Política de Segurança da Informação para Fornecedores, Terceiros e Parceiros de Negócio

SUMÁRIO

1. OBJETIVO

A Política de Segurança da Informação para Fornecedores/Terceiros e Parceiros de Negócio ("Política) tem como objetivo principal direcionar um programa efetivo de proteção dos ativos de informação, sendo a base para o estabelecimento de todos os padrões e procedimentos de Segurança. A política de Segurança estabelece os requisitos de Segurança necessários para a homologação de um serviço, produto oferecido pelo fornecedor, ou parceria de negócio pela área de Segurança da Informação, antes do início da prestação do serviço, nos casos em que o fornecedor processe dados pessoais gerais ou sensíveis de clientes (ex. Nome, RG, CPF, endereço, telefone, e-mail), e de funcionários (ex. Nome, RG, CPF, endereço, telefone, e-mail ou seja referentes a uma conta e/ou aplicação de/ou em Cloud/Nuvem.

A informação é um dos elementos de negócio mais importantes para o Grupo XP Inc. ("Grupo ou Grupo XP") e, dessa forma, manter a sua confidencialidade, integridade e disponibilidade são fatores relevantes para o sucesso do Grupo. Este documento se destina a todos os colaboradores que façam parte do Grupo XP Inc. e quaisquer terceiros/parceiros que usufruam de sua infraestrutura, e que estejam envolvidos na concepção de soluções, sistemas, processos, produtos ou serviços.

2. ABRANGÊNCIA

Todos os ambientes corporativos, sistemas, colaboradores, parceiros do Grupo XP Inc., e as próprias empresas do Grupo XP Inc.

3. DOCUMENTOS DE REFERÊNCIA

- Política de Segurança da Informação.
- Norma de Segurança em Contratações e Aquisições de Fornecedores/Terceiros e Parceiros de negócio.
- Procedimento de Avaliação de Fornecedores/Terceiros e Parceiros de Negócio.

4. VIGÊNCIA, REVOGAÇÃO E CICLO DE REVISÃO

Esse documento entra em vigor a partir da data de sua aprovação, descrita na folha de controle e cancela as versões anteriores ou que tratam do mesmo assunto. Esse documento pode ser revisado anualmente ou, quando necessário, caso haja alguma mudança nas normas do Grupo XP Inc., alteração de diretrizes de Segurança da Informação, objetivos de negócio ou se requerido pelo regulador alguma das Controladas.

5. DEFINIÇÕES

Acionista Controlador: O acionista ou grupo de acionistas que controlam a Companhia e suas Coligadas, vinculado(s) por acordo ou sob controle comum, que exerça(m) o poder de controle, direto ou indireto, sobre sociedade, nos termos da Lei nº 6.404/76.

API: Application Programming Interfaces - Conjuntos de definições e protocolos que permitem a interação entre diferentes sistemas de software.

***AppSec* -** Application Security: Área responsável por avaliar prestações de serviço/parceria que envolve integrações ou conexões com sistemas/ambiente do Grupo XP Inc.

Área de Privacidade: Área responsável por avaliar prestações de serviço/parceria que envolve coleta, tratamento ou compartilhamento de dados pessoais e/ou dados pessoais sensíveis.

Áreas de negócio: Áreas internas do Grupo XP Inc. responsável pela contratação do fornecedor e/ou estabelecimento de parcerias de negócio.

Coligadas: As sociedades em que a o Acionista Controlador tenha influência significativa (art. 243, §1º, da Lei nº 6.404/76).

Conglomerado Prudencial XP: a XP Investimentos CCTVM S.A., Banco XP S.A., XP DTVM Ltda. e demais empresas do Grupo XP Inc., constituídas no Brasil e no Exterior, que se enquadram na definição que consta da Resolução n° 4.950/21, do CMN.

Consentimento: O consentimento é uma das hipóteses legais para o tratamento de dados pessoais, sendo fundamental para garantir que o titular tenha controle sobre suas informações. De acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD), o consentimento deve ser:

a. Livre: O titular deve ter a opção de consentir ou não, sem coerção ou consequências negativas por não dar seu consentimento.

b. Informado: O titular deve ser informado de forma clara sobre quais dados estão sendo coletados, para que finalidade e como serão utilizados. Isso inclui informações sobre o compartilhamento com terceiros, se aplicável.

c. Inequívoco: O consentimento deve ser expresso de maneira clara, evitando ambiguidades.

Controladas: As sociedades nas quais a XP Investimentos S.A. são Acionista Controlador.

Controlador do dado: Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, notadamente o Grupo XP Inc.

