

Política de Seguridad de la Información

Área de Seguridad e Infraestructura Gerencia de Servicios Institucionales

Emitido por:	Revisado y Validado por:	Aprobado por:
Departamento de Seguridad Lógica Gerencia de Seguridad e Infraestructura	Comité Ejecutivo de Dirección	Directorio
Abril 2022	Julio 2022	Agosto 2022

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. Resulta indispensable para el cumplimiento de sus cometidos disponer y brindar en forma oportuna información exacta y completa.

El BCU dispone de un Sistema de Gestión de Seguridad de la Información (SGSI) que consiste en un conjunto de normas, procedimientos, técnicas, controles y recomendaciones.

La Seguridad de la Información tiene como cometido la preservación de su:

- Disponibilidad: garantizar que la información que se procese, transmita o almacene esté accesible en las oportunidades y formas adecuadas para las personas autorizadas.
- Confidencialidad: establecer que la información solo puede ser accedida por las personas que tienen autorización y están identificadas fehacientemente.
- Integridad: asegurar que los datos se mantienen exactos y completos, protegidos de pérdidas o alteraciones accidentales o no autorizadas.

El SGSI se orienta a alcanzar los siguientes objetivos:

- Cumplir con los requisitos legales aplicables a la gestión de la seguridad de la información.
- Estar alineado con las buenas prácticas de seguridad de la información, reconocidas y aceptadas por el BCU.
- Clasificar y proteger la información de acuerdo a la normativa vigente y a los criterios de valoración, basados en la importancia que cada activo posee para el BCU.
- Gestionar los riesgos de seguridad de la información conforme a los parámetros definidos.
- Establecer los medios necesarios para la continuidad de las operaciones y la seguridad de la información.
- Implementar la mejora continua de la seguridad de la información y del SGSI.
- Designar a los responsables de llevar a cabo los procedimientos comprendidos en el SGSI.
- Elaborar un plan anual para cumplir con los presentes objetivos.

Las disposiciones contenidas en la presente política, así como las establecidas por el SGSI 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 del Banco o tutelada por el mismo y a recursos tecnológicos que integran sus plataformas informáticas (hardware, software y comunicaciones).

En el caso de identificar desviaciones al cumplimiento de los controles establecidos en el SGSI, el personal del Banco deberá reportar los mismos, conforme a los procedimientos definidos a tal efecto.

El Directorio ejerce el liderazgo de la seguridad de la información, asignando los recursos necesarios y delegando convenientemente atribuciones específicas a los jerarcas y servicios de la organización.

La presente política de seguridad de la información será revisada periódicamente o cuando las circunstancias lo demanden, y será aprobada por el Directorio de la Institución.

Antecedentes de la actualización propuesta para el texto de la Política de Seguridad de la Información.

Todos los marcos de buenas prácticas que se utilizan en la actualidad para el control y la mejora de la gestión institucional, incluyen recomendaciones en el sentido de la necesidad de realizar revisiones periódicas de las políticas y los procedimientos, actualizando concurrentemente los documentos que las respaldan.

En el caso de la política de Seguridad de la información del Banco, coincidieron en el tiempo la necesidad de realizar una revisión periódica, ya que la última versión de la citada política fue aprobada el 20 de junio de 2019 (RD N° 123-2019), y la presentación por parte de la Auditoría interna, de un informe acerca del gobierno de la Seguridad de la Información. El referido informe, recaído en el expediente 2022/00301, da cuenta de que si se compara la política de Seguridad de la información aprobada en el Banco en 2019 con la política publicada por AGESIC (Agencia de Gobierno Electrónico y la Sociedad de la Información y el Conocimiento), en el documento del Banco no se hace mención explícita de objetivos de especial relevancia para un sistema de gestión de seguridad de la información (en adelante SGSI).

