# Política de Segurança Cibernética

**SUMÁRIO**

## 1. OBJETIVO

A Política de Segurança Cibernética ("Política") das empresas do Grupo XP Inc. ("Grupo") tem como objetivo assegurar a integridade, disponibilidade e confidencialidade das informações de sua propriedade e/ou sob sua guarda, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, definindo as regras que representam, em nível estratégico, os princípios fundamentais incorporados pelo Grupo para o alcance dos objetivos de segurança da informação.

Essa Política demonstra o compromisso do Grupo em zelar e tratar as informações, seguindo as boas práticas e diretrizes do Grupo frente a LGPD (Lei Geral de Proteção de Dados). Demonstramos também o nosso compromisso com os aspectos regulatórios e estratégicos do Grupo, estando assim, em conformidade com as principais regulamentações vigentes.

Por fim, este documento se destina a todos os usuários do Grupo e quaisquer terceiros que usufruam de sua infraestrutura, e que estejam envolvidos na concepção de soluções, sistemas, processos, produtos ou serviços, conforme previsto na Política de Segurança da Informação para Fornecedores/Terceiros e Parceiros de Negócio.

## 2. ABRANGÊNCIA

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

## 3. VIGÊNCIA, REVOGAÇÃO E CICLO DE REVISÃO

Esse documento entra em vigor a partir da data de sua aprovação e cancela as versões anteriores ou que tratam do mesmo assunto. Esta Política pode ser revisada anualmente ou, quando necessário, caso haja alguma mudança nas normas do Grupo, alteração de diretrizes de segurança da informação, objetivos de negócio ou se requerido pelo regulador local de alguma das Controladas.

## 4. DEFINIÇÕES

**Grupo XP Inc.:** Empresas Controladas pela XP Inc. e suas Coligadas, constituídas no Brasil, consideradas em conjunto.

**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.

**Administradores:** São os membros da Diretoria devidamente constituídos.

**Anti-malware:** Um programa de computador que protege o dispositivo contra software malicioso, como vírus, spyware e ransomware. Ele detecta, bloqueia e remove esses tipos de ameaças para manter o dispositivo seguro.

**Ativo de Informação:** É qualquer dado ou conjunto de dados que possui valor para uma organização, seja em termos de apoio à tomada de decisões, conformidade regulatória, ou vantagem competitiva. Isso inclui informações como documentos, registros, bancos de dados e conhecimento especializado, que são essenciais para as operações e estratégias da empresa.

**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., a XP Serviços Financeiros 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.

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

**Dado Anonimizado:** Dado relativo a titular que não pode ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

**Dado pessoal geral:** Segundo o inciso II, do artigo 5º da LGPD , trata-se de informação relacionada a pessoa natural identificada ou identificável;

**Dado pessoal sensível:**Segundo o inciso II, do artigo 5º da LGPD , trata-se de 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.

**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.

***Deep-web* e *Dark-web*:** A *Deep Web* compreende os recursos e conteúdo da internet não indexados por mecanismos de busca públicos. A *Dark Web* constitui uma subcamada específica da *Deep Web*, formada por conteúdos intencionalmente ocultos e acessíveis exclusivamente por redes e softwares de anonimização, caracterizando-se pelo uso intensivo de criptografia e técnicas de ocultação de identidade. Em conjunto, esses ambientes representam fontes relevantes para monitoramento e inteligência cibernética, especialmente no contexto de vazamento de informações, comercialização de credenciais, planejamento de ataques e outras ameaças à segurança da informação.

**Firewall:** É um dispositivo de segurança que monitora o tráfego de rede de entrada e saída, permitindo ou bloqueando determinado tipo de fluxo.

**Incidente de Segurança:** 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.

**Malware:** Programas maliciosos que são criados com a intenção de causar danos, roubar informações ou comprometer a segurança de computadores e redes. Isto inclui vírus, worms, trojans, spyware, ransomware, entre outros.