DAST: Dynamic Application Security Testing, ou Teste de Segurança de Aplicações Dinâmicas -Abordagem de segurança de software que analisa uma aplicação em execução para identificar vulnerabilidades e falhas de segurança.

DaaS: Desktop as a Service - Modelo de computação em nuvem onde a infraestrutura de desktop virtual é oferecida e gerenciada por um provedor de serviços terceirizado, neste caso pelo Grupo XP Inc.

EHT: Engenharia de Hacking de Testes:- Conjunto de práticas e metodologias utilizadas para avaliar e melhorar a segurança de sistemas, aplicações e redes através de técnicas de *hacking* ético. O objetivo da EHT é identificar vulnerabilidades e fraquezas em um ambiente de TI antes que possam ser exploradas por atacantes mal-intencionados.

Fornecedor/Terceiro e Parceiro relevante: Um fornecedor/terceiro e parceiro relevante é aquele que, de acordo com as análises realizadas pela equipe de Segurança da Informação (Governança de Segurança da Informação) e Continuidade de Negócios mencionadas anteriormente neste documento, é altamente relevante para o cenário tecnológico do Grupo XP Inc. Para determinar se o âmbito da prestação de serviços é relevante, o fornecedor deve cumprir todos os critérios: Processa dados pessoais gerais e/ou sensíveis de clientes e/ou funcionários, fornece serviços de processamento/armazenamento em nuvem externa ao Grupo e fornece serviço que impacta a continuidade dos negócios do Grupo XP Inc. Os fornecedores/Parceiros de desenvolvimento, consultoria e auditoria não são classificados como fornecedores/parceiros relevantes.

Grupo XP Inc. ou XP: Empresas Controladas pela XP Inc. e suas Coligadas, constituídas no Brasil e nos Estados Unidos, consideradas em conjunto.

Hardening: Refere-se ao processo de reforçar a segurança de sistemas, redes e aplicações para reduzir suas vulnerabilidades e minimizar o risco de ataques. O objetivo do *hardening* é criar uma configuração segura que proteja os ativos de informação contra acessos não autorizados e ameaças cibernéticas.

Incidente: É um evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo e/ou sistema de informação, assim como qualquer violação da Política de Segurança da Informação e/ou de Privacidade de Dados.

Incidente relevante: Incidente relevante é aquele que cause, direta ou indiretamente, um impacto crítico sobre os ativos, serviços e sistemas de informação ou recursos computacionais do Grupo XP Inc., ou que acarrete um risco ou dano relevante aos titulares de dados.

ISO 27001: É uma norma internacional que especifica os requisitos para um sistema de gestão de Segurança da Informação (SGSI) para proteger informações sensíveis e garantir a confidencialidade, integridade e disponibilidade dos dados.

NetSec – Arquitetura de SI: Área responsável por avaliar prestações de serviço/parceria que envolve algum componente de arquitetura do fornecedor/parceiro no ambiente do Grupo XP Inc.

Oferta: Refere-se ao item que pode ser solicitado via Catálogo de Serviços do Grupo XP Inc.

***Open Banking* ou *Open Finance*:** Conjunto de regras e tecnologias que permite o compartilhamento de dados e serviços financeiros entre instituições financeiras e provedores autorizados.

Operador do dado: Segundo o inciso II, do artigo 5º da LGPD, trata-se pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

Opt-In: O *opt-in* é um modelo de consentimento em que o titular dos dados deve manifestar sua vontade de forma explícita para que seus dados pessoais sejam coletados e tratados. Isso significa que o usuário precisa tomar uma ação ativa, como marcar uma caixa de seleção ou clicar em um botão, para consentir com o uso de seus dados.

Opt-Out: O *opt-out* é a opção de se retirar ou recusar o tratamento baseado no consentimento. O consentimento é presumido até que o titular decida cancelar.

OWASP: *Open Web Application Security Project* (OWASP*)* Top 10 - uma lista dos dez principais riscos de segurança em aplicações web, publicada pela *Open Web Application Security Project* (OWASP*).* Esta lista é amplamente reconhecida e utilizada como um guia para ajudar desenvolvedores, profissionais de segurança e organizações a entender e mitigar as vulnerabilidades mais críticas em suas aplicações. A lista é atualizada periodicamente para refletir as mudanças no cenário de ameaças.

Parceiros de Negócios: Entidades Parceiras do Grupo que possuem alianças e vínculo contratual.

Patches: Patch (ou Atualização de Software) é um conjunto de alterações no código de um software que é aplicado para corrigir problemas, melhorar a funcionalidade ou aumentar a segurança do sistema. Os patches são frequentemente lançados por desenvolvedores de software para resolver vulnerabilidades conhecidas, bugs e falhas que podem afetar o desempenho ou a segurança do software.

