1. Objetivo

El presente documento establece el compromiso de Kueski para lograr la implementación, mantenimiento y mejora continua de su Sistema de Gestión de la Información (SGSI), la cual da cumplimiento a la cláusula 5 del estándar ISO/IEC 27001:2022.

Kueski reafirma su compromiso y dedicación en el diseño e implementación de un Sistema de Gestión para la Seguridad de la Información, la cual se alinea a estándares internacionales como ISO 27001 y Leyes Federales de Protección de Datos Personales.

2. Alcance

Esta política aplica a todas las personas (colaboradores o terceros) que son parte en los procesos de negocio o procesos técnicos de Kueski que manejen, procesen, transformen, resguarden o transmitan la información definida en el alcance del SGSI.

3. Lineamientos

3.1 En Kueski reconocemos a la información como un activo importante para la ejecución de los procesos de negocio y la entrega de los productos y servicios comprometidos con nuestros clientes y socios de negocio.

3.2 Por lo anterior nos comprometemos a la preservación de las propiedades de confidencialidad, integridad y disponibilidad de la información y protección de datos personales.

3.3 De igual forma, en Kueski nos comprometemos a cumplir con las leyes, regulaciones, contratos y acuerdos relativos a la seguridad de la información y protección de datos personales a las que Kueski esté obligado o requerido a observar.

3.4 Reconocemos que en la actualidad la información se encuentra sujeta a múltiples riesgos que podrían afectar sus propiedades, teniendo como consecuencia posibles impactos operacionales, económicos, reputacionales y de cumplimiento.

3.5 Para gestionar apropiadamente estos riesgos, Kueski se compromete, a través de su alta dirección, a planificar, implementar, operar, monitorear, medir, analizar, evaluar, revisar,

auditar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) en conformidad con las buenas prácticas internacionales más actualizadas.

3.6 La responsabilidad interna sobre el mantenimiento del SGSI de Kueski se encuentra a cargo del equipo de Seguridad y todo el personal que forma parte de la organización tiene la responsabilidad de cumplir con los roles y actividades que les sean designados dentro del sistema.

3.7 El SGSI de Kueski debe incorporar como mínimo los siguientes requisitos:

- Entendimiento de la organización a través de un análisis de contexto interno y externo, así como el análisis de requerimientos y expectativas de partes interesadas.
- Establecer y documentar un alcance del SGSI indicando explícitamente cualquier exclusión aplicable.
- Planificar, implementar, operar y mejorar un proceso de gestión y tratamiento de riesgos de Seguridad de la Información.
- Mantener un documento actualizado de Declaración de Aplicabilidad de controles.
- Planificación de cambios en el SGSI.
- Aseguramiento de recursos, incluyendo la gestión de un presupuesto anual para su mantenimiento, así como el personal con las competencias y habilidades apropiadas para la operación del SGSI.
- Mantener un programa permanente de concientización en Seguridad de la Información para todo el personal de Kueski y otras partes interesadas relevantes.
- Un control de documentos del SGSI que permita asegurar la clasificación de estos, así como el aseguramiento de su disponibilidad, idoneidad y seguridad.
- Programa de monitoreo, medición, análisis y evaluación.
- Programa de auditoría interna.
- Revisión de la dirección de forma periódica.
- Programa de comunicación interna y externa sobre Seguridad de la Información.
- Procedimiento de gestión de no conformidades y acciones correctivas.

3.8 Como parte del SGSI se deberán establecer y actualizar de forma periódica los resultados de los objetivos de seguridad de la información que incluyan como mínimo: lo que se va a hacer, los recursos necesarios, responsabilidades, fechas de conclusión y criterios de evaluación de resultados.

3.9 En Kueski nos comprometemos con la mejora continua de las condiciones de seguridad de la información y protección de datos personales, así como del Sistema de Gestión de Seguridad de la Información.

3.10 Cualquier excepción a las políticas definidas en este documento o asociadas al SGSI deberán ser documentadas de acuerdo al procedimiento de manejo de excepciones de Seguridad correspondiente.