ITAÚ UNIBANCO HOLDING S.A.

CNPJ 60.872.504/0001-23 Companhia Aberta NIRE 35300010230

POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E CYBER SECURITY (GLOBAL)

OBJETIVO

Estabelecer os princípios, diretrizes e atribuições relacionadas à segurança da informação, protegendo as informações da instituição, dos clientes e do público em geral, observando as melhores práticas de mercado e regulamentações aplicáveis.

PÚBLICO-ALVO

Colaboradores do Itaú Unibanco *Holding* e suas empresas controladas no Brasil e no exterior e entidades mantidas ou geridas pelo Conglomerado Itaú Unibanco.

INTRODUÇÃO

A informação é um dos principais bens da instituição. Assim, o Itaú Unibanco *Holding* S.A define a estratégia de segurança da Informação e *Cyber Security* para proteger a integridade, disponibilidade e confidencialidade da informação.

Esta estratégia é baseada na detecção, prevenção, monitoramento e resposta à incidentes e fortalece a gestão do risco de segurança cibernética e a construção de um alicerce robusto para o futuro cada vez mais digital do Itaú Unibanco.

Para alcançarmos esse objetivo, utilizamos a estratégia de proteção de perímetro expandido. Esse conceito considera que a informação deve ser protegida independentemente de onde esteja, seja internamente, em uma coligada, em um serviço de cloud, em um prestador de serviço ou em uma unidade internacional, em todo o seu ciclo de vida, desde a coleta até o descarte.

PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

Nosso compromisso com o tratamento adequado das informações do Itaú Unibanco, clientes e público em geral está fundamentado nos seguintes princípios:

- **Confidencialidade**: garantir que o acesso à informação seja obtido somente por pessoas autorizadas;
- **Disponibilidade**: garantir que as pessoas autorizadas tenham acesso à informação sempre que necessário;
- **Integridade**: garantir a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

DIRETRIZES

Os documentos de segurança da informação (política, regras e procedimentos) devem estar disponíveis em local acessível aos colaboradores e protegidos contra alterações.

A Política Corporativa de Segurança da Informação e Cyber Security é revisada anualmente pelo Itaú Unibanco com aplicação no Brasil e no exterior.

A inclusão de diretrizes ou exceções por requisito regulatório e a publicação nas unidades do exterior, serão identificadas pelo responsável por segurança da informação da unidade, que deverá formalizar e submeter de forma prévia a proposta de diretrizes ou exceções para aprovação pela Diretoria de Segurança Corporativa.

A adesão à essa Política e eventuais desvios, no Brasil e nas unidades no exterior, são reportados periodicamente pela Diretoria de Segurança Corporativa aos Comitê Executivo, Comitê de Auditoria e demais comitês de risco.

A informação deve ser utilizada de forma transparente, para as finalidades informadas ao cliente e de acordo com a legislação vigente, conforme descrito em políticas internas.

As diretrizes e eventuais exceções são complementadas em procedimentos com regras específicas que devem ser observadas.

PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

Para assegurar que as informações tratadas estejam adequadamente protegidas, o Itaú Unibanco adota os seguintes processos:

a) Gestão de Ativos

Entende-se por ativo, tudo aquilo que a instituição considerar como relevante para o negócio, desde ativos tecnológicos (p.ex. *software* e *hardware*) como não tecnológicos (p.ex. pessoas, processos e dependências físicas) desde que estejam relacionados à proteção da informação.

Os ativos, de acordo com sua criticidade, devem ser identificados, inventariados, mantidos atualizados, possuírem um proprietário, descartados de forma segura e serem protegidos contra acessos indevidos. A proteção pode ser, física (p.ex. salas com acesso controlado) e lógica (p.ex. configurações de blindagem ou *hardening*, *patch management*, autenticação e autorização).

Os ativos do Itaú Unibanco, dos clientes e do público em geral devem ser tratados de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, promovendo o uso adequado e prevenindo exposição indevida das informações.

b) Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade, conforme descrito em documento internos.

Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações. De acordo com a classificação da confidencialidade devem ser estabelecidas as proteções necessárias durante todo o seu ciclo de vida.

O ciclo de vida da informação compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

c) Gestão de Acessos

As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos corporativos do Itaú Unibanco.

Os acessos devem ser rastreáveis, a fim de permitir a identificação individual do colaborador ou prestador de serviço que tenha acessado ou alterado as informações, permitindo sua responsabilização.

A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários devem ter acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades e devidamente autorizados.

A segregação de funções deve permear todos os processos críticos, evitando que um único responsável possa executar e controlar o processo durante todo seu ciclo de vida.

A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

A senha é uma informação confidencial, pessoal e intransferível, deve ser utilizada como assinatura eletrônica, sendo proibido seu compartilhamento.

d) Gestão de Riscos

Os riscos devem ser identificados por meio de um processo estabelecido para análise de ameaças, vulnerabilidades, probabilidades e impactos sobre os ativos do Itaú Unibanco, para que sejam recomendadas as proteções adequadas. As recomendações são discutidas nos fóruns apropriados.

Produtos, processos e tecnologias devem ter a adequada gestão dos riscos de Segurança da Informação, para redução dos riscos à níveis aceitáveis, independentemente de estarem dentro da infraestrutura do Itaú Unibanco *Holding*, parceiros ou prestadores de serviços.

As tecnologias em uso pela instituição devem estar em versões suportadas pelos seus fabricantes e devidamente atualizadas. Eventuais exceções devem ser aprovadas na alçada competente ou possuir controles compensatórios.

e) Gestão de Riscos em Prestadores de Serviços e Parceiros

Os prestadores de serviços e parceiros contratados pelo banco devem ser classificados considerando alguns critérios, conforme em documento internos.

Dependendo da classificação, o prestador de serviço ou parceiro passará por avaliação de risco, que pode incluir a validação *in loco* dos controles de SI, avaliação remota das evidências ou outras avaliações, além do acompanhamento de eventuais correções e melhorias implementadas pelos prestadores de serviços e parceiros.

Os prestadores de serviços e parceiros devem informar os incidentes relevantes (conforme definido no item 6.f deste documento), relacionados às informações do Itaú Unibanco armazenadas ou processadas por eles em cumprimento às determinações legais e regulamentares.

As diretrizes para contratação de serviços relevantes conforme definições regulamentares, estão descritas em documento internos.

f) Tratamento de Incidentes de Segurança da Informação e *Cyber Security*

A área de Cyber Security monitora a segurança do ambiente tecnológico do Itaú Unibanco no Brasil, analisando os eventos e alertas para identificar possíveis incidentes.

Os incidentes que são identificados pelos alertas são classificados com relação ao impacto, de acordo com os critérios adotados pelo Itaú Unibanco. Para o seu grau de relevância serão considerados aspectos como impacto ao sistema financeiro e comprometimento de dados de clientes e do público em geral, conforme descrito no Plano de Tratamento de Incidentes de Segurança Da Informação e Cyber Security (Brasil). Incidentes classificados como relevantes devem ser comunicados ao Regulador, ao titular do dado, e ao Comitê de Auditoria (CAUD), quando envolverem dados pessoais que possam acarretar risco ou causar dano relevante aos titulares e havendo o envolvimento de colaboradores internos, os casos serão reportados para atuação conjunta com a Inspetoria.

Todos os incidentes passam por um processo de tratamento e comunicação, onde são registradas todas as informações pertinentes aos incidentes como causa, impacto, classificação, etc.

Informações sobre incidentes que possam impactar outras instituições financeiras no Brasil, devem ser compartilhadas com as demais instituições, visando colaborar com a mitigação do risco conforme determinações legais e regulamentares.

No exterior, a gestão de incidentes de segurança da informação e cibernéticos é realizada por cada Unidade Internacional que deve reportá-los tempestivamente à Diretoria de Segurança Corporativa no Brasil.