**Testes de intrusão ou Penetration Testing (Pentest):** 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.

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

**Token:** É um dispositivo eletrônico adicional para complementar a autenticação do usuário.

**Vulnerabilidade:** É uma deficiência de configuração que, quando explorada por um atacante, pode resultar em uma violação de segurança.

## 5. DISPOSIÇÕES GERAIS

A Política do Grupo tem como objetivo assegurar a confidencialidade, integridade e disponibilidade das informações que são de propriedade ou estão sob a responsabilidade do Grupo. Além disso, estabelece que terceiros, coligadas, parceiros de negócios, fornecedores e prestadores de serviços devem cumprir todos os requisitos estabelecidos, comprometendo-se a seguir integralmente os itens desta política e da Política de Segurança da Informação para Fornecedores/Terceiros e Parceiros de Negócio.

A alta administração possui o compromisso contínuo com a segurança cibernética ao promover a melhoria constante dos procedimentos e práticas relacionadas ao tema. Esse comprometimento está refletido na alocação de recursos adequados, na definição, aprovação e revisão de políticas claras e na liderança ativa para garantir que as medidas de proteção estejam sempre atualizadas e alinhadas às melhores práticas e às exigências regulatórias. Além disso, a alta administração incentiva a cultura de segurança em toda a organização, promovendo treinamentos, avaliações periódicas e a revisão contínua dos processos para fortalecer a resiliência cibernética da instituição.

## 6. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Consideramos que o ativo de informação é o bem mais importantes no mercado financeiro, portanto, tratá-los com responsabilidade é o nosso compromisso. Dessa forma, estamos fundamentados nos princípios de segurança da informação, cujos objetivos constituem a preservação da propriedade da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e compartilhamento de forma controlada, bem como o monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

**Confidencialidade:** garantir que as informações tratadas sejam de conhecimento exclusivo de pessoas especificamente autorizadas;

**Integridade:** garantir que as informações sejam mantidas íntegras, sem modificações indevidas – acidentais ou propositais;

**Disponibilidade:** garantir que as informações estejam disponíveis a todas as pessoas autorizadas a tratá-las.

## 7. INFORMAÇÕES CONFIDENCIAIS

O acesso às informações confidenciais, incluindo dados pessoais gerais e/ou sensíveis, coletadas e armazenadas pelo Grupo é restrito aos profissionais autorizados ao uso direto dessas informações, e necessário à prestação de seus serviços, sendo o uso limitado, devendo respeitar, ainda, as definições de Classificação da Informação previstas. O Grupo preza pela privacidade e proteção das informações no âmbito da Lei Geral de Proteção de Dados (“LGPD”) e da Política de Proteção de Dados.

O Grupo poderá revelar as informações confidenciais nas seguintes hipóteses:

- Sempre que estiver obrigado a revelá-las, seja em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial;
- Aos órgãos de proteção e defesa de crédito e prestadores de serviços autorizados pelo Grupo a defender seus direitos e créditos;
- Aos órgãos reguladores do mercado financeiro; e

- Para outras instituições financeiras, desde que respeitados os parâmetros legais estabelecidos e a autorização previamente concedida pelo cliente. O cliente (titular) reserva-se o direito de revogar essa autorização a qualquer momento.

**Conceito:**

**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 (habilidade e/ou conhecimento adquirido), invenções, processos, fórmulas e desenhos, patenteáveis ou não, planos de negócios, 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., seus clientes, parceiros, fornecedores e colaboradores.

## 8. ESTRUTURA DE GERENCIAMENTO DE SEGURANÇA CIBERNÉTICA

O gerenciamento dos controles de segurança visa assegurar que os procedimentos operacionais sejam desenvolvidos, implantados e mantidos ou modificados de acordo com os objetivos estabelecidos nesta Política.

### 8.1 GESTÃO DE ACESSOS ÀS INFORMAÇÕES

Os acessos às informações são controlados, monitorados, restringidos à menor permissão e privilégios possíveis, revistos periodicamente e revogados tempestivamente ao término do contrato de trabalho do colaborador ou do prestador de serviço.