***Phishing*:** É uma técnica utilizada para roubar informações através de envio de e-mails falsos, afim de obter informações pessoais como senhas, cartão de crédito, CPF, número de contas bancárias, entre outros.

PoC: *Proof of Concept* ou Prova de Conceito - Trata-se de testes/validação da solução, sistema, processo etc., antes da efetiva contratação ou parceria.

Runbooks: Documentos que contêm instruções detalhadas sobre como executar tarefas específicas, procedimentos operacionais ou processos de resposta a incidentes em ambientes de TI. Eles são frequentemente utilizados por equipes de operações, suporte técnico e segurança da informação para garantir que as atividades sejam realizadas de maneira consistente e eficiente.

SAST: *Static Application Security Testing*, ou Teste de Segurança de Aplicações Estáticas - Abordagem de segurança de software que analisa o código-fonte de uma aplicação em busca de vulnerabilidades e falhas de segurança antes que o software seja executado. Essa técnica é realizada durante as fases iniciais do desenvolvimento, permitindo que os desenvolvedores identifiquem e corrijam problemas de segurança de forma proativa.

SecOps – BlueTeam: Área responsável por avaliar prestações de serviço/parceria que envolve acesso em aplicação web (site).

Self Assessment: Matriz de avaliação elaborada pela XP com controles de Segurança e Privacidade baseado na ISO 27001, boas práticas de mercado e controles da XP.

Service Desk N3: Área responsável por avaliar prestações de serviço/parceria que necessitam de instalações no notebook/desktop do Grupo XP Inc.

SOC 2 Tipo 2: Estrutura para organizações de serviços que demonstra controles adequados para critérios de segurança de dados.

Terceiros: Fornecedores/Parceiros de negócio que realizam prestação de serviço ou oferta de produtos para o Grupo XP Inc.

***Pentest*:** Testes de intrusão - *Penetration Testing* - Prática de segurança da informação que envolve simular ataques cibernéticos em sistemas, redes ou aplicações para identificar vulnerabilidades que poderiam ser exploradas por atacantes mal-intencionados. O objetivo dos testes de intrusão é avaliar a segurança de um ambiente e fornece recomendações para mitigar riscos.

6. DIPOSIÇÕES GERAIS

Os fornecedores/terceiros ou parceiros de negócio devem cumprir com todos os requisitos da legislação brasileira e estadunidense, quando aplicáveis, bem como devem se comprometer a seguir integralmente os itens e os requisitos a seguir:

- Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada, mantendo a sua confidencialidade;
- Assegurar que os recursos colocados à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Grupo XP Inc.;
- Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos seguindo os requisitos de Segurança;

- Garantir a continuidade do processamento das informações relevantes de negócios;
- Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
- Atender às leis que regulamentam as atividades do Grupo XP Inc. e seu mercado de atuação;
- Selecionar os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;
- Comunicar imediatamente o Grupo XP Inc. qualquer descumprimento da Política de Segurança da Informação para Fornecedores/Terceiros e Parceiros de Negócios.
- Todos os fornecedores homologados pelo Grupo XP Inc., deverão estar de acordo com o TCG - "Termo e Condições Gerais de Fornecimento" ou possuir cláusulas equivalentes no contrato. As alterações contratuais ou salvaguardas devem seguir o processo com Compras, Gestão de Contratos e Jurídico no qual, se necessário, solicitam a validação das partes interessadas, sendo da responsabilidade do Jurídico a inclusão de cláusulas e salvaguardas quando necessário.
- O TCG não se aplica a fornecedores internacionais.
- Fornecedores/Terceiros e Parceiros de Negócio que armazenam e/ou processam dados pessoais gerais e/ou sensíveis de clientes, funcionários ou acessam o ambiente Grupo XP Inc, fornece e/ou disponibiliza o sistema e/ou prestação de serviço em nuvem devem passar por processo de Avaliação de Fornecedor/Prestação de Serviço/Parceiro de Negócio, sendo exigido quando aplicável, o relatório SOC 2 tipo 2 ou outro relatório de auditoria independente na contratação além de *scan* de vulnerabilidade através de ferramenta de verificação de cyber saúde caso este escopo contemple o compartilhamento e/ou tratamento de dados pessoais gerais e/ou sensíveis.