A área de Riscos elaborará Relatório Anual contendo os incidentes relevantes ocorridos no período, ações realizadas de prevenção e resposta aos incidentes e resultados dos testes de continuidade. Este relatório deverá ser apresentado ao Comitê de Risco, ao Comitê de Auditoria e ao Conselho de Administração, conforme determinações legais e regulamentares.

Visando aprimorar a capacidade de resposta a incidentes, o Itaú Unibanco realiza testes de continuidade de negócios simulando cenários de incidentes críticos de Cyber Security, que podem comprometer a disponibilidade e/ou a confidencialidade das informações.

Todo colaborador deve ser proativo e diligente na identificação, comunicação para a área de Segurança da Informação e na mitigação dos riscos relacionados à segurança da informação.

g) Conscientização em Segurança da Informação e *Cyber Security*

O Itaú Unibanco promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização e capacitação para fortalecer a cultura de Segurança da Informação, fazendo parte do Programa de Integridade e Ética, conforme descrito em documento interno.

Periodicamente, são disponibilizadas campanhas de conscientização ou treinamentos que podem ser presenciais ou on-line, relacionados a confidencialidade, integridade e disponibilidade da informação. Estas campanhas são veiculadas através de e-mails, portal corporativo, e-learning, elemídias ou redes sociais aos colaboradores e clientes.

h) Governança com as Áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com os princípios e diretrizes de segurança da informação.

i) Segurança Física do Ambiente

O processo de Segurança Física estabelece controles relacionados à concessão de acesso físico aos ambientes, de acordo com a criticidade das informações tratadas nestes ambientes, conforme descrito em documento internos.

j) Segurança no Desenvolvimento de Sistemas de Aplicação

O processo de desenvolvimento de sistemas deve garantir a aderência aos documentos internos para as Unidades Internacionais e boas práticas de segurança da instituição.

Os ambientes produtivos devem ser segregados dos demais ambientes e com acesso somente via aplicação por usuários previamente autorizados ou por ferramentas homologadas.

k) Configuração Segura

O processo de configuração segura deve garantir a aderência a documentos internos de Configuração Segura – Hardening definida pela área de Arquitetura de Segurança da Informação, estabelecendo uma configuração segura dos sistemas adquiridos pela instituição de acordo com as boas práticas de Segurança.

l) Gravação de *Logs*

É obrigatória a gravação de *logs* ou trilhas de auditoria do ambiente computacional, para todas as plataformas, de forma a permitir identificar: quem fez o acesso, quando o acesso foi feito, o que foi acessado e como foi acessado.

Essas informações devem ser protegidas contra modificações e acessos não autorizados.

m) Programa de *Cyber Security*

O Programa de *Cyber Security* do Itaú-Unibanco é norteado pelos seguintes princípios:

- Regulamentações vigentes;
- Melhores práticas;
- Cenários mundiais;
- Análises de risco da própria instituição.

Conforme sua criticidade, as ações do programa dividem-se em:

- **Críticas:** Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;
- **Sustentação:** Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da instituição e permitindo que ações de longo prazo/estruturantes possam ser realizadas;
- **Estruturantes:** Iniciativas de médio/longo prazo que tratam a causa raiz dos riscos e que preparam o banco para o futuro.

n) Proteção de perímetro

Para proteção da infraestrutura do Itaú Unibanco contra um ataque externo, utilizamos, no mínimo, ferramentas e controles contra: ataques de DDoS, *Spam*, *Phishing*, APT/*Malware*, invasão de dispositivos de rede e servidores, ataques a aplicação e *scan* externos, além de testes de penetração.

Para mitigação do risco de vazamento de informações utilizamos ferramentas preventivas instaladas em dispositivos móveis, estações de trabalho, no serviço de correio eletrônico, no serviço de navegação WEB, no serviço de impressão, além do uso de criptografia para dados em repouso e em transporte.

