1. Objetivo

El objetivo de esta política de alto nivel es establecer el propósito, la dirección, los principios y las reglas fundamentales para la gestión de la Seguridad de la Información en la organización.

2. Alcance

Esta política aplica a todo el marco de gestión de seguridad de la información con el que cuenta el Banco Macro S.A. (en adelante, "El Banco" / "la Entidad"). Este marco contempla la gestión de la seguridad de la información, y se encuentra alineado a los objetivos estratégicos del negocio y de tecnología, la gestión del dato, la clasificación de datos e información, los activos de información y los riesgos.

3. Áreas Impactadas

Alcanza tanto a colaboradores del Banco y proveedores que participen de la gestión de seguridad como a aquellas dependencias vigentes que existan con terceras partes.

Como parte del proceso tendrán especial participación: la Gerencia de Tecnología y Sistemas, la Gerencia de Seguridad de la Información, la Gerencia de Riesgos y aquellas Terceras Partes involucradas.

La función de Seguridad de la Información es ejercida por la Gerencia de Seguridad de la Información y reporta de forma periódica a la Alta Dirección y al Directorio, asegurando su alineación con los objetivos estratégicos de la Entidad.

4. Responsabilidades

Las responsabilidades relacionadas con el Marco de Gestión de Seguridad de la información son las siguientes:

La Dirección es responsable de asegurar la implementación, mantenimiento y mejora continua del SGSI, así como la provisión de los recursos necesarios para su funcionamiento eficaz.

El Comité de Seguridad de la Información (CSI) es responsable de la coordinación operativa del SGSI y de informar regularmente sobre su desempeño.

La Dirección realizará revisiones del SGSI al menos una vez al año, o ante cambios significativos, con el fin de evaluar su idoneidad, adecuación y eficacia.

El Comité de Seguridad de la Información promoverá e implementará programas de capacitación y concientización en seguridad de la información.

Los propietarios de los activos son responsables de asegurar la protección de la confidencialidad, integridad y disponibilidad de la información bajo su control.

Todos los colaboradores deben reportar de manera inmediata cualquier incidente o debilidad de seguridad conforme a los procedimientos establecidos.

5. Política de Seguridad de la Información

La Dirección reconoce la importancia de proteger los activos de información y se compromete a prevenir la destrucción, divulgación, modificación o uso no autorizado de la información, mediante la implementación, mantenimiento y mejora continua.

La Seguridad de la Información se define como la preservación de:
Confidencialidad, garantizando que la información sea accesible únicamente a quienes estén autorizados.
Integridad, asegurando la exactitud y completitud de la información y sus procesos asociados.
Disponibilidad, garantizando que la información esté accesible para los usuarios autorizados cuando se requiera.
La organización establecerá, implementará, mantendrá y mejorará continuamente un conjunto de controles apropiados, basados en la gestión de riesgos, incluyendo políticas, procedimientos, estructuras organizativas y soluciones tecnológicas, con el fin de proteger

la confidencialidad, integridad y disponibilidad de la información, incluyendo los datos personales (PII), a lo largo de todo su ciclo de vida.

Asimismo, la organización establece:

- La definición de objetivos anuales de seguridad de la información.
- La implementación de un proceso de gestión de riesgos que permita identificar, evaluar y tratar los riesgos de seguridad.
- La clasificación y protección de la información según su criticidad y sensibilidad.
- La concientización y formación continua del personal.
- La gestión y reporte de incidentes de seguridad.
- La implementación de medidas para asegurar la continuidad de las operaciones.

6. Objetivos y Medición

Los objetivos del SGSI están alineados con la estrategia y los objetivos de negocio de la organización, y tienen como finalidad fortalecer la protección de la información, mejorar la reputación corporativa y reducir el impacto de incidentes de seguridad.

La organización medirá periódicamente el grado de cumplimiento de los objetivos, registrando los resultados, metodologías y frecuencias en el Informe de Medición correspondiente.

7. Cumplimiento Regulatorio

La organización se compromete a cumplir con la legislación vigente, los requisitos regulatorios y las obligaciones contractuales aplicables en materia de seguridad de la información y protección de datos personales y con toda la normativa del BCRA y local vigente.

La presente política es de cumplimiento obligatorio para todo el personal y terceros relevantes.