Política de Segurança Cibernética

SUMÁRIO

[CLASSIFICAÇÃO: INTERNA]

1. OBJETIVO

A Política de Segurança Cibernética ("Política") das empresas do Grupo XP Inc. ("Grupo") visa garantir a proteção, a manutenção da privacidade, 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 e de sua Alta Administração em zelar e tratar as informações de seus clientes, de forma a proporcionar plena satisfação quanto à segurança e privacidade de suas informações. Demonstramos também o nosso compromisso com os aspectos regulatórios e estratégicos do Grupo, estando assim, em conformidade com as principais regulamentações vigentes.

Essa Política é aplicada as empresas do Grupo XP Inc., notadamente para a XP Investimentos CCTVM S.A. ("XP Investimentos"), Banco XP S.A. ("Banco XP") e XP DTVM Ltda. ("XP DTVM"), no que se refere a Resolução nº 4983/21, bem como para as XP Corretora de Seguros Ltda. ("XPCS"). DM10 Corretora de Seguros e Assessoria Ltda. ("DM10") e XP Vida e Previdência S.A. ("XP Seguros"), no que se refere a Circular SUSEP nº 638/21.

2. VIGÊNCIA

Esta Política pode ser revisada 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 local de alguma das Controladas.

3. DEFINIÇÕES

Grupo XP Inc.: XP Investimentos S.A., suas Controladas e 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.

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

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

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° 4.280/13, do CMN.

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, seus clientes, parceiros, fornecedores e colaboradores.

4. PRINCÍPIO DE SEGURANÇA DA INFORMAÇÃO

Consideramos que os ativos de informação são os bens 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.

5. INFORMAÇÕES CONFIDENCIAIS

O acesso às informações confidenciais, incluindo dados pessoais, coletadas e armazenadas pelo Grupo é restrito aos profissionais autorizados ao uso direto dessas informações, e necessário à prestação de seus serviços, sendo limitado o uso para outras tarefas, devendo respeitar, ainda, as definições de Classificação da Informação previstas. O Grupo preza pela privacidade das informações no âmbito da Lei Geral de Proteção de Dados (“LGPD”) e da Política de Privacidade 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;
- Para outras instituições financeiras, desde que dentro dos parâmetros legais estabelecidos para tanto, podendo, nesta hipótese, o usuário, a qualquer tempo, cancelar sua autorização.

6. ESTRUTURA DE GERENCIAMENTO DE SEGURANÇA CIBERNÉTICA

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

6.1 GESTÃO DE ACESSOS ÀS INFORMAÇÕES

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

Os equipamentos e instalações de processamento de informação crítica ou sensível são mantidos em áreas seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

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

6.2 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.

6.2.1 Autenticação

O acesso às informações e aos ambientes tecnológicos do Grupo deve ser permitido apenas às pessoas autorizadas pelo Proprietário da Informação, levando em consideração o princípio do menor privilégio, a segregação de funções conflitantes e a classificação da informação.

O controle de acesso aos sistemas deve ser formalizado e contemplar, no mínimo, os seguintes controles:

- A utilização de identificadores (credencial de acesso) individualizados, monitorado e passíveis de bloqueios e restrições (automatizados e manuais);
- A remoção de autorizações dadas a usuários afastados ou desligados do Grupo, ou ainda que tenham mudado de função;
- A revisão periódica das autorizações concedidas.

6.2.2 Gestão de Incidentes de Segurança da Informação

O comportamento de possíveis ataques é identificado por meio de controles de detecção implementados no ambiente, como filtro de conteúdo, ferramenta de detecção de comportamentos maliciosos, Antivírus, *Antispam*, entre outros. Os incidentes identificados devem seguir o processo de resposta a incidentes.

6.2.3 Prevenção a Vazamento de Informações

É utilizado controle para prevenção de perda de dados, o qual é responsável por garantir que dados confidenciais não sejam perdidos, roubados, mal utilizados ou vazados na *web* por usuários não autorizados.