7. RESPONSABILIDADES

7.1. Área Contratante de Serviços de Fornecedores/Terceiros e Parcerias

- Quando da contratação de fornecedores/terceiros ou estabelecimento de parcerias que tenham colaboradores que venham a acessar a rede interna e os dados do Grupo XP Inc., a área contratante deverá garantir que todos estejam cientes dessa Política de Segurança da Informação para Fornecedores Terceiros e Parceiros de Negócio, bem como providenciar notebook XP ou DaaS (Desktop as a service) e usuário de terceiro/parceiro individual para os colaboradores do fornecedor/terceiro e parceiro.
- É responsabilidade da área de negócio prover documentação para análise, incluindo, mas não se limitando, ao relatório SOC 2 tipo 2. Nos casos dos fornecedores/terceiros e parceiros relevantes que o SOC 2 tipo 2 seja obrigatório, se este fornecedor não possuir o relatório, será analisado internamente por Riscos Corporativos.
- É responsabilidade da área de negócio garantir que todos os requisitos de Segurança da Informação foram cumpridos no início da prestação do serviço do fornecedor ou início da parceria;
- Acionar as áreas especialistas para análise e avaliação dos requisitos por meio do preenchimento da Oferta "Avaliação de Fornecedor/Prestação de Serviço/Parceiro de Negócio" presente no catálogo de serviços do Grupo XP Inc.

- Garantir que o Jurídico receba as informações adequadas quando da validação de contratos via sistema de Contratos, indicando os detalhes necessários para que o Jurídico possa contemplar as cláusulas regulatórias adequadas.

7.2. Fornecedores/Terceiros e Parceiros

- É de responsabilidade dos Fornecedores/Terceiros e Parceiros do Grupo XP Inc., observar e seguir as orientações estabelecidas para o cumprimento da presente Política de Segurança da Informação para Terceiros e Parceiros de Negócio;

- Os terceiros/parceiros que acessarem o ambiente do Grupo XP Inc., processarem dados pessoais gerais e sensíveis e/ou informações sensíveis devem ter ciência desta Política.

- Todas as atividades executadas devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras com relação a Segurança da Informação;

- É vedada a contratação de parcerias entre instituições autorizadas a funcionar pelo Banco Central do Brasil ou em que o parceiro contratado atue em nome da instituição contratante para fins de compartilhamento (Open Banking ou Open Finance) de dados. Para a possibilidade de contratação de parcerias com entidades não reguladas pelo Banco Central, a contratação deve observar os requisitos presentes neste documento. No caso da participação para fins de compartilhamento de dados e prestação conjunta de serviços ao consumidor, deve haver consentimento prévio e explícito do cliente.

É obrigatório o preenchimento do *Self Assessment* da XP em caso de prestação de serviço ou parceria de Call Center.

7.3. Segurança da Informação (Governança de Segurança da Informação)

- Avaliar e direcionar para as áreas especializadas de Segurança da informação, bem como emitir um parecer consolidado das áreas consultadas para que o fornecedor/terceiro e parceiro implemente as recomendações necessárias para cada tipo de produto ou serviço específico.
- As áreas especialistas de Segurança da Informação que podem avaliar uma prestação de serviço ou parceria são: Privacidade, SecOps – BlueTeam, NetSec – Arquitetura de SI, AppSec – Application Security e Service Desk N3.
- Analisar os requisitos da solicitação de contratação, parceria ou qualquer tipo de procedimento para PoC ou homologação de produtos e serviços.
- Indicar com a visão de Segurança da Informação os fornecedores/parceiros relevantes que devem ser comunicados ao BACEN e SUSEP, sendo que a comunicação aos órgãos deve ser realizada pelo Jurídico.
- Registrar toda a documentação correspondente a Segurança da Informação, inclusive os documentos de revisão de relatório SOC 2 tipo 2.
- Revisar fornecedores/parceiros relevantes com base no relatório SOC 2 tipo 2, pelo menos anualmente.

7.4. Continuidade dos Negócios

- Analisar os requisitos da nova solicitação de contratação ou qualquer tipo de procedimento para PoC ou homologação de produtos e serviços.
- Avaliar e dar um parecer de Continuidade dos Negócios para que o fornecedor implemente as recomendações necessárias para cada tipo de produto ou serviço específico.

- Verificar as respostas dos fornecedores em cenários de indisponibilidade do produto ou serviço.
- Revisar e indicar com a visão de Continuidade quais fornecedores relevantes de Continuidade devem ser comunicados ao BACEN e SUSEP, sendo que a comunicação aos órgãos deve ser realizada pelo Jurídico.
- Solicitar assinatura e registrar toda a documentação correspondente a Continuidade dos Negócios.

7.5. Compliance Offshore

- Intermediar comunicações ou pedidos de entidades reguladores (NFA, FINRA, SEC entre outros) aplicáveis nos EUA em casos de auditoria.

