# Política de Segurança da Informação para Terceiros

## FOLHA DE CONTROLE

### Informações Gerais

| | |
|---|---|
| **Título** | Política de Segurança da Informação para Terceiros |
| **Número de Referência** | POL_001 |
| **Número da Versão** | V1 |
| **Classificação da Informação** | Público |
| **Status** | Nova |
| **Escopo do Negócio** | Terceiros do Grupo XP |
| **Escopo da Geografia** | Brasil |
| **Procedimentos e Outros Documentos Relacionados** | Resolução do Conselho Monetário Nacional do Banco Central do Brasil nº 4.658/2018. |
| **Dispensa da Política** | N/A |
| **Palavras-chave para Procura Rápida** | PSI, política, norma, regras, obrigações, responsabilidade, segurança da informação |

### Histórico de Versões

| Versão | Motivo da Alteração | Data | Autor | Departamento |
|---|---|---|---|---|
| 1 | Versão Inicial<br>Revisão<br>Revisão | 19/03/2019<br>19/03/2019<br>15/04/2019 | Dalton Reis<br>Bruno Stuani<br>Paulo Fernandes | Segurança da Informação<br>Segurança da Informação<br>Paulo Fernandes |

| | | |
|---|---|---|
| **Aprovado por:** | Guilherme Benchimol<br>Diretor | Fabricio Cunha de Almeida<br>Diretor |
| **Data:** 15/04/2019 | | |

**SUMÁRIO**

## 1. INTRODUÇÃO

A informação é um dos elementos de negócio mais importantes para o Grupo XP 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 ("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.

## 2. ABRANGÊNCIA

Todas as empresas que estabelecem contratos formais com o Grupo XP, 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. VIGÊNCIA

Esta Política pode ser revisada anualmente ou, quando necessário, caso haja alguma mudança nas normas do Grupo XP, alteração de diretrizes de segurança da informação, objetivos de negócio ou se requerido pelo regulador local.

## 4. DOCUMENTOS RELACIONADOS

Política de Segurança da Informação do Grupo XP

## 5. RESPONSABILIDADES

### 5.1 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 XP, a área contratante deverá garantir que todos estejam cientes dessa Política.

### 5.2 Prestador de Serviços

- É de responsabilidade dos prestadores de serviços do Grupo XP, observar e seguir as orientações estabelecidas para o cumprimento da Política;
- Todas as atividades executadas devem observar a legislação vigente e a normatização de órgãos e entidades reguladoras com relação à Segurança da Informação.

## 6. DIRETRIZES

### 6.1 Geral

Os terceiros prestadores de serviços 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 XP;

- 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 e seu mercado de atuação;
- Selecionar os mecanismos de segurança da informação, balanceando fatores de risco, tecnologia e custo;
- Comunicar imediatamente ao Grupo XP qualquer descumprimento da Política.
- Em caso de armazenamento ou processamento de dados do Grupo XP, deverá estar de acordo com o TCG - "Termos e Condições Gerais de Fornecimento".
- Critérios a serem avaliados durante a contratação para o envio do TCG:

Requisitos de infraestrutura

- O fornecedor processa dados do Grupo XP em sua infraestrutura? (OU)
- O fornecedor armazena dados do Grupo XP em sua infraestrutura? (OU)
- O fornecedor provê serviços de computação em nuvem?

Requisitos de relevância

- Suporta um processo ou uma aplicação crítica que poderia causar interrupção em caso de parada do fornecedor? (OU)
- O fornecedor utiliza informações de clientes?

# 7. REQUISITOS DE SEGURANÇA DA INFORMAÇÃO

## 7.1 CONDUTA DE TERCEIROS NO AMBIENTE DO GRUPO XP

### 7.1.1 Acesso Lógico e Uso aceitável

- O acesso lógico ao ambiente da rede interna do Grupo XP 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;
- 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 XP 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 XP. 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 os mesmos tenham seus acessos devidamente cancelados no ambiente do grupo XP;
- É proibido o compartilhamento de usuários e senhas entre os prestadores de serviços.

