Política Corporativa de Segurança da Informação

1. OBJETIVO

A informação é um dos principais bens de qualquer organização. Assim, a Instituição estabelece a presente Política Corporativa de Segurança da Informação, a fim de garantir a aplicação dos princípios e diretrizes de proteção das informações da organização, dos clientes e do público em geral.

2. PÚBLICO-ALVO

Esta política destina-se a todos os colaboradores e órgãos usuários de informações do Itaú Unibanco Holding S.A., suas empresas controladas no Brasil e exterior.

Para os fins do disposto nesta política “Itaú Unibanco Holding S.A." passa a ser substituído pelo termo “Instituição” no restante do texto, “Itaú Unibanco Brasil” passa a ser substituído por “Matriz” e o termo “Colaboradores” abrange todos os empregados, menores aprendizes, estagiários e administradores da Instituição.

3. RESPONSABILIDADES

As políticas, estratégias e processos corporativos de Segurança da Informação são supervisionados pelo Comitê Corporativo de Segurança da Informação, coordenado pela Diretoria de Segurança Corporativa e composto por representantes das áreas de Riscos e Controles Internos, Auditoria, Tecnologia e Negócios da Instituição.

4. REGRAS

4.1 Regra Geral

As políticas de segurança da informação precisam estar disponíveis em local de acesso dos Colaboradores e protegida contra alterações.

A nomenclatura e o código das políticas de segurança da informação precisam ser mantidos com a mesma identificação da Matriz.

As políticas de segurança da informação são revisadas anualmente pela Matriz, encaminhadas para as unidades onde forem aplicáveis e sua revisão e publicação é de responsabilidade da unidade local após aprovação da Matriz.

4.2 Princípios de Segurança da Informação

Nosso compromisso com o tratamento adequado das informações da Instituição, 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.

4.3 Diretrizes de Segurança da Informação

A Segurança da Informação na Instituição estabelece os principais controles, denominados diretrizes:

a) As informações da Instituição, 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.

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) Os riscos às informações da Instituição devem ser reportados à área de Segurança da Informação.

i) As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos Colaboradores, que devem entender e assegurar estas diretrizes.

4.4 Tratamento da Informação

A informação deve receber proteção adequada em observância aos princípios e diretrizes de Segurança da Informação da Instituição em todo o seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

4.5 Gestão da Segurança da Informação

Para assegurar que as informações tratadas estejam adequadamente protegidas, a Instituição adota os seguintes processos:

a) Gestão de Ativos da Informação

Os ativos da informação devem ser identificados de forma individual, inventariados e protegidos de acessos indevidos, e ter documentação e planos de manutenção atualizados.

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 da Instituição.

Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o Colaborador, 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 da Instituição, para que sejam recomendadas as proteções adequadas.

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

e) Tratamento de Incidentes de Segurança da Informação

Os incidentes de Segurança da Informação da Instituição devem ser reportados à Diretoria de Segurança Corporativa.

f) Conscientização em Segurança da Informação

A Instituição 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.

g) Avaliação Independente da Auditoria

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

4.6 Propriedade Intelectual

Tecnologias, marcas, metodologias e quaisquer informações que pertençam à Instituição não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho.

4.7 Declaração de Responsabilidade

Os Colaboradores e Prestadores de Serviços diretamente contratados pela Instituição devem aderir formalmente a um termo, comprometendo-se a agir de acordo com as políticas de Segurança da Informação.

Os contratos da Instituição devem possuir cláusula que assegure a confidencialidade das informações.

4.8 Medidas Disciplinares

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

5. DOCUMENTOS RELACIONADOS

Esta Política Corporativa de Segurança da Informação é complementada por normas específicas de Segurança da Informação (circulares SI, integrantes do conjunto de normativos do Itaú Unibanco) em conformidade com os aspectos legais e regulamentares e aprovadas pela Superintendência de Continuidade de Negócios e Gestão de Crises e pela Superintendência de Segurança da Informação, subordinadas à Diretoria de Segurança Corporativa, na estrutura da Área Seguros, Controles e Apoio Operacional da Instituição. Devem ser observadas, também, as regras estabelecidas na política sobre Gerenciamento de Risco Operacional em Serviços Terceirizados.

6. GLOSSÁRIO

Instituição: Itaú Unibanco Holding S.A., suas empresas controladas no Brasil e exterior.

Matriz: Itaú Unibanco Brasil.

Segregação de funções: o ato pelo qual o Colaborador não pode exercer mais que uma função no processo de aprovação.

7. ÓRGÃO RESPONSÁVEL

A Diretoria de Segurança Corporativa é responsável por manter e atualizar esta política.