POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

La información es uno de los principales bienes de cualquier organización. Por eso mismo, la Institución establece la presente política de Seguridad de la Información con el fin de garantizar la aplicación de los principios y directrices de protección de las informaciones de la organización, y de la propiedad intelectual de la organización, de los clientes y del público en general.

2. ALCANCE

Esta política está dirigida a todos los empleados y usuarios de los órganos de información de Itaú Unibanco Holding S.A., sus filiales en Brasil y en el extranjero.

A los efectos de esta política, "Itaú Unibanco Holding S.A." se sustituye por el término "Institución" en el resto del texto “Itaú Unibanco Brasil” se sustituye por “Casa Matriz” y el término "empleados" incluye a todos los empleados, aprendices y directivos de la institución.

3. RESPONSABILIDADES

Las políticas, estrategias y procesos corporativos de Seguridad de la Información son supervisados por Diretoria de Segurança Corporativa y discutidos en los foros específicos de riesgos de las áreas y en las Comisiones Ejecutivas que tratan de Riesgo Operativo o Tecnología.

4. REGLAS

4.1 Regla General

Todas las políticas de seguridad de la información necesitan estar disponibles para que los empleados puedan consultarlas y protegidas frente a cambios.

La nomenclatura y el código de las políticas de seguridad de la información necesitan mantenerse con la misma identificación de la Matriz.

Las políticas de seguridad de la información son revisadas anualmente por la Casa Matriz, encaminadas a las unidades cuando sea aplicable y su revisión y publicación es responsabilidad de la unidad local después de la aprobación de Casa Matriz.

4.2 Principios de Seguridad de la Información

Nuestro compromiso con el tratamiento adecuado de las informaciones de la Institución, clientes y público en general se fundamenta en los siguientes principios:

- Confidencialidad – Garantizamos que el acceso a la información lo obtengan solamente personas autorizadas y cuando realmente sea necesario;
- Disponibilidad – Garantizamos que las personas autorizadas tengan acceso a la información siempre que sea necesario;
- Integridad – Garantizamos la exactitud y la completitud de la información y de los métodos de su procesamiento, así como de la transparencia en el trato con los públicos involucrados.

4.3 Directrices de Seguridad de la Información

La Seguridad de la Información en la Institución establece los principales controles, denominados directrices:

a) Las informaciones de la institución, de los clientes y del público en general se deben tratar de forma ética y sigilosa y de acuerdo con las leyes vigentes y normas internas, evitándose el mal uso y la exposición indebida;

b) La información debe utilizarse de forma transparente y solamente para la finalidad para la que se recopiló;

c) Todo el proceso, durante su ciclo de vida, debe garantizar la segregación de funciones por medio de la participación de más de un colaborador o equipo de colaboradores, de modo que la actividad no es ejecutado y controlado por el mismo desarrollador o equipo.

d) El acceso a las informaciones y recursos solo se debe hacer si se está debidamente autorizado;

e) La identificación de cualquier colaborador debe ser única, personal e intransferible, cualificándolo como responsable de las acciones realizadas;

f) La concesión de accesos debe obedecer el criterio de menor privilegio, según el cual los usuarios tienen acceso solamente a los recursos de información imprescindibles para el pleno desempeño de sus actividades;

g) La clave utilizada como firma electrónica debe mantenerse en secreto, estando prohibido compartirla;

h) Los riesgos que corran las informaciones de la Institución deben informarse al área de Segurança da Informação;

i) Las responsabilidades en lo que se refiere a la Seguridad de la Información deben divulgarse ampliamente entre los colaboradores, que deben entender y asegurar estas directrices.

4.4 Tratamiento de la Información

La información debe recibir una protección adecuada en observancia a los principios y directrices de Seguridad de la Información de Itaú Unibanco en todo su ciclo de vida, que abarca: Generación, Manejo, Almacenamiento, Transporte y Desecho.

4.5 Proceso de Seguridad de la Información

Para asegurar que las Informaciones tratadas estén adecuadamente protegidas, Itaú Unibanco adopta los siguientes procesos:

a) Gestión de Activos de la Información

Los activos de la información se deben identificar de forma individual, inventariar y proteger de accesos indebidos, y tener documentación y planes de manejo actualizados.

b) Clasificación de la Información

Las informaciones deben clasificarse de acuerdo con la confidencialidad y las protecciones necesarias en los siguientes niveles: Restricta, Confidencial, Interna y Pública. Para ello, hay que considerar las necesidades relacionadas al negocio, el compartimiento o restricción de acceso y los impactos en el caso de utilización indebida de las Informaciones.

c) Gestión de Accesos

Las concesiones, revisiones y exclusiones de acceso deben utilizar las herramientas y los procesos de Itaú Unibanco.