Os equipamentos e instalações de processamento de informação relevante, mas não se limitando a ela, são mantidos em áreas seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

Os colaboradores do Grupo são treinados, periodicamente, sobre os conceitos de Segurança da Informação e Privacidade de Dados através de um programa efetivo de conscientização e disseminação da cultura de segurança cibernética e proteção de dados.

### 8.2 PROTEÇÃO DO AMBIENTE DO GRUPO

São constituídos controles e responsabilidades pela gestão e operação dos recursos de processamento das informações, visando garantir a segurança na infraestrutura tecnológica do Grupo por meio de um gerenciamento efetivo no monitoramento, tratamento e na resposta aos incidentes, com o intuito de minimizar o risco de falhas e a administração segura de redes de comunicações.

#### 8.2.1 AUTENTICAÇÃO

O acesso às informações e aos ambientes tecnológicos do Grupo deve ser concedido somente a pessoas devidamente autorizadas, observando o princípio do menor privilégio, a segregação de funções e a classificação da informação. Os controles de acesso são formalizados e auditados, e incluem:

- Credenciais individualizadas
- Gestão de contas não nominais

- Gestão de contas de terceiros
- Mecanismos de monitoramento contínuo
- Bloqueios e/ou revogações automáticos
- Remoção imediata de permissões de usuários/terceiros desligados ou transferidos
- Revisões periódicas das autorizações concedidas.

A gestão de acessos se apoia em indicadores acompanhados regularmente, permitindo decisões baseadas em dados e ações de correção sempre que identificadas inconsistências. Além disso, os controles contemplam medidas de proteção contra acessos indevidos, prevenção de vazamento de informações, rastreabilidade das ações de usuários e avaliação contínua de vulnerabilidades.

Tais práticas abrangem não apenas os ambientes internos, mas também sistemas desenvolvidos ou operados por terceiros, assegurando padrões consistentes de segurança e monitoramento contínuo em toda a cadeia tecnológica.

### 8.2.2 CONTROLES DE ACESSO

Os controles de acesso do Grupo são baseados minimamente em autenticação, conforme disposto acima e autorização de acesso. No que tange a autorização de acessos, o Grupo conta com mecanismos de limitação de autenticação ao ambiente do grupo baseado em credenciais e em dispositivos autorizados do Grupo.

Todos os acessos baseados em credenciais, além da autenticação de usuário e senha, há a obrigatoriedade de utilização de múltiplos fatores de autenticação.

A revisão dos acessos de autenticação e de autorização ocorre de forma periódica e tempestiva para usuários internos e externos (terceiros), tendo todas as revisões registradas no sistema interno de controle de acesso.

### 8.2.3 GESTÃO DE CERTIFICADOS DIGITAIS

O Grupo estabelece diretrizes para a gestão e o monitoramento de certificados digitais utilizados em seus ambientes tecnológicos, com o objetivo de prevenir riscos de segurança e atender aos requisitos legais e regulatórios aplicáveis. Sempre que aplicável, são adotados controles para o acompanhamento do ciclo de vida dos certificados digitais, compatíveis com a criticidade dos ambientes e a evolução dos controles institucionais.

A gestão de certificados e assinaturas digitais contempla a rastreabilidade, guarda de informações e/ou segredos de forma centralizada, revogação e validação tempestiva bem como monitoramento relacionado a prevenção de vazamentos das informações.

### 8.2.4 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

O comportamento de possíveis ataques é identificado por meio de controles de prevenção e detecção de intrusão implementados no ambiente através de controles como filtro de conteúdo, ferramenta de detecção de comportamentos maliciosos, antivírus, AntiSpam, proteção de borda, entre outros. Adotamos procedimentos voltados para a prevenção, análise e tratativa dos incidentes.

