Política de Segurança Cibernética

SUMÁRIO

1. OBJETIVO 2
2. ABRANGÊNCIA 2
3. VIGÊNCIA, REVOGAÇÃO E CICLO DE REVISÃO 2
4. DEFINIÇÕES 2
5. DISPOSIÇÕES GERAIS 3
6. DESCRIÇÃO DAS REGRAS/PROCEDIMENTOS 4
6.1 PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO 4
7. INFORMAÇÕES CONFIDENCIAIS 4
8. ESTRUTURA DE GERENCIAMENTO DE SEGURANÇA CIBERNÉTICA 5
8.1 GESTÃO DE ACESSOS ÀS INFORMAÇÕES 5
8.2 PROTEÇÃO DO AMBIENTE DO GRUPO 5
8.2.1 Autenticação 5
8.2.2 Gestão de Incidentes de Segurança da Informação 6
8.2.3 Prevenção a Vazamento de Informações 6
8.2.4 Teste de Intrusão (Pentest) 6
8.2.5 Varredura de Vulnerabilidades 6
8.2.6 Controle Contra Software Malicioso 6
8.2.7 Criptografia 6
8.2.8 Rastreabilidade 6
8.2.9 Segmentação de Rede 6
8.2.10 Desenvolvimento Seguro 7
8.2.11 Cópias de Segurança (Backup) 7
8.3 CONTINUIDADE DOS NEGÓCIOS 7
8.4 SEGURANÇA CIBERNÉTICA EM FORNECEDORES 7
8.5 PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM 7
9. PRINCIPAIS RECOMENDAÇÕES DE SEGURANÇA AOS CLIENTES e USUÁRIOS 8
9.1 AUTENTICAÇÃO E SENHA 8
9.2 ANTIVÍRUS 8
9.3 ENGENHARIA SOCIAL 8
9.3.1 PHISHING, SMISHING e/ou VISHING 8
9.3.2 *SPAM* 8
9.3.3 FALSO CONTATO TELEFÔNICO 9
9.3.4 FALSA CENTRAL DE ATENDIMENTO 9
10. SAIBA MAIS 9

©2025 / 2026 Grupo XP Inc.

1. OBJETIVO

A Política de Segurança Cibernética ("Política") das empresas do Grupo. ("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

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).

©2025 / 2026 Grupo XP Inc.

Conglomerado Prudencial XP: a XP Investimentos CCTVM S.A., Banco XP S.A., XP DTVM Ltda. e demais empresas do Grupo., constituídas no Brasil e no Exterior, que se enquadram na definição que consta da Resolução n° 4.280/13, 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.

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 fornecer 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 de Segurança Cibernética 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 Terceiros e Parceiros de Negócio.

©2025 / 2026 Grupo XP Inc.

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. DESCRIÇÃO DAS REGRAS/PROCEDIMENTOS

6.1 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 reserva-se o direito de revogar essa autorização a qualquer momento.

Conceito:

©2025 / 2026 Grupo XP Inc.

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 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 e/ou colaboradores afastados ou desligados do Grupo., ou ainda que tenham mudado de função; e

©2025 / 2026 Grupo XP Inc.

- A revisão periódica das autorizações concedidas.

8.2.2 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. Adotamos procedimentos voltados para a prevenção, análise e tratativa dos incidentes.

O Grupo compartilhará os dados referentes aos 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.

8.2.3 Prevenção a Vazamento de Informações

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.

8.2.4 Teste de Intrusão (Pentest)

Testes de Intrusão (Pentests) interno e externo nas camadas de rede e aplicação devem ser realizados anualmente.

8.2.5 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.

8.2.6 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.

8.2.7 Criptografia

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

8.2.8 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, mas não se limitando, a criação, atualização ou remoção de objetos do sistema.

8.2.9 Segmentação de Rede

As redes devem ser segmentadas de forma lógica, de modo que apenas ambientes aprovados se comuniquem entre si, sendo que:

©2025 / 2026 Grupo XP Inc.

- 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.

8.2.10 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.

8.2.11 Cópias de Segurança (Backup)

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

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 e os testes previstos para os cenários de ataques cibernéticos.

8.4 SEGURANÇA CIBERNÉTICA EM FORNECEDORES

O Grupo possui um processo de gestão de fornecedores, parceiros e terceiros que disponibilizam serviços de tecnologia e/ou manuseiem dados sensíveis ou informações relevantes para as atividades operacionais do Grupo, os quais devem adotar procedimentos e controles rigorosos voltados à prevenção e ao tratamento de incidentes de segurança conforme regulamentações aplicáveis.

Esses procedimentos incluem a implementação de medidas proativas para identificar, mitigar e responder rapidamente a eventuais ameaças ou vulnerabilidades, garantindo a integridade, confidencialidade e disponibilidade das informações. Além disso, é obrigatório que tais empresas mantenham registros detalhados dos incidentes e realizem comunicação imediata ao Grupo, assegurando transparência e agilidade na resolução dos problemas, em conformidade com as normas internas e regulamentações aplicáveis.

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.

©2025 / 2026 Grupo XP Inc.

9. PRINCIPAIS RECOMENDAÇÕES DE SEGURANÇA AOS CLIENTES e USUÁRIOS

9.1 AUTENTICAÇÃO E SENHA

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

Recomendamos que:

- Mantenha a confidencialidade, memorize e não registre a senha em lugar algum. Ou seja, não contar a ninguém e não anotar em papel;
- Altere a senha sempre que existir qualquer suspeita do comprometimento dela;
- Elabore senhas de qualidade, de modo que sejam complexas e de difícil adivinhação;
- Impeça o uso do seu equipamento por outras pessoas, enquanto este estiver conectado/"logado" com a sua identificação;
- Bloqueie sempre o equipamento ao se ausentar.
- Sempre que possível, habilite um segundo fator de autenticação (Por exemplo: SMS, Token etc.).

9.2 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.

9.3 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, objetivando ludibriar, aplicar golpes ou obter informações sigilosas.

9.3.1 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;

9.3.2 *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

©2025 / 2026 Grupo XP Inc.

de segurança, sendo eles um dos principais responsáveis pela propagação de códigos maliciosos, venda ilegal de produtos e disseminação de golpes.

9.3.3 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.

9.3.4 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.

©2025 / 2026 Grupo XP Inc.