INFORMATION SECURITY POLICY

1. Objective

The objective of this Information Security Policy is to establish a reference framework for the protection of information at Maakal, Inc. and its subsidiaries, guaranteeing its confidentiality, integrity, and availability. This policy seeks to mitigate risks associated with information management, prevent security incidents, and ensure compliance with applicable standards and regulations, including the protection of customer information

2. Scope

This policy applies to all employees, contractors, suppliers, and third parties who access, process, store, or manage information of Maakal, Inc.. It extends to all information systems, databases, storage devices, and any other technological resource used in the company's operation.

3. Definitions

Information Security: A set of measures and controls designed to protect information against unauthorized access, alteration, or destruction.

Confidentiality: Guarantee that information is accessible only by authorized persons.

Integrity: Ensuring that information remains accurate, complete, and free from unauthorized modifications.

Availability: Guarantee that information is available when required by authorized users.

Security Incident: An event that puts the security of information at risk.

Information Security Risk: The possibility that a threat exploits a vulnerability, causing an impact on the organization.

Supplier: An external company or entity that supplies goods, services, or technologies to Maakal, Inc., and must comply with the information security requirements established in this policy.

Client: A person or entity receiving services from Maakal, Inc., whose information must be protected in accordance with this policy.

4. Responsibilities

Role	Responsibility
Senior Management	Senior Management is responsible for approving the general cybersecurity policy and ensuring it is aligned with the organization's strategic objectives.
CISO	In charge of designing, implementing, maintaining, and reviewing the general cybersecurity policy. Additionally, leads the management of information-related risks, coordinates the implementation of controls, supervises compliance with policies, and reports periodically to Senior Management.
Collaborators	All users and collaborators of the organization have the responsibility to comply with the guidelines established in the cybersecurity policy.

5. General Description

Maakal, Inc. recognizes the importance of information security in its operation and in its relationship with employees, clients, and suppliers. Information is a fundamental asset that must be protected against internal and external threats to ensure business continuity and the fulfillment of strategic objectives.

5.1 Security Principles

- The principle of least privilege will be applied, limiting access to information only to those who require it for their functions.Access control measures will be implemented, ensuring adequate authentication and authorization.
- Periodic backups will be performed to ensure information availability.
- Cryptographic controls will be applied for the protection of sensitive data.
- An incident response plan will be established to mitigate possible security breaches.
- Periodic risk analyses will be conducted, identifying potential threats and applying appropriate mitigation measures.
- Suppliers will be required to comply with security standards and notify of relevant incidents.
- The protection of client information will be guaranteed through appropriate processes and controls.

5.2 Risk Management

- Information security risk assessments will be conducted periodically.
- Potential threats such as cyberattacks, human errors, technological failures, and natural disasters will be identified.

- The impact and probability of risks will be evaluated, defining strategies to reduce their impact on the organization.
- Security controls will be implemented based on a risk management approach.
- Policies and procedures will be reviewed regularly to adapt to new emerging risks.

5.3 Security Incident Management

- A formal incident management process will be established, including detection, notification, analysis, containment, eradication, and recovery from security incidents.
- A team responsible for incident response will be designated with clearly defined roles and responsibilities.
- All incidents must be reported immediately to the Information Security Officer.
- A post-incident analysis will be conducted to identify root causes and prevent recurrence.
- Detailed records of security incidents will be maintained for future audits and policy improvements.
- Suppliers will be required to report any security incident that may affect Maakal, Inc. and its clients.

5.4 Information Backups

- Backups of information, software, and system images will be performed according to data criticality and business recovery requirements.
- Backups will have adequate physical and logical protection measures (such as encryption) and, where feasible, will be stored in a geographic location distinct from the main one to prevent data loss in the event of physical disasters.
- Periodic restoration tests will be performed to verify that backup media are reliable and that information can be effectively recovered within the required time.

5.5 Training and Awareness

- Training programs on information security will be carried out for all employees.
- A security culture based on good practices and regulatory compliance will be fostered.
- Specific training on risk management will be included for all key employees and collaborators.
- Training will be provided to suppliers regarding Maakal, Inc.'s security expectations and requirements.
- Employees will be trained on the secure handling of client information.

5.6 Audit, Compliance, and Continuous Improvement

- Periodic internal and external audits will be conducted to evaluate policy compliance, verifying the correct implementation of security measures and compliance with standards by suppliers.

- Findings will be documented, improvement plans will be executed, and senior management will be informed about results and progress in security.