O Grupo compartilhará os dados referentes aos resultados dos testes de intrusão e correlatos, incidentes relevantes dentro de um período estabelecido bem como ações de resposta aos incidentes e resultados dos testes de Continuidade dos Negócios em formato de relatório. Este relatório será aprovado

pela alta Diretoria conforme regulamentações aplicáveis.

### 8.2.5 PREVENÇÃO A VAZAMENTO DE INFORMAÇÕES

O Grupo possui tecnologias para controle para prevenção de perda de dados visando por garantir que dados confidenciais não sejam perdidos, roubados ou disponibilizados indevidamente no meio externo por usuários não autorizados.

### 8.2.6 TESTE DE INTRUSÃO (PENTEST)

O Grupo conta com Testes de Intrusão (*Pentests*) interno e externo são realizados nas camadas de rede e aplicação com periodicidade minimamente anual. Os testes são divididos em equipes internas e externas, ambos com independência e imparcialidade no teste, gerando relatório com as vulnerabilidades identificados, escopo do teste, correções e/ou planos de ação.

### 8.2.7 GESTÃO DE VULNERABILIDADES

O Grupo conta com um processo estabelecido e documentado a respeito de vulnerabilidades de segurança da informação, tendo a devida classificação e tratamento priorizado conforme o nível de criticidade. A identificação de vulnerabilidades ocorre de forma tempestiva em diversos métodos, incluindo, mas não se limitando a varreduras periódicas em sistemas, recursos computacionais e/ou dispositivos internos e externos e testes de intrusão. As varreduras ou monitoramento podem identificar ativos conectados indevidamente a rede corporativa do Grupo, dispositivos com versões de software obsoletas, entre outros.

No que tange teste de intrusão, há processo estabelecido para tratativa das respectivas vulnerabilidades, conforme detalhado nesta política e nas demais normas internas. Todo o ativo que possa comprometer a segurança da instituição, é imediatamente isolado para devidas providências.

### 8.2.8 RASTREAMENTO DE AMEAÇAS E INTELIGÊNCIA CIBERNÉTICA

O Grupo mantém processo de monitoramento contínuo da sua marca e exposição digital, incluindo verificações e varreduras na internet, *deep web* e *dark web*, realizado por meio de fornecedores especializados integrados ao processo de incidentes. As ocorrências identificadas são registradas, tratadas e acompanhadas por meio dos fluxos institucionais de gestão de incidentes, observando os requisitos legais e regulatórios aplicáveis.

### 8.2.9 CONTROLE CONTRA SOFTWARE MALICIOSO

O Grupo adota mecanismos integrados de proteção contra softwares maliciosos, combinando técnicas heurísticas e comportamentais, monitoramento contínuo dos ativos, bloqueio automático de atividades suspeitas, isolamento de dispositivos potencialmente comprometidos, inspeção de tráfego e gestão centralizada das soluções de segurança. Esses mecanismos são complementados por processos estruturados de atualização contínua dos componentes de proteção, bem como por procedimentos formais de detecção, resposta e melhoria contínua.

Todos os ativos, incluindo computadores, servidores e demais equipamentos, que estejam conectados à rede corporativa ou processem informações do Grupo, devem, sempre que tecnicamente compatível, estar protegidos por soluções anti-malware definidas e homologadas pela área de Segurança da Informação.

### 8.2.10 CRIPTOGRAFIA

Toda solução de criptografia utilizada no Grupo seguem as regras de Segurança da Informação e os padrões de segurança dos Órgãos reguladores. As soluções adotadas pela companhia prezam por acompanhar as melhores tecnologias do mercado.

### 8.2.11 RASTREABILIDADE

Trilhas de auditoria automatizadas são implantadas para todos os componentes de sistema para reconstruir os seguintes eventos:

- Autenticação de usuários (tentativas válidas e inválidas);
- Acesso a informações;
- Ações executadas pelos usuários incluindo, mas não se limitando, a criação, atualização ou remoção de objetos do sistema.

