ITAÚ UNIBANCO HOLDING S.A.

CNPJ 60.872.504/0001-23 Companhia Aberta NIRE 35300010230

POLÍTICA CORPORATIVA DE SEGURANÇA DA INFORMAÇÃO E CYBER SECURITY

OBJETIVO

Garantir a aplicação dos princípios e diretrizes de proteção da propriedade intelectual e das informações da organização, dos clientes e do público em geral, observando as regulamentações aplicáveis e melhores práticas de mercado.

INTRODUÇÃO

A informação é um dos principais bens de qualquer organização. Para a devida proteção desse bem, o Itaú Unibanco Holding S.A. estabelece a presente política de Segurança da Informação e Cyber Security, a fim de garantir a aplicação dos princípios e diretrizes de proteção da propriedade intelectual e das informações da organização, dos clientes e do público em geral.

Nossa estratégia de Segurança da Informação e Cyber Security foi desenvolvida para evitar violações da segurança dos dados, minimizar os riscos de indisponibilidade dos nossos serviços, proteger a integridade e evitar qualquer vazamento de informação. Para alcançarmos esse objetivo nossa estratégia está baseada na proteção de perímetro expandido, apoiado em processos de controle para detecção, prevenção, monitoramento e resposta a incidentes garantindo a gestão do risco de segurança cibernética e a construção de um alicerce robusto para o futuro cada vez mais digital do Itaú Unibanco. O conceito de perímetro expandido considera que a informação deve ser protegida independentemente de onde ela esteja, seja em um prestador de serviço ou em uma unidade internacional, em todo o seu ciclo de vida, desde o momento que ela é coletada, passando pelo processamento, transmissão, armazenamento, analise e seu descarte.

PÚBLICO-ALVO

Colaboradores do Itaú Unibanco Holding S.A. e suas empresas controladas no Brasil e no exterior (Conglomerado).

Para os fins do disposto nesta política o termo "Colaboradores" abrange todos os empregados, menores aprendizes, estagiários e administradores do Itaú Unibanco.

REGRAS

Regra Geral

Todas as políticas de segurança da informação precisam estar disponíveis em local acessível aos colaboradores e devem ser protegidas contra alterações.

As políticas de segurança da informação são revisadas anualmente pelo Itaú Unibanco com aplicação no Brasil e no exterior.

A revisão e publicação nas unidades do exterior, são de responsabilidade da própria unidade, sendo necessária a aprovação pelo Brasil.

A adesão a 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 de demais comitês de risco.

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: garantimos que o acesso à informação seja obtido somente por pessoas autorizadas e quando ele for de fato necessário;

- Disponibilidade: garantimos que as pessoas autorizadas tenham acesso à informação sempre que necessário;

- Integridade: garantimos a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

Diretrizes de Segurança da Informação

A Segurança da Informação no Itaú Unibanco estabelece as seguintes diretrizes:

a) As informações do Itaú Unibanco, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.

b) A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.

c) Todo processo, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de um colaborador ou equipe de colaboradores, para que a atividade não seja executada e controlada pelo mesmo colaborador ou equipe.

d) O acesso às informações e recursos só deve ser feito se devidamente autorizado.

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

f) A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.

g) A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

h) Todo colaborador deve reportar os riscos às informações à área de Segurança da Informação.

i) A área de Segurança de Informação deve divulgar amplamente as responsabilidades sobre Segurança da Informação aos Colaboradores, que devem entender e assegurar estas diretrizes.

Processo de Segurança da Informação

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

a) Gestão de Ativos da Informação

Entende-se por Ativos da Informação tudo o que pode criar, processar, armazenar, transmitir e até excluir a informação. Podem ser tecnológicos ("software" e "hardware") e não tecnológicos (pessoas, processos e dependências físicas).

Os ativos da informação, de acordo com sua criticidade, devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, fisicamente (salas com acesso controlado) e logicamente (configurações de blindagem ou "hardening", patch management, autenticação e autorização) e ter documentação e planos de manutenção atualizados anualmente.

b) Classificação da Informação

As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Restrita, Confidencial, Interna e Pública. 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.

c) Gestão de Acessos

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

Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o Colaborador, prestador de serviço, para que seja responsabilizado por suas ações.

d) Gestão de Riscos

Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação do Itaú Unibanco, para que sejam recomendadas as proteções adequadas.

Os cenários de riscos de segurança da informação são escalonados nos fóruns apropriados, para decisão.

e) Gestão de Riscos em Prestadores de Serviços

Os prestadores de serviços contratados pelo banco são classificados considerando alguns critérios, tais como: Criticidade do segmento; Auditoria remota; Informações mais críticas manipuladas pelo fornecedor; Forma de acesso às informações; Frequência de acesso às informações; Histórico de fraude e/ou de vazamento de informação; Certificações; Data da última avaliação; Top fornecedor do segmento; classificação do risco identificado na última avaliação.

