


MARCO NORMATIVO DE SEGURIDAD

POL_001_A POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PÚBLICA



	POL_001_a Política de Seguridad de la Información Pública	Conf.: Uso Interno Fecha: 27/06/2023
		VERSIÓN: 1.1

1. DECLARACIÓN DE ACEPTACIÓN

La Política de Seguridad de la Información de KANBANLOG establece los principios, directrices y responsabilidades para salvaguardar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de los servicios e información de nuestra organización. Esta política se desarrolla en línea con las directrices del Esquema Nacional de Seguridad (ENS) 311/2022 y tiene como objetivo garantizar la protección adecuada de los activos de información y tecnología de la organización.

2. Ámbito de Aplicación:

Esta política es aplicable a todos los empleados, contratistas, proveedores y terceros que tengan acceso a la información y a los sistemas de tecnología de la información de KANBANLOG. Todos los usuarios están obligados a cumplir con esta política y las medidas de seguridad establecidas para proteger la información de la organización.

3. Dimensiones de Seguridad de la Información:


La seguridad de la información en KANBANLOG se aborda desde cinco dimensiones fundamentales, las cuales son:

a. Seguridad Física

Se implementarán controles físicos para proteger los activos y equipos de la organización contra daños, robo, acceso no autorizado y riesgos ambientales. Se establecerán procedimientos para gestionar el acceso a las instalaciones y áreas restringidas, garantizando así la seguridad de la información almacenada físicamente.

b. Seguridad Lógica

Se establecerán medidas para proteger los sistemas de información y los datos almacenados en ellos contra el acceso no autorizado, el uso indebido y la manipulación malintencionada. Se implementarán políticas de contraseñas

	POL_001_a Política de Seguridad de la Información Pública	Conf.: Uso Interno Fecha: 27/06/2023
		VERSIÓN: 1.1

robustas, controles de acceso basados en roles y sistemas de autenticación seguros para prevenir incidentes de seguridad informática.

c. Seguridad Organizativa

Se definirán claramente las responsabilidades y roles de seguridad de la información dentro de la organización. Se promoverá una cultura de seguridad, donde todos los miembros de KANBANLOG sean conscientes de la importancia de proteger la información y se fomentará la capacitación periódica en seguridad de la información.

d. Seguridad Jurídica

Se cumplirán todas las leyes y regulaciones aplicables en materia de protección de datos y seguridad de la información. Se establecerán procedimientos para gestionar incidentes de seguridad, notificando a las autoridades correspondientes y a los afectados, en caso de que ocurra una brecha de seguridad que pueda afectar la privacidad de los datos.


e. Seguridad Tecnológica

Se implementarán medidas de seguridad en los sistemas y tecnologías de la información para protegerlos contra amenazas internas y externas. Se realizarán evaluaciones de riesgos y auditorías periódicas para garantizar la efectividad de los controles de seguridad y se tomarán acciones correctivas en caso de identificar vulnerabilidades o debilidades en los sistemas.

4. Compromiso con la Confidencialidad, Integridad, Disponibilidad, Autenticidad y Trazabilidad

En KANBANLOG, nos comprometemos a salvaguardar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de nuestros servicios e información.

Nuestro objetivo es garantizar la protección adecuada de la información sensible y valiosa que maneja nuestra organización, asegurando su disponibilidad cuando sea requerida, su autenticidad para que pueda confiarse y su trazabilidad para conocer su origen y uso.

	POL_001_a Política de Seguridad de la Información Pública	Conf.: Uso Interno Fecha: 27/06/2023
		VERSIÓN: 1.1

5. Responsabilidades

Todos los miembros de KANBANLOG tienen la responsabilidad de cumplir con esta Política de Seguridad de la Información y las medidas de seguridad establecidas. Los líderes de equipos y gerentes tienen la responsabilidad de garantizar que sus equipos comprendan y cumplan con estas directrices.

6. Actualizaciones y Revisiones

Esta Política de Seguridad de la Información se revisará periódicamente para asegurar su vigencia y relevancia. Las actualizaciones serán comunicadas a todos los miembros de la organización, y se espera que todos estén al tanto de los cambios y los cumplan.

7. Incumplimiento

El incumplimiento de esta política y las medidas de seguridad establecidas puede dar lugar a acciones disciplinarias, incluyendo sanciones o terminación de la relación laboral o contractual.

La Dirección

Valencia, a Junio de 2023