Os eventos de sistemas aplicáveis são monitoramento pela equipe de Segurança da Informação como um dos métodos de detecção. Em caso de eventos positivos, os procedimentos de resposta estão definidos em políticas internas.

Os eventos são retidos em prazo definido pelas políticas internas, observando as regulamentações aplicáveis, sendo a retenção realiza em ferramenta centralizada.

### 8.2.12 PROTEÇÃO E SEGMENTAÇÃO DE REDE

As redes são segmentadas em redes de desenvolvimento, homologação e produção e são segmentadas, quando aplicável, de forma física e lógica de modo que apenas ambientes aprovados se comuniquem entre si, sendo que:

- Computadores conectados à rede corporativa não devem ser acessíveis diretamente pela Internet, com a ressalva para serviço DaaS (Desktop as a Service);
- Não é permitida a conexão direta de rede de terceiros nem a utilização de protocolos de controle remoto aos servidores conectados diretamente na rede corporativa;
- O Grupo implementa controle de rede, tráfego e/ou proteção por firewall.

Toda a comunicação entre e fora das redes, incluindo autenticações de fora da rede corporativa, são controlados e monitorados através de proteção de firewall. Todos os alertas gerados através de eventos possuem a respectiva tratativa de segurança da informação, independente do horário de detecção do evento. Liberações de novas comunicações são realizadas conforme fluxo interno de aprovação de liberação, sendo liberado somente portas e/ou comunicações especificas, preservando e limitando a liberação somente ao estritamente necessário. No que tange comunicações com ambiente externos, é necessário possuir aprovação da esteira de times técnicos que avaliam a contratação/parceria deste fornecedor antes de estabelecer conexão com o ambiente.

Independentemente do método de comunicação, há amplo monitoramento de eventos, contemplando a identificação, tratamento, contenção e erradicação, quando aplicável.

### 8.2.13 DESENVOLVIMENTO SEGURO

O Grupo mantém um conjunto de princípios para desenvolver sistemas de forma segura, garantindo que a segurança cibernética seja projetada e implementada no ciclo de vida de desenvolvimento de sistemas.

### 8.2.14 CÓPIAS DE SEGURANÇA (BACKUP)

O processo de execução de cópias de segurança (backups) é realizado periodicamente, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

### 8.2.13 GESTÃO DE CONFIGURAÇÃO SEGURA EM ATIVOS DE TECNOLOGIA

O Grupo conta com um processo estabelecido, documentado, monitorado e reportado de gestão de configurações seguras em ativos de tecnologia. O processo determina a criação de padrões de configuração segura em ativos como estações e servidores desde a homologação, geração de guia, aplicação, entre outros.

O Grupo conta com o processo de gestão do ciclo de vida dos recursos computacionais da instituição, onde durante a vida ativa do recurso há a garantia de aplicabilidade de correções de segurança, configurações seguras, monitoramento, entre outros.

## 8.3 CONTINUIDADE DOS NEGÓCIOS

O processo de continuidade de negócios é implementado por meio do mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres. Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados na nuvem.

## 8.4 SEGURANÇA CIBERNÉTICA EM FORNECEDORES/TERCEIROS E PARCEIROS

O Grupo adota práticas estruturadas para assegurar que fornecedores/terceiros e parceiros que prestam serviços tecnológicos ou tratam dados de escopo da Lei Geral de Proteção de Dados - LGPD mantenham padrões rigorosos de segurança cibernética, em conformidade com as regulamentações aplicáveis e com as diretrizes internas. Esses terceiros devem implementar controles eficazes para prevenir, identificar e mitigar incidentes ou vulnerabilidades, bem como registrar e comunicar prontamente ao Grupo quaisquer eventos relevantes que possam afetar a integridade, confidencialidade ou disponibilidade das informações.

