BCU
SERVICIOS INSTITUCIONALES
Seguridad e Infraestructura

Política de Seguridad de la Información

Área de Seguridad e Infraestructura

Gerencia de Servicios Institucionales

Emitido por:	Revisado por:	Aprobado por:
Área de Seguridad e Infraestructura	Área de Tecnología de la Información Gerencia de Servicios Institucionales	Gerencia de Servicios Institucionales
Abril 2019	Abril 2019	Abril 2019

Clasificación del Documento según Acceso a la Información Pública:	**Público**

Política de Seguridad de la Información

El Banco Central del Uruguay (BCU) considera a la información como uno de sus activos de mayor relevancia. Por lo tanto, resulta indispensable, para el cumplimiento de sus cometidos, disponer y brindar en forma oportuna de la información exacta y completa. Por consiguiente, realizar una gestión segura de la información es uno de sus compromisos primordiales.

El Sistema de Gobernanza de Seguridad de la Información (SGSI) se entiende como el conjunto de normas, procedimientos y técnicas dispuesto por la organización a efectos de:

- garantizar que la información que se procese, transmita o almacene esté disponible en las oportunidades y formas requeridas
- preservar la confidencialidad de la información limitando el acceso a la misma a las personas autorizadas e identificadas fehacientemente
- asegurar la integridad de los datos frente a alteraciones accidentales o maliciosas o ante la posibilidad de repudio de los actos cuyo respaldo recae en el almacenamiento de información.

El BCU dispondrá de la organización y de los recursos necesarios para mantener su SGSI alineado a sus cometidos, conforme a las disposiciones jurídicas aplicables y a los compendios de normas o prácticas de orden tecnológico que resulten recomendables, en consistencia con los niveles riesgo y con las estrategias de respuesta aprobadas por su Dirección.

El SGSI del Banco será proactivo con el fin de acotar la exposición al riesgo inherente al uso de la tecnología de la información, en la medida que la estrategia del Banco es decididamente favorable a la incorporación de las soluciones tecnológicas que reporten oportunidades de mejora en el logro de sus cometidos.

El SGSI deberá actualizarse en marco de un ciclo de mejora continua, alternando la revisión periódica de su diseño en relación con los cambios en el contexto de necesidades y riesgos, la planificación e implementación de nuevos controles y la evaluación de los resultados obtenidos.

Las disposiciones contenidas en el SGSI (políticas, protocolos, recomendaciones u otros) deberán ser conocidas, comprendidas y cumplidas tanto por el personal del Banco como por las personas que, en virtud de sus vínculos contractuales o de cualquier otra índole, puedan tener acceso a información propia o tutelada por el mismo y a recursos tecnológicos que integran sus plataformas informáticas (hardware, software y comunicaciones). A estos efectos el SGSI deberá incluir entre sus funciones la comunicación y el control de cumplimiento de sus normas y recomendaciones por parte de las personas dentro de su alcance, ya que el conocimiento, la comprensión y la observancia de las prácticas indicadas son condiciones indispensables para una gestión segura de los activos de información.

El Directorio y el Comité de Ejecutivo de Dirección del Banco asumirán la responsabilidad y ejercerán el liderazgo en el desarrollo de la seguridad de la información, delegando convenientemente roles y responsabilidades específicas a los jerarcas y servicios de la organización.