6.2.4 Testes de Intrusão

Testes de Intrusão interno e externo nas camadas de rede e aplicação devem ser realizados no mínimo anualmente.

6.2.5 Varredura de Vulnerabilidades

As varreduras das redes internas e externas devem ser executadas periodicamente. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

6.2.6 Controle Contra Software Malicioso

Todos os ativos (computadores, servidores, etc.) que estejam conectados à rede corporativa ou façam uso de informações do Grupo, devem, sempre que compatível, ser protegidos com uma solução *anti-malware* determinada pela área de Segurança da Informação.

6.2.7 Criptografia

Toda solução de criptografia utilizada no Grupo deve seguir as regras de Segurança da Informação e os padrões de segurança dos Órgãos reguladores.

6.2.8 Rastreabilidade

Trilhas de auditoria automatizadas devem ser 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 criação ou remoção de objetos do sistema.

6.2.9 Segmentação de Rede

- Computadores conectados à rede corporativa não devem ser acessíveis diretamente pela Internet;
- Não é permitida a conexão direta de rede de terceiros utilizando-se protocolos de controle remoto aos servidores conectados diretamente na rede corporativa;
- Criação, alteração e exclusão de regras nos firewalls e ativos de rede devem ser analisadas por Segurança da Informação e executadas pela área de Tecnologia da Informação.

6.2.10 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.

6.2.11 Cópias de Segurança (Backup)

O processo de execução de backups é realizado, periodicamente, nos ativos de informação do Grupo, de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes.

6.3 CONTINUIDADE DOS NEGÓCIOS

O processo de continuidade de negócios é implementado com o intuito de reduzir os impactos e perdas de ativos da informação após um incidente crítico a um nível aceitável, 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 e os testes previstos para os cenários de ataques cibernéticos.

6.4 PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

Conforme a Resolução BACEN nº 4.893/2021, bem como Circular SUSEP nº 638/21, do Conselho Monetário Nacional, para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, o Grupo assegura-se de um procedimento efetivo para a aderência às regras previstas na regulamentação em vigor.

7. PRINCIPAIS RECOMENDAÇÕES DE SEGURANÇA AOS CLIENTES e USUÁRIOS

7.1 AUTENTICAÇÃO E SENHA

O cliente é responsável pelos atos executados com seu identificador (*login* / sigla), que é único, e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia.

Recomendamos:

- Manter a confidencialidade, memorize e não registre a senha em lugar algum. Ou seja, não contar a ninguém e não anotar em papel;
- Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
- Elaborar senhas de qualidade, de modo que sejam complexas e de difícil adivinhação;
    - Não contemplar na senha informações como datas de nascimento, sequências de letras e números.
- Impedir o uso do seu equipamento e dispositivo móvel por outras pessoas, enquanto este estiver conectado/ "logado" com a sua identificação;
- Bloquear sempre o equipamento ao se ausentar;
- Sempre que possível, habilitar um segundo fator de autenticação (Por exemplo: SMS, Token, etc.).

7.2 ANTIVÍRUS

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

7.3 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 do usuário, objetivando ludibriar, aplicar golpes ou obter informações sigilosas.

7.3.1 *PHISHING*

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

- Quando procuram atrair as atenções dos usuários, seja pela possibilidade de obter alguma vantagem financeira, seja por curiosidade ou seja 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 preencher 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;

Recomendados:

- Não clicar em links suspeitos (por exemplo com erros de português, ofertas e benefícios extraordinários) através de computadores e dispositivos móveis;
- Não expor dados pessoais em redes sociais;
- Instalar em seus dispositivos móveis aplicativos publicados somente nas lojas oficiais;

7.3.2 *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.

7.3.3 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.

8. COMUNICAÇÃO

Quaisquer indícios de irregularidades no cumprimento das determinações desta Política serão alvo de investigação interna e devem ser comunicadas imediatamente aos nossos canais de atendimento.