Los accesos deben ser rastreables, a fin de garantizar que todas las acciones pasibles de auditoría puedan identificar individualmente al colaborador para que se responsabilice de sus acciones.

d) Gestión de Riesgos

Los riesgos deben identificarse por medio de un proceso establecido para analizar vulnerabilidades, amenazas e impactos sobre los activos de información de Itaú Unibanco, a efectos de recomendar las protecciones adecuadas.

Los escenarios de riesgos de seguridad de la información se presentan en los foros adecuados para la toma de decisiones.

e) Tratamiento de Incidentes de Seguridad de la Información

Los incidentes de Seguridad de la Información de la Institución deben informarse a Diretoria de Segurança Corporativa.

f) Concienciación en Seguridad de la Información

Itaú Unibanco promueve la diseminación de los principios y directrices de Seguridad de la Información por medio de programas de concienciación y capacitación, con el objetivo de fortalecer la cultura de Seguridad de la Información.

g) Gobierno con las Áreas de Negocio y Tecnología

Las iniciativas y proyectos de las áreas de negocio y tecnología deben estar alineados con las directrices y arquitecturas de seguridad de la información a efectos de garantizar la confidencialidad, integridad y disponibilidad de las informaciones.

h) Gobierno con las Unidades Internacionales

Toda y cualquier unidad de Itaú Unibanco debe contar con un responsable de la Seguridad de la Información, independiente de las áreas de negocio y tecnología, que se reportará matricialmente a Diretoria de Segurança Corporativa de la Casa Matriz.

i) Seguridad Física del Ambiente

El proceso de Seguridad Física pretende establecer controles que solamente permitan el acceso de personas autorizadas, de acuerdo con la criticidad de las informaciones previamente mapeadas.

j) Sistemas de desarrollo de aplicaciones de seguridad

El proceso de desarrollo de sistemas de aplicación para garantizar la adhesión a las políticas de seguridad Itaú Unibanco y las mejores prácticas de seguridad.

4.6 Evaluación Independiente de la Auditoría

La efectividad de las políticas de Seguridad de la Información se verifica por medio de evaluaciones periódicas de auditoría.

4.7 Propiedad Intelectual

La propiedad intelectual se compone de bienes inmateriales, tales como: marcas, señales distintivos, eslóganes publicitarios, nombres de dominio, nombres empresariales, indicaciones geográficas, diseños industriales, patentes de invención y de modelo de utilidad, obras intelectuales (tales como obras literarias, artísticas y científicas, bases de datos, fotografías, dibujos, ilustraciones, proyectos de arquitectura, obras musicales, obras audiovisuales, textos, etc.), programas de informática y secretos empresariales (incluidos secretos de industria y comercio).

Toda y cualquier información y propiedad intelectual que pertenezca a Itaú Unibanco, o que él ofrezca, no debe utilizarse para fines particulares, ni trasladarse a otro, aunque haya sido obtenida, inferida o desarrollada por el propio colaborador en su ambiente de trabajo.

4.8 Declaración de Responsabilidad

Los Colaboradores y Prestadores de Servicios directamente contratados por Itaú Unibanco deben adherirse formalmente mediante un documento por el que se comprometan a actuar de acuerdo a las políticas de Seguridad de la Información.

Los contratos de la Institución deben tener una cláusula que asegure la confidencialidad de las informaciones.

4.9 Medidas Disciplinarias

Violaciones de esta política están sujetas a las sanciones disciplinarias establecidas en la circular RP-29, en los reglamentos internos de negocio de Itaú Unibanco y en la legislación vigente en Brasil y en los países donde las empresas se encuentren.

5. GLOSARIO

Casa Matriz: Itaú Unibanco Brasil

Segregación de funciones: acto por el cual el colaborador no puede ejercer más de una función en el proceso de aprobación.

6. AGENCIA RESPONSABLE

El Conselho de Segurança Corporativa es responsable de mantener y actualizar esta política.