### 7.1.2 Notificação de Incidentes de Segurança da Informação

Incidentes e não-conformidades de Segurança da Informação que sejam de conhecimento do terceiro devem ser imediatamente notificados por meio da abertura de chamado no Portal da Intranet (https://xpinvestimentos.service-now.com/sp -> Página Inicial -> Catálogo de Serviços -> Serviços de Segurança da Informação -> Incidente de Segurança). Caso o prestador de serviço não tenha acesso à Intranet, o mesmo deverá comunicar ao gestor do contrato para que o mesmo realize o processo de notificação do incidente.

### 7.1.3 Segurança de Equipamentos

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

### 7.1.4 Violação de Conduta

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

- Quaisquer ações ou situações que possam expor o Grupo XP 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;
- 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 XP;
- A não-comunicação imediata de quaisquer descumprimentos da Política.

## 7.2 CONTROLES DE SEGURANÇA NO AMBIENTE DO TERCEIRO

O fornecedor que venha a oferecer serviços em nuvem, processar ou armazenar dados do Grupo XP em seu ambiente, deve seguir as seguintes diretrizes de segurança da informação:

### 7.2.1 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 XP, por meio de controles físicos ou lógicos.

### 7.2.2 Gestão de Vulnerabilidade

- Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, envidando 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 informações, a realização periódica de testes e varreduras para detecção de vulnerabilidade, a proteção contra *softwares* maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.

### 7.2.3 Monitoramento dos Serviços

- 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 XP e/ou BACEN para a execução dos serviços contratados;

- Informar e dar acesso ao Grupo XP, quando solicitado, sobre os recursos de gestão adequados ao monitoramento dos serviços contratados.

### 7.2.4 Gestão de Incidentes

- Possuir um processo estruturado de Resposta a Incidentes;

- Fornecer, quando solicitado, as informações relacionadas a quantidade de incidentes ocorridos no período de 12 meses, classificando-os pela sua relevância;

- Manter o Grupo XP permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

### 7.2.5 Segurança no Desenvolvimento de Sistemas

- Desenvolver levando em consideração os padrões de segurança aceitos pelo mercado;

- 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;

- 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”.

### 7.2.6 Armazenamento de Dados

- Informar e dar acesso ao Grupo XP, quando solicitado, sobre as medidas de segurança para a transmissão e armazenamento dos dados e informações.

### 7.2.7 Continuidade de Negócios

- Definir um programa de continuidade de negócios, para assegurar que possíveis incidentes não afetem os serviços prestados ao Grupo XP.

### 7.2.8 Gestão e Retenção de Dados

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

### 7.2.9 Treinamento e Conscientização

- Assegurar da existência de um programa anual de treinamento e conscientização em Segurança da Informação 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.

### 7.2.10 Subcontratação de Serviços

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

- 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.

### 7.2.11 Certificações e Auditorias independentes

- Informar e dar acesso ao Grupo XP, 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.

## 8. AVALIAÇÕES PERIÓDICAS

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

## 9. SANÇÕES

A violação a um controle ou a não-aderência a essa Política e suas definições são consideradas faltas graves ou violações, podendo ser aplicadas penalidades ou sanções de acordo com os termos contratuais.

## 10. DEFINIÇÕES

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

**Companhia**: XP Investimentos S.A.

**Controladas**: As sociedades nas quais a Companhia é Acionista Controladora.

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

**Informação Confidencial:** Toda e qualquer informação patenteada ou não, verbal ou de qualquer modo apresentada, tangível ou intangível, podendo incluir mas não se limitando a, de natureza técnica, operacional, comercial, financeira, jurídica, know-how, invenções, processos, fórmulas e desenhos, patenteáveis ou não, planos de negócios (*business plans*), métodos de contabilidade, técnicas e experiências acumuladas, planos comerciais, orçamentos, preços, planos de expansão, estratégias comerciais, descobertas, ideias, conceitos, técnicas, projetos, especificações, diagramas, modelos, amostras, fluxogramas, programas de computador, códigos, dados, códigos fonte, discos, disquetes, fitas, planos de marketing e vendas, qualquer informação de clientes, e quaisquer outras informações técnicas, financeiras, jurídicas e/ou comerciais relacionadas ao Grupo XP, seus clientes, parceiros, fornecedores e colaboradores.