Se tienen en cuenta del informe de auditoría puntualizaciones sobre la actual política de seguridad de la información, que son las siguientes:

- 1) No se menciona como objetivo de seguridad de la información la clasificación de la información, la que resulta necesaria para ejercer su protección en forma acorde con la clase que se asigna a cada activo.
- 2) No se establece con la necesaria claridad la responsabilidad del personal respecto a la tarea de reportar violaciones a la seguridad tanto sean éstas confirmadas como que existan indicios suficientes para proceder a su tratamiento.
- 3) No se define el acrónimo SGSI en la forma convencional, sino que la palabra "gestión" fue cambiada en esa oportunidad por "gobernanza", creando una superposición con el concepto de "gobierno de seguridad de la información", para el cual ya existen definiciones y normas específicas.
- 4) No se mencionan como un objetivo del SGSI la gestión integral de riesgos de seguridad de la información y la planificación estratégica, metodologías de uso interno, altamente vinculadas con el SGSI.

A los efectos de actualizar la política aprobada en 2019, incorporando al texto los objetivos permanentes en materia de seguridad de la información, de cuya ausencia da cuenta el referido informe, se elaboró el documento que se adjunta en el cual se redujo la longitud de la parte inicial, de carácter meramente declarativo, se abreviaron las definiciones de los "principios rectores de la

seguridad de la información, que son "disponibilidad", "confidencialidad" e "integridad" para incluir los objetivos de Seguridad de la Información (SI) destacados conforme a lo observado y a la comparación con la política de uso preceptivo en unidades del Gobierno Central, publicada por AGESIC en 2009.

Los objetivos de seguridad de la información incorporados expresamente en el texto de la nueva versión de la política de seguridad de la información comprenden: el cumplimiento de normas legales y la adhesión a buenas prácticas que cuenten con reconocimiento, la gestión de los riesgos de SI, la clasificación y la protección de la información en forma consistente, la gestión de la continuidad de las operaciones, la mejora continua del sistema de SI, el gobierno de la seguridad de la información y la planificación de metas con periodicidad anual.

El documento presentado no aborda el tema del gobierno de SI, manteniendo al Directorio del Instituto como responsable y líder en la materia, con su prerrogativa de atribuir tareas específicas a los comités, servicios y jerarquías de la organización.

El texto fue inicialmente elaborado por el Departamento de Seguridad Lógica y revisado con los especialistas en seguridad informática del área de TI.

El día 12 de julio se realizó la presentación del borrador de la nueva política ante el Comité Ejecutivo de Dirección, el que validó el texto, luego de proponer la realización de algunas modificaciones. Se evacuaron también, a instancias del CED, consultas al departamento de Auditoría de Sistemas de la AIIG en tanto el texto recoge recomendaciones de su precitado informe y a la gerencia de Planificación y Gestión Estratégica (junto a su Departamento de Procesos y Riesgos) acerca del uso del acrónimo SGSI y de la inclusión de la continuidad de las operaciones como uno de los objetivos del SGSI, lo que contó con la aprobación sin observaciones.

En función de lo expuesto se propone el presente

PROYECTO DE RESOLUCIÓN

VISTO: La Política de Seguridad de la Información aprobada por Resolución D/4/2016 de 20 de enero de 2016 y actualizada por Resolución D/123/2019 de 20 de junio de 2019.

RESULTANDO: Que es una buena práctica actualizar las políticas periódicamente a los efectos de recoger los cambios en el entorno y en las

buenas prácticas establecidas por distintos estándares internacionales y locales.

CONSIDERANDO:

1. Que para la elaboración de la nueva Política de Seguridad de la Información se recogieron las recomendaciones de la Auditoría Interna que figuran en el expediente 2022/00301.
2. Que la nueva Política de Seguridad de la Información fue elaborada con el acuerdo de las áreas de Seguridad e Infraestructura y de Tecnología de la Información.
3. Que la misma fue validada por el CED el cual propuso algunas modificaciones las que fueron recogidas en el texto que se eleva, según consta en Acta de 226 del 12 de julio de 2022.

ATENTO: A los informes presentados

SE RESUELVE:

1. Aprobar la Política de Seguridad de la Información para el Banco Central del Uruguay, cuyo texto luce de fojas 27 a 29 del expediente N° 2019-50-1-00078.
2. Encomendar a la Gerencia de Servicios Institucionales promover la publicación de la Política de Seguridad de la Información, en el marco de la transparencia activa y su difusión interna.
3. Dejar sin efecto la Resolución D/123/2019 de fecha 20/06/2019.