Visando elevar a proteção, não é permitida a conexão física ou lógica à rede corporativa da instituição, por equipamentos particulares não gerenciados ou não homologados.

o) Governança com as Unidades Internacionais

As unidades internacionais devem possuir um responsável por segurança da informação, independente das áreas de negócio e tecnologia, que se reporta matricialmente à Diretoria de Segurança Corporativa.

Propriedade Intelectual

A propriedade intelectual é a proteção que recai sobre bens imateriais, tais como: marcas, sinais distintivos, *slogans* publicitários, nomes de domínio, nomes empresariais, indicações geográficas, desenhos industriais, patentes de invenção e de modelo de utilidade, obras intelectuais (tais como obras literárias, artísticas e científicas, base de dados, fotografias, desenhos, ilustrações, projetos de arquitetura, obras musicais, obras audiovisuais, textos e etc.), programas de computador e segredos empresariais (inclusive segredos de indústria e comércio).

Pertencem exclusivamente ao Itaú Unibanco todas e quaisquer invenções, criações, obras e aperfeiçoamentos que tenham sido ou venham a ser criados ou realizados pelo colaborador ao Itaú Unibanco, na qualidade de administrador, empregado e/ou estagiário, durante todo o prazo de vigência do mandato, contrato de trabalho ou contrato de estágio do colaborador. Quaisquer informações e conteúdos cuja propriedade intelectual pertença ao Itaú Unibanco, ou tenham sido por ele disponibilizado, inclusive informações e conteúdos que tenham sido obtidos, inferidos ou desenvolvidos pelo próprio colaborador em seu ambiente de trabalho ou utilizando recursos da instituição não devem ser utilizados para fins particulares, nem repassados a terceiros, sem autorização prévia e expressa do Itaú Unibanco

É dever de todos os colaboradores zelar pela proteção da propriedade intelectual do Itaú Unibanco.

Declaração de Responsabilidade

Periodicamente os colaboradores do Itaú Unibanco devem aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de Segurança da Informação.

Os contratos firmados com o Itaú Unibanco devem possuir cláusula que assegure a confidencialidade das informações e a obrigatoriedade de seguir as regulamentações vigentes, referentes ao tema de segurança da informação.

PAPÉIS E RESPONSABILIDADES
As políticas, estratégias e processos corporativos de Segurança da Informação são supervisionadas no Brasil e no exterior pela Diretoria de Segurança Corporativa e discutidos nos fóruns específicos de riscos das áreas e nas Comissões Executivas que tratam Risco Operacional ou Tecnologia.

Auditoria Interna
Os papéis e responsabilidades da Auditoria Interna estão descritos na Política de Auditoria Interna (Global).

Risco Operacional
Os papéis e responsabilidades de Risco Operacional estão descritos na Política de Gerenciamento Integrado de Risco Operacional e Controles Internos (Global).

Segurança Corporativa

- Aprimorar a qualidade e efetividade de seus processos, buscando a integridade, disponibilidade e confidencialidade das informações;
- Proteger a informação de ameaças buscando garantir a continuidade do negócio e minimizar os riscos ao negócio;
- Estabelecer, implementar, operar, monitorar e garantir a melhoria contínua do sistema de gestão de segurança da informação (SGSI).
- Definir e formalizar os objetivos, controles e a estratégia de governança de segurança da informação, em conjunto com o Comitê Executivo de Segurança da Informação.
- Coordenar as ações para atingimento dos objetivos e da estratégia de governança de segurança da informação aprovados pelos comitês, envolvendo as áreas responsáveis.
- Estabelecer e disseminar uma cultura de segurança da informação.
- Propor o investimento para a segurança da informação para atender aos objetivos desta política.
- Definir as políticas e padrões de segurança da informação a serem aplicados nos processos, produtos e tecnologias.
- Definir padrões mínimos de segurança para as Unidades Internacionais e Empresas controladas no Brasil e no exterior e Entidades mantidas ou geridas pelo Conglomerado Itaú Unibanco, garantindo alinhamento com os objetivos de segurança da informação definidos pela Holding.