Dependendo da classificação do prestador de serviço referente aos critérios acima, deverá passar por avaliação de risco, que vai desde a validação in loco dos controles de segurança da informação, avaliação remota das evidências ou outros processos de avaliação, além do acompanhamento de eventuais correções e melhorias implementadas pelos prestadores de serviços.

Para avaliação de risco, é utilizado um Baseline de Fornecedores, que consiste em um documento com diversos controles de segurança baseado em padrões internacionais e melhores práticas do segmento.

Existe um canal de comunicação para que os prestadores de serviços, que prestam serviços ao Itaú Unibanco no Brasil, informem as ocorrências de incidentes relevantes relacionados as informações do Itaú Unibanco armazenadas ou processadas na empresa contratada, em cumprimento às determinações legais e regulamentares.

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

A área de Cyber Security realiza a monitoração de segurança do ambiente tecnológico do Itaú Unibanco no Brasil, analisando os eventos e alertas com o objetivo de 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 comprometimento de dados de clientes e impacto ao sistema financeiro.

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, de acordo com o procedimento operacional.

Visando aprimorar a capacidade do Itaú Unibanco na resposta a incidentes cibernéticos, alguns cenários que possam afetar a continuidade de negócios são considerados nos testes.

Para os incidentes que possam impactar outras instituições financeiras no Brasil, há um processo de troca de informações entre as instituições, visando a colaboração na mitigação do risco do incidente em cumprimento às determinações legais e regulamentares.

No exterior a gestão de incidentes de segurança da informação e cibernéticos é realizada por cada Unidade Internacional.

Os incidentes de Segurança da Informação e cibernéticos do Itaú Unibanco no Brasil e no exterior devem ser reportados à Diretoria de Segurança Corporativa no Brasil.

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

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, com o objetivo de fortalecer a cultura de Segurança da Informação.

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, mídia indoor, 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 as diretrizes e arquiteturas de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade das informações.

i) Segurança Física do Ambiente

O processo de Segurança Física visa estabelecer controles relacionados à concessão de acesso físico ao ambiente somente a pessoas autorizadas, de acordo com a criticidade das informações previamente mapeadas e declaradas à Administração Predial.

j) Segurança no Desenvolvimento de Sistemas de Aplicação

O processo de desenvolvimento de sistemas de aplicação deve garantir a aderência às políticas de segurança do Itaú Unibanco e às boas práticas de segurança.

k) Gravação de LOGs

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

As informações dos registros (logs) ou trilhas de auditoria devem ser protegidas contra modificações e acessos não autorizados.

l) Programa de Cyber Security

O Programa de Cyber Security do Itaú Unibanco é norteado pelos seguintes fatores:

- Regulamentações vigentes;

- Melhores práticas;

- Cenário mundiais.

Conforme sua criticidade, o programa divide-se em:

- Ações críticas - Consiste de correções emergenciais e imediatas para mitigar riscos iminentes;

- Ações de Sustentação - Iniciativas de curto / médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da Organização e permitindo que ações de longo prazo/estruturantes possam ser realizadas;

- Ações Estruturantes - Iniciativas de médio / longo prazo que tratam a causa raiz dos riscos e que preparam o Banco para o futuro.

m) Proteção de perímetro

Para proteção da infraestrutura do Itaú Unibanco contra um ataque externo, utilizamos ferramentas e controles contra: ataques que afetem a disponibilidade (DDoS), Spam, Phishing, ataques avançados persistentes (APT), Malware, invasão de dispositivos de rede e servidores, ataques de aplicação e scan externos.

No sentido de nos protegermos contra vazamento de informações, utilizamos diversas ferramentas preventivas contra vazamento de informação, instaladas em estações de trabalho, no serviço de correio eletrônico, no serviço de navegação WEB, no serviço de impressão, além de criptografia de disco em notebooks e solução de proteção de dispositivos móveis.

n) Governança com as Unidades Internacionais

Toda Unidade do Itaú Unibanco deve possuir um responsável por segurança da informação, que deve possuir independência das áreas de negócio e tecnologia, bem como reportar-se matricialmente à Diretoria de Segurança Corporativa.

Avaliação Independente da Auditoria

A efetividade das políticas de Segurança da Informação é verificada por meio de avaliações periódicas de Auditoria Interna.

Propriedade Intelectual

A propriedade intelectual é composta por 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).

Quaisquer informações e propriedade intelectual que pertençam ao Itaú Unibanco, ou por ele disponibilizadas, não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas, inferidas ou desenvolvidas pelo próprio colaborador em seu ambiente de trabalho

Declaração de Responsabilidade

Periodicamente os Colaboradores e Prestadores de Serviços diretamente contratados pelo 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.

Medidas Disciplinares

As violações a esta política estão sujeitas às sanções disciplinares previstas nas normas internas das empresas do Itaú Unibanco, e na legislação vigente no Brasil e nos países onde as empresas estiverem localizadas.

GLOSSÁRIO

Matriz: Itaú Unibanco no Brasil.

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.

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.

APT: Adbvanced Persintent Threat, ou ataques avançados persistentes

Aprovado pelo Conselho de Administração de 28.03.2019.