Política de Segurança da Informação para Terceiros

SUMÁRIO

1. INTRODUÇÃO

A informação é um dos elementos de negócio mais importantes para o Grupo XP Inc. ("Grupo") e, dessa forma, manter a sua confidencialidade, integridade e disponibilidade são fatores críticos para o sucesso para o nosso Grupo.

A Política de Segurança da Informação para Terceiros 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.

2. ABRANGÊNCIA

Todas as empresas que estabelecem contratos formais com o Grupo, se obrigam a cumprir os requisitos de Segurança da Informação aqui definidos.

O cumprimento das diretrizes estabelecidas é fundamental para a efetiva relação de parceria firmada para atingir níveis adequados de proteção à informação.

3. DOCUMENTOS RELACIONADOS

- Política de Segurança da Informação

4. RESPONSABILIDADES

4.1. Área Contratante de Serviços de Fornecedores

- Quando da contratação de fornecedores que tenham colaboradores que venham a acessar a rede interna e os dados do Grupo, a área contratante deverá garantir que todos estejam cientes dessa política de segurança da informação.

4.2. Prestador de Serviços/Fornecedores

- É de responsabilidade dos prestadores de serviços do Grupo, observar e seguir as orientações estabelecidas para o cumprimento da presente Política de Segurança da Informação; e
- Todas as atividades executadas devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras com relação à Segurança da Informação.
- É vedada a contratação de parcerias entre instituições autorizadas a funcionar pelo BCB ou em que o parceiro contratado atue em nome da instituição contratante para fins de compartilhamento. Para a possibilidade de haver contratos de parcerias com entidades não reguladas pelo BCB, 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.

5. DIRETRIZES

5.1. Geral

Os terceiros prestadores de serviços/fornecedores devem cumprir com todos os requisitos da legislação brasileira aplicáveis, e devem comprometer-se a seguir integralmente os itens 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;
- Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas 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 ao Grupo XP Inc. qualquer descumprimento da Política de Segurança da Informação para Terceiros.
- Em caso de armazenamento e/ou processamento de dados pessoais de clientes, funcionários, financeiro ou prestação de serviço de nuvem para o Grupo, deverá estar de acordo com o TCG - "Termos e Condições Gerais de Fornecimento".
- Prestadores de Serviço/Fornecedores classificados como críticos devido a armazenamento e/ou processamento de dados pessoais de clientes, funcionários, financeiro ou prestação de serviço de nuvem devem passar por processo de avaliação de Segurança da Informação, através de SelfAssessment de SI na pré-contratação ou contratação e posteriormente verificação *in-loco*. Serão dispensados da avaliação *in-loco* prestadores de serviço/fornecedores que possuem relatório de auditória externo válido (e.g. SOC 2).

6. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

6.1 CONDUTA DE TERCEIROS NO AMBIENTE DO GRUPO XP INC

6.1.1. Acesso Lógico e Uso Aceitável

- O acesso lógico ao ambiente da rede interna do Grupo deverá ser solicitado pelo gestor responsável pela contratação, por meio da ferramenta de chamados. A solicitação será avaliada e aprovada de acordo com a necessidade, seguindo as diretrizes corporativas de Segurança da Informação. O acesso só deve ser concedido após conclusão do treinamento de segurança da informação e ciência do Termo de Responsabilidade;
- Para prestadores de serviço/fornecedores que precisam acessar o ambiente do Grupo remotamente, o gestor responsável pelo contrato deve providenciar acesso através de usuário único e individual com acesso a VPN, no qual somente poderá ter acesso aos recursos de trabalho e ambientes necessários para o desempenho de suas funções;
- É dever do gestor responsável pelo terceiro informar a validade do contrato de prestação de serviços no momento da solicitação do acesso, bem como solicitar a exclusão do acesso quando não houver mais necessidade;
- Os computadores de terceiros não podem ser conectados na rede interna do Grupo sem a aprovação prévia da TI, sendo que estes deverão estar protegidos por software antivírus/*anti-malware* e demais softwares devidamente licenciados;

- É proibido o acesso, download ou distribuição de qualquer conteúdo que viole direitos autorais e de propriedade dentro da rede do Grupo. 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 terceiro são de uso exclusivo e não podem ser divulgados ou compartilhados;
- O terceiro deve manter suas credenciais de acesso seguras, sendo de sua responsabilidade qualquer utilização indevida;
- É responsabilidade da empresa terceira comunicar qualquer desligamento de seus colaboradores para que eles tenham seus acessos devidamente cancelados no ambiente do Grupo; e
- É proibido o compartilhamento de usuários e senhas entre os prestadores de serviços.

6.1.2. Notificação de Incidentes de Segurança da Informação

Incidentes e não-conformidades de Segurança da Informação que sejam de conhecimento do terceiro 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.