As vulnerabilidades identificadas a partir dos testes de intrusão e classificadas como de alta ou crítica severidade deve ser tratadas dentro dos prazos estabelecidos na Norma de Gestão de Vulnerabilidades, garantindo aderência aos requisitos internos e mitigação tempestiva dos riscos. Todas as vulnerabilidades identificadas são registradas e disponibilizadas em painéis gerenciais para acompanhamento pelas áreas responsáveis e pela alta administração. Para fins de evidência ou auditoria, resultados de testes de intrusão podem ser apresentados de forma amostral, assegurando transparência, rastreabilidade e conformidade no processo. Esse conjunto integrado de práticas fortalece a capacidade preventiva e reativa do Grupo, garantindo que fornecedores e parceiros operem em alinhamento com os padrões de segurança exigidos pela organização.

O Grupo possui uma Política de Segurança da Informação para Fornecedores, Terceiros e Parceiros de Negócios com a definição de fornecedor/terceiro e parceiro relevante para o Grupo. Os critérios para fornecedor/terceiro e parceiro relevante incluem prestadores de serviço com escopo de conexão com o sistema de pagamentos nacional e todos os fornecedores/terceiros e parceiros cumprem os manuais fornecidos pelo Banco Central do Brasil e as regulamentações aplicáveis.

### 8.4.1 REQUISITOS TÉCNICOS PARA FORNECEDORES/TERCEIROS E PARCEIROS

Como parte desse processo, o Grupo realiza avaliações contínuas de segurança com requisitos mínimos de segurança para cada tipo de prestação de serviço que envolvam estes terceiros. Estes requisitos,

incluem, mas não se limitam a: padrões de autenticação, criptografia, rastreabilidade, integração de sistemas por meio de interfaces eletrônicas, análises estáticas, dinâmicas e de composição de código, entre outros requisitos, além de testes de intrusão internos e externos, conduzidos periodicamente com o objetivo de identificar falhas e validar a eficácia dos controles implementados. Estes requisitos são obrigatórios em todas as tecnologias adquiridas e/ou adotadas pelo Grupo e em caso de desenvolvimento interno, os requisitos são equivalentes.

#### 8.4.1.1 SEGURANÇA EM INTEGRAÇÕES/APIS/INTERFACES

O Grupo estabelece requisitos mínimos de segurança para integrações sistêmicas, incluindo autenticação forte, criptografia, rastreabilidade, limitação de escopo, monitoramento contínuo e testes periódicos, aplicáveis a APIs, webservices e demais interfaces eletrônicas internas e externas.

#### 8.4.1.2 SEGURANÇA EM APLICAÇÕES WEB

O Grupo estabelece requisitos mínimos de segurança para utilização de sistemas e/ou aplicações web (saas), onde além do controle de camadas aplicadas no ambiente, incluem incluindo autenticação padrão, criptografia, rastreabilidade, entre outros.

#### 8.4.1.3 DEMAIS ESCOPOS DE PRESTAÇÃO DE SERVIÇO

O Grupo estabelece demais requisitos mínimos obrigatórios para utilização de outros escopos de prestação de serviço, garantindo o compromisso com a segurança das informações.

### 8.5 PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

O Grupo possui um procedimento efetivo para a contratação e uso de processamento e armazenamento de dados e computação em nuvem, visando a aderência às regras previstas na regulamentação em vigor.

O processamento e armazenamento de aplicações e dados devem ser realizados exclusivamente em ambientes de nuvem previamente aprovados pela área de Segurança da Informação, sejam eles públicos ou privados. Os acessos a esses ambientes devem ser gerenciados e centralizados por meio de plataformas que possibilitem o rastreamento detalhado das solicitações e revisões de forma ágil e tempestiva. Além disso, todos os controles de segurança estabelecidos em normas internas devem ser rigorosamente aplicados. O uso de quaisquer produtos ou serviços oferecidos por provedores de nuvem deve passar por avaliação prévia da Segurança da Informação, garantindo conformidade e mitigação de riscos.