6. Periodicity

This policy must be reviewed periodically whenever required (at least once a year). If necessary, the policy will be adjusted based on presenting conditions.

Likewise, it will be reviewed in the event of changes to national regulations

7. Sanctions

Non-compliance with this policy by employees, contractors, suppliers, or any linked third party may result in disciplinary sanctions in accordance with Maakal, Inc.'s internal regulations, including warnings, suspension, or termination of the labor or commercial contract. In serious cases, legal actions may be taken according to current legislation. These measures also apply to negligence in protecting client information or failure to report security incidents

8. References

This policy is developed in conformity with the ISO/IEC 27001:2022 standard, ensuring its alignment with international best practices in information security management.

9. Validity

This policy enters into force upon its approval and is mandatory for all members of Maakal, Inc.

Change control

Version	Prepared by	Approved by	Changes
1.0	Alejandro Coral Zambrano 11/03/2025	Jorge Mario Ramírez 02/07/2025	Document creation
1.1	Alejandro Coral Zambrano 20/11/2025	Jorge Mario Ramírez 27/11/2025	Format, compliance, and audit points updated; Backups point added.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. Objetivo

La presente Política de Seguridad de la Información tiene como objetivo establecer un marco de referencia para la protección de la información de Maakal, Inc. y sus filiales, garantizando su confidencialidad, integridad y disponibilidad. Esta política busca mitigar riesgos asociados a la gestión de la información, prevenir incidentes de seguridad y asegurar el cumplimiento de normativas y regulaciones aplicables, incluyendo la protección de la información de clientes.

2. Alcance

Esta política aplica a todos los empleados, contratistas, proveedores y terceros que accedan, procesen, almacenen o gestionen información de Maakal, Inc. Se extiende a todos los sistemas de información, bases de datos, dispositivos de almacenamiento y cualquier otro recurso tecnológico utilizado en la operación de la empresa.

3. Definiciones

Seguridad de la información: Conjunto de medidas y controles destinados a proteger la información contra accesos no autorizados, alteraciones o destrucciones.

Confidencialidad: Garantía de que la información solo es accesible por personas autorizadas.

Integridad: Asegurar que la información se mantiene exacta, completa y libre de modificaciones no autorizadas.

Disponibilidad: Garantía de que la información esté disponible cuando sea requerida por usuarios autorizados.

Incidente de seguridad: Evento que pone en riesgo la seguridad de la información.

Riesgo de seguridad de la información: Posibilidad de que una amenaza explote una vulnerabilidad, causando un impacto en la organización.

Proveedor: Empresa o entidad externa que suministra bienes, servicios o tecnologías a Maakal, Inc., y que debe cumplir con los requisitos de seguridad de la información establecidos en esta política.

Cliente: Persona o entidad que recibe servicios de Maakal, Inc., y cuya información debe ser protegida conforme a esta política.

4. Responsables

Cargo	Responsable
Alta dirección	La Alta Dirección es responsable de aprobar la política general de ciberseguridad y garantizar que esté alineada con los objetivos estratégicos de la organización.
CISO	Encargado de diseñar, implementar, mantener y revisar la política general de ciberseguridad. Además, lidera la gestión de riesgos relacionados con la información, coordina la implementación de controles, supervisa el cumplimiento de las políticas y reporta periódicamente a la Alta Dirección.
Colaboradores	Todos los usuarios y colaboradores de la organización tienen la responsabilidad de cumplir con los lineamientos establecidos en la política de ciberseguridad.

5. Descripción General

Maakal, Inc. reconoce la importancia de la seguridad de la información en su operación y en la relación con sus empleados, clientes y proveedores. La información es un activo fundamental que debe ser protegido contra amenazas internas y externas para asegurar la continuidad del negocio y el cumplimiento de sus objetivos estratégicos.

5.1 Principios de Seguridad

- Se aplicará el principio de mínimo privilegio, limitando el acceso a la información solo a quienes lo requieran para sus funciones.
- Se implementarán medidas de control de acceso, asegurando la autenticación y autorización adecuadas.
- Se realizarán copias de seguridad periódicas para garantizar la disponibilidad de la información.
- Se aplicarán controles criptográficos para la protección de datos sensibles.
- Se establecerá un plan de respuesta a incidentes para mitigar posibles brechas de seguridad.
- Se realizarán análisis de riesgos periódicos, identificando amenazas potenciales y aplicando medidas de mitigación adecuadas.
- Se exigirá a los proveedores el cumplimiento de los estándares de seguridad y la notificación de incidentes relevantes.
- Se garantizará la protección de la información de los clientes mediante procesos y controles adecuados.