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

6.1.3. Segurança de Equipamentos

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

6.1.4. 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 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;
- Uso de dados, informações, equipamentos, software, sistemas 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; e
- A não-comunicação imediata de quaisquer descumprimentos da Política.

6.2. CONTROLES DE SEGURANÇA E PRIVACIDADE NO AMBIENTE DO TERCEIRO

Ao ser requisitado pela área de negócio, o fornecedor em questão será cadastrado pelo time de Governança em Segurança da Informação em uma ferramenta de verificação de sua cyber-saúde. 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 prestador deverá ser B, recebendo um relatório de adequação e compliance a fim de atingir o score A. Caso o mesmo não atinja o resultado mínimo para a prestação de seu serviço, ele será negado pelo time de Governança em 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 da empresa, devidamente formalizado.

O fornecedor que venha a oferecer serviços em nuvem, processar e/ou armazenar dados do Grupo em seu ambiente, deve seguir as seguintes diretrizes de segurança da informação, dispostas também no documento de Self Assessment enviado e mantido pela área de Segurança da Informação:

6.2.1. Privacidade

- Apresentar por meio de documentação o fluxo dos dados da XP no ambiente do fornecedor, contendo todo o seu ciclo de vida (coleta, processamento, armazenamento, compartilhamento e exclusão).
- Informar ao Grupo XP Inc. quais informações são coletadas, para qual finalidade, qual a base legal que 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 de um titular (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 cliente acerca do compartilhamento por meio de uma parceria.
- Para fornecedores Open Banking, é vedada a contratação de parcerias com o objetivo de que o parceiro contratado atue em nome da instituição contratante para fins de compartilhamento.

6.2.2. Controle de Acesso

- Possuir documentado um processo de Gerenciamento de Acessos;
- Dar acesso irrestrito aos dados e informações armazenadas ou a serem processadas, 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 de clientes do Grupo, por meio de controles físicos ou lógicos;
- Não permitir o uso de contas compartilhadas ou usuários genéricos, tal qual mantém controles relacionados a login, como forçar alteração no primeiro acesso, bloquear o usuário com determinadas tentativas inválidas, exigir padrão de senha complexa;
- Possuir um processo formalizado de concessão, alteração e revogação de acessos, principalmente àqueles 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 em período de *home office*.

6.2.3. 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,

6.2.4 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 pelo Grupo e/ou BACEN para a execução dos serviços contratados; e

- Informar e dar acesso ao Grupo, 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 tickets 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; e

- 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.

6.2.5. 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 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 ou anonimizações e em ambiente não produtivo;

- Realizar análise de segurança 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.

6.2.6. 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, contemplando especialmente o plano de recuperação de desastres, testando regularmente os controles de asseguração a fim de se verificar o quão preparada a empresa está para casos reais;

- Informar e dar acesso ao 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, o qual 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; e

6.2.7. Treinamento e Conscientização

- Assegurar da existência de um programa anual de treinamento e conscientização em Segurança da Informação e Privacidade de Dados para todos os colaboradores, sendo que o mesmo deve ser contemplado com 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 algumas campanhas como *phishing*, orientação sobre engenharia social, palestras externas, boletins informativos de SI e Privacidade de Dados etc.

- Os terceiros que acessarem ou processarem dados pessoais e/ou informações sensíveis devem ter ciência desta Política e do que diz respeito a treinamento de segurança da informação proveniente pelo Grupo XP Inc.

6.2.8. 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.

- Possuir reconhecimentos de segurança da informação ou continuidade dos negócios, comprovados por relatórios de auditorias externas independentes;

- Informar e dar acesso ao 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 ao Grupo XP Inc., aos Indivíduos envolvidos e à Autoridade Nacional de Proteção de Dados.

7. AVALIAÇÕES PERIÓDICAS

O Grupo poderá realizar, sempre que achar necessário, avaliações para atestar sobre a efetividade da implementação dos controles apresentados neste documento, devendo para isso, comunicar o parceiro com 30 dias de antecedência.

8. SANÇÕES

A violação a um controle ou a não-aderência à Política de Segurança da Informação para Terceiros e suas definições são consideradas faltas graves ou violações, podendo ser aplicadas penalidades ou sanções cabíveis de acordo com as Políticas internas do Grupo XP Inc.

9. DEFINIÇÕES

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

Controladas: As sociedades constituídas no Brasil nas quais a Grupo é Acionista Controladora.

Grupo XP Inc.: A Companhia, suas Controladas e Coligadas constituídas no Brasil, consideradas em conjunto, incluindo o Banco XP e a XP Investimentos.

Companhia: XP Investimentos S.A.

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 Terceiro 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		