Unidades Internacionais
Atuar proativamente na identificação, prevenção e correção dos riscos e reportar periodicamente à Diretoria de Segurança Corporativa.

Empresas e Entidades do Conglomerado
Empresas do conglomerado controladas no Brasil e no exterior e entidades mantidas ou geridas pelo Conglomerado Itaú Unibanco devem avaliar as diretrizes e requisitos estabelecidos nesta política e em seus anexos, reportando periodicamente à Diretoria de Segurança Corporativa os riscos identificados, adequando seus procedimentos de segurança internos conforme seu segmento de negócio e apetite de riscos. Estas empresas devem ser classificadas e ter modelo de governança baseado na avaliação de riscos, que considera os seguintes aspectos: Impacto na imagem da Holding, Modelo de Arquitetura e Conectividade com a Holding, e Volume de dados sensíveis armazenados. Este modelo de governança pode variar entre avaliação e acompanhamento direto de aderência aos controles definidos ou seguindo declaração de aderência a ser realizado pela própria empresa.

Comitê Executivo de Segurança da Informação
Aprovar a estratégia, objetivos, orçamento e ações necessárias para a mitigação dos riscos dos processos de segurança da informação.

Comitê de Auditoria – CAUD
Supervisionar a estratégia de gestão dos riscos, seus respectivos processos e controles internos, bem como acompanhar os projetos de segurança da informação do Conglomerado Itaú Unibanco.

Área de Tecnologia
Manter o parque tecnológico disponível e atualizado com os padrões de segurança implementados, dentro dos prazos compatíveis com os níveis de riscos.

Área de Negócio
Proteger as informações do Itaú Unibanco sob sua responsabilidade.

SANÇÕES DISCIPLINARES
As violações a esta política estão sujeitas às sanções disciplinares previstas em documento internos, bem como nas normas internas das empresas do Itaú Unibanco e na legislação vigente onde as empresas estiverem localizadas.

DOCUMENTOS RELACIONADOS
Esta Política Corporativa de Segurança da Informação é complementada por procedimentos específicos de Segurança da Informação em conformidade com os aspectos legais e regulamentares e aprovadas pelas Superintendência de Governança e Projetos de Cyber Security e Superintendência Operacional de Cyber Security, subordinadas à Diretoria de Segurança Corporativa, na estrutura da Área de Riscos e Finanças do Itaú Unibanco.

Frameworks e Regulamentações
- Resolução 4.893 do Banco Central;

- Resolução nº 85 do Banco Central;

- Resolução 4.752 do Banco Central;

- Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018;

- Resolução nº 35 da CVM;

- Resolução Conjunta Nº 1, de 4 de maio de 2020 (Open Finance);

- Circular 638 da SUSEP;

- Resolução CNSP n° 415 da SUSEP, de 30 de Julho de 2021 (Open Insurance);

- E demais regulamentações e leis relacionadas ao tema.

- ABNT NBR ISO/IEC 27001:2013 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão da segurança da informação – Requisitos;

- ABNT NBR ISO/IEC 27701:2019 – Técnicas de segurança – Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e diretrizes;

GLOSSÁRIO
APT (*Advanced Persintent Threat*): ataques avançados persistentes.

***Cyber Security*:** é o termo que designa o conjunto de meios e tecnologias empregadas na defesa dos sistemas de informação, infraestrutura, redes de computadores e/ou dispositivos pessoais, com o objetivo de prevenir danos, roubo, intrusão, alterações ou destruição de informações.

Dano Relevante: Ação que possa causar impacto à privacidade do indivíduo, podendo ocasionar risco elevado à sua integridade física ou moral.

Parque tecnológico: conjunto de ativos de infraestrutura e sistemas de tecnologia.

Segregação de funções: consiste na separação das atividades entre áreas e pessoas potencialmente conflitantes ou que possuem informações privilegiadas, na qual, o colaborador não pode exercer mais que uma função nos processos de autorização, aprovação, execução, controle e contabilização.

Aprovado pelo Conselho de Administração de 26.01.2023.