## 9 PRINCIPAIS RECOMENDAÇÕES DE SEGURANÇA AOS CLIENTES e USUÁRIOS

### 9.2 AUTENTICAÇÃO E SENHA

O cliente é integralmente responsável pelos atos praticados por meio de seu identificador de acesso (login), o qual é de uso pessoal, exclusivo e intransferível, associado a senha individual destinada à sua identificação e autenticação no acesso às informações e aos recursos de tecnologia da informação. Com o objetivo de preservar a segurança das informações e dos ambientes tecnológicos, recomenda-se que o cliente adote, no mínimo, as seguintes boas práticas:

- Mantenha a confidencialidade de suas credenciais de acesso, memorizando a senha e abstendo-se de registrá-la em qualquer meio físico ou digital, bem como de compartilhá-la com terceiros;
- Altere imediatamente a senha sempre que houver qualquer indício ou suspeita de comprometimento;

- Utilize senhas fortes, com nível adequado de complexidade, de modo a dificultar sua adivinhação ou quebra;
- Evite o uso de seus equipamentos por terceiros enquanto estiverem conectados ou autenticados com sua identificação;
- Sempre que aplicável, habilite mecanismos adicionais de autenticação, como a autenticação multifator (MFA), por meio de fatores complementares, a exemplo de token, aplicativo autenticador ou mensagem SMS, em especial para acessos a ambientes críticos e regulados.

### 9.3 ANTIVÍRUS

Recomendamos que o cliente mantenha uma solução de antivírus atualizada e instalada no dispositivo utilizado para acesso aos serviços oferecidos pelo Grupo. Além disso, é importante, possuir o sistema operacional atualizado com as últimas atualizações disponíveis.

### 9.4 ENGENHARIA SOCIAL

A engenharia social, no contexto de segurança da informação, refere-se à técnica pela qual uma pessoa procura persuadir outra, muitas vezes abusando da ingenuidade ou confiança, objetivando ludibriar, aplicar golpes ou obter informações sigilosas.

#### 9.4.1 PHISHING, SMISHING e/ou VISHING

Técnica utilizada por cibercriminosos para enganar os usuários, através de envio de *e-mails, SMS* e/ou mensagens de voz maliciosos, a fim de obter informações pessoais como senhas, cartão de crédito, CPF, número de contas bancárias, entre outros. As abordagens dos podem ocorrem das seguintes maneiras:

- Quando procuram atrair a atenção dos usuários, seja pela possibilidade de obter alguma vantagem financeira, seja por curiosidade ou por caridade;
- Quando tentam se passar pela comunicação oficial de instituições conhecidas como: Bancos, Lojas de comércio eletrônico, entre outros sites populares;
- Quando tentam induzir os usuários a preencherem formulários com os seus dados pessoais e/ou financeiros, ou até mesmo a instalação de softwares maliciosos que possuem o objetivo de coletar informações sensíveis dos usuários;

#### *9.4.2 SPAM*

São e-mails não solicitados, os quais geralmente são enviados para muitas pessoas, possuindo tipicamente conteúdo com fins publicitários. Além disso, os Spams estão diretamente associados a ataques de segurança, sendo eles um dos principais responsáveis pela propagação de códigos maliciosos, venda ilegal de produtos e disseminação de golpes.

#### 9.4.3 FALSO CONTATO TELEFÔNICO

São técnicas utilizadas pelos fraudadores para conseguir informações como dados pessoais, senhas, token, código de identificação do aparelho celular (IMEI) ou qualquer outro tipo de informação para a prática da fraude.

#### 9.4.4 FALSA CENTRAL DE ATENDIMENTO

São técnicas utilizadas pelos fraudadores para conseguir informações através do atendimento ao cliente, ao conseguir contato argumenta de que há alguma pendência de atualização cadastral. Na

sequência, pede a confirmação ou atualização do número de telefone. Então é pedido ao cliente que seja informado o código de segurança que foi enviado, a partir disso, o golpista consegue redefinir a senha.

## 10 SAIBA MAIS

Além das recomendações descritas neste documento, disponibilizamos um guia completo de melhores práticas de Segurança da Informação. Acesse pelo link: XP Investimentos.