

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.

12.3. 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) pelo **Target Bank** e/ou objeto contratado.

12.4. Minimização

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

12.5. Limitação de Uso, Retenção e Divulgação

O fornecedor deve notificar o **Target Bank**, 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.

12.6. Precisão e Qualidade

O fornecedor deve possibilitar meios para o **Target Bank** 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 sua qualidade;
- mecanismos de controle para verificar periodicamente a precisão e a qualidade dos dados pessoais coletados e armazenados.

12.7. Abertura, Transparência e Notificação

O uso de subcontratados pelo fornecedor para tratar os dados pessoais deve ser divulgado ao **Target Bank** antes da sua utilização. Também é necessário que seja informado, em tempo hábil, sobre quaisquer alterações pretendidas a este respeito, de modo que o **Target Bank** tenha a possibilidade 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. É obrigatório que estas medidas não sejam sujeitas à redução unilateral pelo subcontratado.

É necessário 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. Em caso de não inclusão, entende-se que só são tratadas no Brasil.

12.8. Acesso e Participação Individual

O fornecedor deve possibilitar meios para o **Target Bank** 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.

12.9. Responsabilização

É necessário que os colaboradores sob controle do fornecedor com acesso aos dados pessoais do **Target Bank** 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.

Que o fornecedor atribua um ponto de contato para uso do **Target Bank** referente ao tratamento de dados pessoais.

O fornecedor deve notificar prontamente o **Target Bank** 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 temporal, 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, é obrigatório que o fornecedor mantenha registro que inclua uma descrição dos dados comprometidos, se forem conhecidos; e se notificações foram realizadas, quais as medidas tomadas para notificar o **Target Bank** 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.

O fornecedor deve disponibilizar as informações necessárias para assegurar ao **Target Bank** 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 do contrato firmado pelo **Target Bank**.

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.

12.10. Transferência e Compartilhamento

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

Os fornecedores devem identificar as identidades dos países decorrentes do uso de fornecedores subcontratados sejam incluídas. 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, ao **Target Bank** sobre quaisquer alterações pretendidas a este respeito, de modo que o **Target Bank** tenha a capacidade de contestar estas alterações ou encerrar o contrato.