7.6. Riscos Corporativos

- Avaliar os Fornecedores que apresentem risco alto/muito alto para o Grupo XP Inc. ou que não possuam os requisitos de Segurança da Informação.

8. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

8.1 CONDUTA DE FORNECEDORES/TERCEIROS E PARCEIROS NO AMBIENTE DO GRUPO XP INC

8.1.1. Acesso Lógico e Uso Aceitável

- O acesso lógico ao ambiente da rede interna do Grupo XP Inc. deverá ser solicitado pelo gestor responsável pela contratação ou parceria, por meio da ferramenta de Catálogo de serviços da XP. A solicitação será avaliada e aprovada de acordo com a necessidade, seguindo as diretrizes corporativas de Segurança da Informação.

- Para fornecedores/terceiros e parceiros que precisam acessar o ambiente do Grupo XP Inc remotamente, o gestor responsável pelo contrato deve providenciar notebook XP ou DaaS (Desktop as a Service) com o acesso através de usuário único e individual, limitado aos recursos de trabalho e ambientes necessários para o desempenho de suas funções;

- É dever do gestor responsável pelo fornecedor/terceiro e parceiro informar a validade do contrato de prestação de serviços ou parceria no momento da solicitação do acesso, bem como solicitar a exclusão do acesso quando não houver mais necessidade;

- É vedada a utilização de computadores de fornecedor/terceiros e parceiros e/ou computadores pessoais/corporativos.

- É proibido o acesso, *download* ou distribuição de qualquer conteúdo que viole direitos autorais e de propriedade dentro da rede do Grupo XP Inc. Da mesma forma, não é permitido acesso ou distribuição de conteúdo pornográfico de qualquer natureza ou conteúdo que viole o Estatuto da Criança e Adolescente;

- Quando aplicável, o usuário e senha disponibilizado para o fornecedor/terceiro e parceiro são de uso exclusivo e não podem ser divulgados ou compartilhados;

- O fornecedor/terceiro e parceiro deve manter suas credenciais de acesso seguras, sendo de sua responsabilidade qualquer utilização indevida;

- É responsabilidade da empresa terceira/parceira comunicar qualquer desligamento de seus colaboradores para que eles tenham seus acessos devidamente cancelados no ambiente do Grupo XP Inc.; e

- É proibido o compartilhamento de usuários e senhas.

8.1.2. Notificação de Incidentes de Segurança da Informação

Incidentes e não-conformidades de Segurança da Informação que sejam de conhecimento do terceiro/parceiro devem ser imediatamente comunicados ao gestor do contrato para que este realize o processo de notificação de incidente pelos meios formais.

Uma vez aberto, o processo de triagem, análise, tratamento e resposta segue o mesmo fluxo dos incidentes internos do Grupo XP Inc.

Para detalhamento dos tipos de incidente e suas criticidades, consulte o Anexo I desta Política.

8.1.3. Segurança de Equipamentos

- Cada usuário é responsável pela proteção e integridade física dos dispositivos físicos ou virtuais contendo informação do Grupo XP Inc que estão sob sua guarda; e
- Cada usuário deve estar ciente que o uso de qualquer recurso de TI no ambiente do Grupo XP Inc, está sujeito a vistoria, sempre que a lei local permitir.

8.1.4. Violação de Conduta

São consideradas violações à esta Política as seguintes situações, não se limitando a:

- Quaisquer ações ou situações que possam expor o Grupo XP Inc. à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos de informação;
- Uso indevido de dados corporativos, divulgação não autorizada de informações, segredos comerciais ou outras informações sem a permissão expressa do Grupo XP Inc.;
- Uso de dados, informações, equipamentos, software, sistemas, códigos ou outros recursos tecnológicos para propósitos ilícitos que possam incluir a violação de leis, de regulamentos internos e externos, da ética ou de exigências de organismos reguladores da área de atuação do Grupo XP Inc.; e
- A não-comunicação imediata de quaisquer descumprimentos da Política.

8.2. CONTROLES DE SEGURANÇA E PRIVACIDADE NO AMBIENTE DO FORNECEDOR/TERCEIRO E PARCEIRO

Se a prestação de serviço envolver compartilhamento e/ou tratamento de dados pessoais gerais e/ou sensíveis, o fornecedor/parceiro em questão será cadastrado pelo time de Governança de Segurança da Informação em uma ferramenta de verificação de cyber-saúde, que analisa as vulnerabilidades expostas para a internet a partir de um domínio. Essa plataforma provê score de pontuação de Segurança com 5 níveis de classificação (A, B, C, D e F), onde o score A é a pontuação máxima.