5.2 Gestión de Riesgos

- Se realizarán evaluaciones de riesgos de seguridad de la información de manera periódica.
- Se identificarán amenazas potenciales como ataques cibernéticos, errores humanos, fallos tecnológicos y desastres naturales.
- Se evaluará el impacto y probabilidad de los riesgos, definiendo estrategias para reducir su impacto en la organización.
- Se implementarán controles de seguridad basados en un enfoque de gestión de riesgos.

- Se revisarán las políticas y procedimientos regularmente para adaptarse a nuevos riesgos emergentes.

5.3 Gestión de Incidentes de Seguridad

- Se establecerá un proceso formal de gestión de incidentes que incluirá la detección, notificación, análisis, contención, erradicación y recuperación ante incidentes de seguridad.
- Se designará un equipo responsable de la respuesta a incidentes con roles y responsabilidades claramente definidos.
- Todos los incidentes deberán ser reportados inmediatamente al Responsable de Seguridad de la Información.
- Se realizará un análisis posterior al incidente para identificar causas raíz y evitar recurrencias.
- Se mantendrán registros detallados de los incidentes de seguridad para futuras auditorías y mejoras en la política.
- Se requerirá que los proveedores informen sobre cualquier incidente de seguridad que pueda afectar a Maakal, Inc. y a sus clientes.

5.4 Respaldos de Información (Backup)

- Se realizarán copias de seguridad de la información, software e imágenes de los sistemas de acuerdo con la criticidad de los datos y los requisitos de recuperación del negocio.
- Las copias de seguridad contarán con medidas de protección física y lógica adecuadas (como cifrado) y, cuando sea factible, se almacenarán en una ubicación geográfica distinta a la principal para prevenir pérdida de datos ante desastres físicos.
- Se realizarán pruebas periódicas de restauración para verificar que los medios de respaldo son fiables y que la información puede ser recuperada efectivamente en el tiempo requerido.

5.5 Capacitación y Concienciación

- Se llevarán a cabo programas de formación para todos los empleados en materia de seguridad de la información.
- Se fomentará una cultura de seguridad basada en buenas prácticas y el cumplimiento de normativas.
- Se incluirá capacitación específica en la gestión de riesgos para todos los empleados y colaboradores clave.
- Se proporcionará formación a proveedores sobre las expectativas y requisitos de seguridad de Maakal, Inc.
- Se capacitará a los empleados en el manejo seguro de la información de los clientes.

5.6 Auditoria , Cumplimiento y Mejora Continua.

- Se realizarán auditorías internas y externas periódicas para evaluar el cumplimiento de la política, verificando la correcta implementación de medidas de seguridad y el cumplimiento de los estándares por parte de proveedores. Se documentarán hallazgos, se ejecutarán planes de mejora y se informará a la alta dirección sobre los resultados y avances en seguridad.

6. Periodicidad

La presente política deberá ser revisada periódicamente cada vez que se requiera (mínimo una vez al año). En caso de ser necesario, la política será ajustada con base en las condiciones que se presenten.

De igual manera, se revisará en caso de que la normativa del país cambie.

7. Sanciones

El incumplimiento de esta política por parte de empleados, contratistas, proveedores o cualquier tercero vinculado podrá dar lugar a sanciones disciplinarias conforme a los reglamentos internos de Maakal, Inc., incluyendo amonestaciones, suspensión o terminación del contrato laboral o comercial. En casos graves, se podrán tomar acciones legales según la legislación vigente. Estas medidas también aplican ante negligencia en la protección de la información de clientes o ante la falta de reporte de incidentes de seguridad.

8. Referencias

Esta política se desarrolla en conformidad con la norma ISO/IEC 27001:2022, asegurando su alineación con las mejores prácticas internacionales en gestión de seguridad de la información.

9. Vigencia

Esta política entra en vigor a partir de su aprobación y es de obligatorio cumplimiento para todos los integrantes de Maakal, Inc.

Control de cambios

Versión	Elaborado por	Aprobado por	Cambios
1.0	Alejandro Coral Zambrano 11/03/2025	Jorge Mario Ramírez 02/07/2025	Creación de documento
1.1	Alejandro Coral Zambrano 20/11/2025	Jorge Mario Ramírez 27/11/2025	Se actualiza formato y puntos de cumplimiento y auditoria, se agrega punto de Backups.