Minimamente, o score geral deste fornecedor/terceiro e prestador deverá ser B, recebendo um relatório de adequação e compliance a fim de atingir o score A. Caso ele não atinja o resultado mínimo para a prestação de seu serviço, ele será reprovado pelo time de Governança de Segurança da Informação, até que implemente as melhorias necessárias geradas pelo plano de recomendações da plataforma ou seja aprovado de forma extraordinária pelo time de Riscos Corporativos da empresa, devidamente formalizado. Caso o fornecedor não possua domínio próprio, a análise será dispensada.

O fornecedor/terceiro e parceiro que venha a oferecer serviços em nuvem, processar e/ou armazenar dados do Grupo XP Inc. em seu ambiente, deve seguir as seguintes diretrizes de Segurança da Informação, dispostas nesta política:

8.2.1. Privacidade

- Apresentar por meio de documentação o fluxo dos dados do Grupo XP Inc. no ambiente do fornecedor/terceiro e parceiro, contendo todo o seu ciclo de vida (coleta, processamento, armazenamento, compartilhamento e exclusão).
- Informar o Grupo XP Inc. quais informações são coletadas, para qual finalidade, qual a hipótese legal se embasa o tratamento do dado, onde são armazenadas e por quanto tempo, bem como minimizá-las sempre que possível.
- Possuir uma avaliação de impacto relacionada aos dados pessoais gerais e/ou sensíveis de um titular (RIPD/DPIA), assim como possuir um processo que conceda acesso irrestrito à XP às suas informações processadas e armazenadas, previstas no escopo do serviço prestado.
- Possuir um processo de *opt-in* e *opt-out* para expressão prévia e livre do titular de dados acerca do compartilhamento por meio de uma prestação de serviço/parceria.
- Para fornecedores Open Banking ou Open Finance, é vedada a contratação de parcerias com o objetivo de que o parceiro contratado atue em nome da instituição contratante para fins de compartilhamento.

8.2.2. Controle de Acesso

- Possuir documentado um processo de Gerenciamento de Acessos;
- Dar acesso irrestrito ao Grupo XP Inc aos dados e informações armazenadas ou a serem processadas do Grupo XP Inc, conforme os serviços específicos definidos, prezando pela confidencialidade, integridade, disponibilidade e pela capacidade de recuperação destes dados e informações;
- Dar visibilidade aos procedimentos e controles utilizados para prestar os serviços, como descrito no item acima, em especial, para a identificação e a segregação dos dados do Grupo, por meio de controles físicos ou lógicos;
- Limitar o uso de contas compartilhadas ou usuários genéricos, manter controles relacionados a login, como forçar alteração de senha no primeiro acesso, bloquear o usuário com determinadas tentativas inválidas, exigir padrão de senha complexa, dentre outras;
- Possuir um processo formalizado de concessão, alteração e revogação de acessos, principalmente aqueles com ações privilegiadas.
- Estabelecer métodos para controle de acesso físico e lógico de visitantes; e
- Possuir controles de VPN e afins para acesso remoto dos colaboradores.

8.2.3. Gestão de Vulnerabilidade

- Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, evidenciando os seus melhores esforços usando de procedimentos e controles, que abranjam, no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de dados, a realização periódica de testes e varreduras para detecção de vulnerabilidade, a aplicação de *patches* de

segurança, a aplicação de *hardening* em seus servidores e estações de trabalho, a proteção contra *softwares* maliciosos e bloqueio de softwares não homologados, o estabelecimento de mecanismos de rastreabilidade e de segmentação da rede de computadores, a manutenção de cópias de segurança dos dados e das informações.

8.2.4. Monitoramento dos Serviços e Gestão de Incidentes

- Assegurar que dispõe do mais alto nível de capacidade no provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados, bem como garantir o cumprimento da legislação e da regulamentação em vigor, além de aderir todas as certificações exigidas pela XP Inc., conforme descrito no tópico 8.2.8, e/ou BACEN para a execução dos serviços contratados; e
- Informar e dar acesso o Grupo XP Inc., quando solicitado, sobre os recursos de gestão adequados ao monitoramento dos serviços contratados.
- Possuir equipes e ferramentas dedicadas para o monitoramento de capacidade e disponibilidade dos seus ativos, correlacionando alertas e gerando alertas de incidentes de forma automatizada;
- Possuir um processo estruturado de Resposta a Incidentes, contemplando a categorização dos incidentes e *runbooks* para tratamento e resolução de incidentes já conhecidos.
- Fornecer, quando solicitado, informações relacionadas a quantidade de incidentes ocorridos no período de 12 meses, classificando-os pela sua relevância;
- Manter o Grupo XP Inc. permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

8.2.5. Segurança no Desenvolvimento de Sistemas

- Desenvolver levando em consideração os padrões de segurança e privacidade (no âmbito da Lei Geral de Proteção de Dados) aceitos pelo mercado (Privacy and Security by Design);
- Descrever os recursos de segurança e os dados acessados pelas aplicações, os quais devem ser avaliados pela área de Segurança de Informação (AppSec – *Application Security*) durante a fase de homologação (Ex: Especificação técnica e/ou Diagrama Funcional);
- Utilizar rotinas de validação de integridade para prevenir erros, seja involuntário ou intencional, utilizando de dados fictícios, anonimizações e mascaramento em ambiente não produtivo;
- Realizar análise de segurança com ferramentas SAST/DAST no código-fonte;
- Realizar análise de segurança em suas aplicações (EHT e testes de intrusão);
- Prever as validações de segurança no processo de qualidade e verificação de código. No mínimo, devem ser consideradas aquelas que constam no OWASP TOP 10, conforme detalhado no documento "Norma de Desenvolvimento Seguro" interna.
- Prever, em caso de plataformas de roteamento de cliente, requisitos mínimos descritos na resolução CVM 35 art. 18 e executar *pentest* de forma semestral, bem como compartilhar todos os relatórios do teste para o Grupo XP Inc.
- Ter mecanismos para proteção de APIs.

8.2.6. Continuidade dos Negócios, Gestão, Retenção e Armazenamento de Dados.

- Definir um programa de continuidade de negócios para assegurar que possíveis incidentes não afetem os serviços prestados ao Grupo XP Inc., contemplando especialmente o plano de recuperação de desastres, com testes regulares dos controles de asseguração a fim de se verificar o quão preparada a empresa Fornecedora/Terceira e Parceira está para casos reais;

- Informar e dar acesso o Grupo XP Inc., quando solicitado, sobre as medidas de segurança para a transmissão e armazenamento dos dados e informações, bem como o seu descarte, utilizando procedimentos seguros de exclusão (mídia e papel);

- Possuir um processo de execução de backups, que seja realizado periodicamente nos ativos que armazenam informações do Grupo XP Inc., de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes;

- Possuir banco de dados com trilha de auditoria habilitada para acessos e comandos aos ativos que armazenam informações do Grupo XP Inc. devem;

- Ativos que armazenam informações do Grupo XP Inc. devem possuir encriptação de dados pessoais.

8.2.7. Treinamento e Conscientização

- Possuir um programa de treinamento anual de conscientização em Segurança da Informação e Privacidade de Dados para todos os colaboradores, contemplando a aplicação obrigatória do Código de Conduta do fornecedor para funcionários recém-admitidos.

- Contemplar em seu programa de treinamento e conscientização de Segurança e Privacidade de dados, campanhas como *phishing*, orientação sobre engenharia social, palestras externas, boletins informativos de Segurança da Informação e Privacidade de Dados etc.

8.2.8. Serviços e Certificações

- Notificar, de imediato, sobre a subcontratação de serviços relevantes para o Grupo XP Inc.;

- Observar, nos casos em que os serviços de computação e/ou armazenamento de dados em nuvem sejam prestados em localidades primárias no exterior, a existência de convênio entre o BACEN e as autoridades supervisoras dos países onde os serviços poderão ser prestados, devendo assegurar que a prestação dos referidos serviços não cause prejuízos ao seu funcionamento, nem embaraço à atuação do BACEN;

- É desejável possuir reconhecimentos de segurança da informação ou continuidade dos negócios, comprovados por certificação e/ou relatórios de auditorias externas independentes, podendo ser o relatório SOC 2 tipo 2. Nos casos de fornecedor/terceiro e parceiro de negócio relevante, é obrigatório possuir e disponibilizar ao Grupo XP Inc. o relatório SOC 2 Tipo 2.;

- Informar e dar acesso o Grupo XP Inc., quando solicitado, sobre as certificações necessárias para a prestação dos serviços, bem como aos relatórios relacionados aos controles utilizados na prestação dos serviços contratados, elaborados por empresa de auditoria independente especializada; e

- Possuir mecanismos para comunicar anomalias ou incidente de segurança relevantes o Grupo XP Inc., aos indivíduos envolvidos e à Autoridade Nacional de Proteção de Dados (ANPD) para casos em que o

fornecedor/terceiro e parceiro de negócio atua como Controlador. Nos casos de Operador dos dados, em incidentes com dados que o Grupo XP Inc. é o Controlador, o fornecedor/terceiro e parceiro de negócio deve comunicar imediatamente o Grupo, conforme descrito no tópico 8.2.4. É vedado a comunicação ao regulador nos casos em que o Controlador dos dados seja o Grupo XP Inc.

9. GESTÃO DE RISCOS CORPORATIVOS

As áreas especialistas de Gestão de Fornecedores, Jurídico, Segurança da Informação e Continuidade dos negócios, definem com uma visão independente o nível de risco da prestação de serviço. O nível de risco varia entre baixo, médio, alto e muito alto. No caso de uma destas áreas informarem que em sua visão o fornecedor/terceiro e parceiro tem um risco alto ou muito alto, o time de Riscos Corporativos é acionado mesmo que não haja uma reprovação. A visão de risco independente não define o risco final da prestação de serviço.

Caso um fornecedor/terceiro e parceiro não atenda aos requisitos/documentações exigidos, apresente fragilidades que exponha o Grupo XP Inc a riscos ou possua um risco alto/muito alto determinado pelas áreas especialistas, será realizada uma análise interna junto a área de Riscos Corporativos, gestor do contrato e demais áreas aplicáveis para endereçamento da resposta adequada aos riscos ou reprovação definitiva da prestação do serviço ou parceria.

10. DESCUMPRIMENTO DAS NORMATIVAS, PROCESSOS OU INSTRUÇÕES DE TRABALHO RELATIVOS À SEGURANÇA

O descumprimento das Políticas, normas e procedimento de Segurança da Informação implicará a abertura de procedimento para apuração das possíveis irregularidades (“Incidente de Segurança da Informação”) e, conforme o caso, ensejará a aplicação das penalidades cabíveis, nos termos da legislação vigente, como notificações, advertências ou ainda a rescisão motivada do contrato de trabalho, estágio ou prestação de serviços com a ciência do gestor responsável pelo profissional.

Vale ressaltar que os colaboradores infratores reincidentes (necessariamente na mesma categoria/natureza de incidente) são direcionados para o time de Compliance, a fim de serem registradas orientações, advertências e/ou outras medidas cabíveis. Todas as ações realizadas pelo time de Compliance impacta (de acordo com o modelo de penalidade escolhido) diretamente no Score de Conduta do colaborador.

Acessos e permissões não condizentes com as diretrizes estabelecidas nessa Normativa, devem ser concedidos em caráter excepcional conforme Procedimento de tratativa de exceções gerenciado por Riscos Corporativos.

As regras aqui estabelecidas deverão ser amplamente divulgadas, bem como revisadas periodicamente junto àqueles que poderão ser afetados por suas diretrizes. Em nenhum momento será admitido, a qualquer colaborador, alegar o desconhecimento das diretrizes de Segurança da Informação para justificar violações ou falta de cumprimento delas.

ANEXO I

Matriz de Eventos e Classificação de Incidentes de Segurança da Informação.

Nível	Característica do Risco	Categoria	Prazo para Reporte	Procedimento a adotar
Muito alto	Os problemas enfrentados ou antecipados têm o potencial de interromper todas as operações e processos críticos por um longo período. Evento que pressupõe um dano financeiro significativo, quebra de sigilo financeiro dos clientes de forma massiva ou acesso direto a informações consideradas críticas.	Ataques Externos	Em até 2 horas da identificação	Comunicar por e-mail o responsável pela intermediação do contrato entre o Fornecedor/Terceiro e Parceiro e o Grupo XP Inc.
		Mau uso ou abuso interno		
		Vazamento ou roubo		
		Interrupção de serviços		
		Erro Humano		
		Vulnerabilidades		
		Outros		
Alto	É provável que ocorra uma degradação observável dos principais serviços e processos críticos com o potencial de afetar o valor ou a reputação organizacional. Quebra de sigilo financeiro dos clientes de forma isolada ou acesso direto a informações consideradas restritas.	Ataques Externos	Em até 6 horas da identificação	
		Mau uso ou abuso interno		
		Vazamento ou roubo		
		Interrupção de serviços		
		Erro Humano		
		Vulnerabilidades		
		Outros		
Médio	É provável que haja um impacto mensurável nas operações e processos críticos, mas o risco de afetar valor ou reputação organizacional é considerado baixo. Evento que caso não tenha o devido tratamento possa evoluir para situação de risco elevado.	Ataques Externos	Em até 24 horas da identificação	
		Mau uso ou abuso interno		
		Vazamento ou roubo		
		Interrupção de serviços		
		Erro Humano		
		Vulnerabilidades		
		Outros		