## CLASIFICACIÓN Y CONFIDENCIALIDAD

Este documento es clasificado como **"Uso Publico"**.

El presente documento es propiedad del grupo Keralty y está restringido a los funcionarios de la organización que cuenten con la autorización expresa para su consulta.

No se permite la reproducción total o parcial de este documento, así como su transmisión a terceros sin la autorización del responsable designado por el grupo Keralty.



## LISTA DE DISTRIBUCIÓN

Este documento es de uso interno del grupo Keralty y su copia debe ser controlada y registrada de acuerdo a los procedimientos establecidos por la organización. Su distribución se debe realizar de acuerdo a la lista definida en la tabla de distribución maestra SGSI.

Todo cambio realizado a este documento debe ser controlado, documentado de acuerdo al procedimiento de Control documental y registrados en la tabla de control de cambios del presente documento.

## TABLA DE CONTENIDO

## 1. OBJETIVO.

El objetivo de la presente política es garantizar la protección de los activos de información, manteniendo un nivel apropiado de seguridad para aquellos que sean accesibles por proveedores y/o terceros, estableciendo las condiciones para el uso de dichos activos y supervisando el cumplimiento de dichas condiciones por parte del personal externo (proveedores y/o terceros) del grupo Keralty.

## 2. ALCANCE.

La presente política aplica para las empresas o personal externo a la organización (proveedores y/o terceros) que tengan acceso a los sistemas de información o a los recursos que manejan activos de información del grupo Keralty.

## 3. DEFINICIONES

Para una mejor comprensión de los términos utilizados en este documento, se recomienda consultar el **SIG-SI-MSC-PL01-FR06 Glosario de conceptos.**



## 4. RELACIONES CON PROVEEDORES.

### 4.1. Seguridad de la Información en las Relaciones con Proveedores.

#### 4.1.1 Política de seguridad de la información para la relación con proveedores

**a.** Todos los procesos de contratación de proveedores y/o terceros del grupo Keralty o quien haga sus veces en los diferentes países, deben incluir los requisitos de seguridad de la información, ciberseguridad, privacidad y recuperación ante desastres (DRP), definidos por las gerencias corporativas de seguridad de la información y tecnología de acuerdo con el objeto a contratar, los cuales están contenidos en las condiciones generales de compra y en el anexo de requerimientos técnicos de la vicepresidencia global de sistemas de información (si aplica) .

**b.** Es responsabilidad de los dueños de la información y/o líderes integrales de los procesos de contratación en los diferentes negocios o quien haga sus veces en los diferentes países, garantizar que los requisitos de seguridad de la información, protección de datos y recuperación ante desastres (DRP) sean incluidos en los procesos de contratación desde su estudio inicial hasta la firma del contrato.

**c.** La gerencia corporativa de seguridad de la información o quien haga sus veces en los diferentes países, debe definir y ejecutar un plan de revisión de acuerdo a su criticidad, a los terceros que accedan, manejen, procesen, almacenen, transporten y/o custodien información confidencial del grupo Keralty, con el fin de verificar el

cumplimiento de los requisitos de seguridad, ciberseguridad, privacidad y recuperación ante desastres (DRP) establecidos en el contrato y los documentos técnicos que le soportan.

**d.** Todos los colaboradores de terceros críticos que accedan, manejen, procesen almacenen, transporten y/o custodien información confidencial del grupo Keralty, deben recibir y aprobar las capacitaciones de seguridad establecidas por la gerencia corporativa de seguridad de la información.

**e.** Todos los colaboradores de terceros críticos que accedan, manejen, procesen almacenen, transporten y/o custodien información confidencial del grupo Keralty, deben cumplir con los requisitos de seguridad de la información y ciberseguridad definidos en las políticas corporativas, procedimientos, estándares y guías corporativas de seguridad de la información aplicables al objeto contractual.

**f.** Es responsabilidad del líder integral del proceso o quien haga sus veces en los diferentes países, supervisor y/o gestor del contrato garantizar que el contrato que sea suscrito con terceros, tenga definidos los requisitos legales relacionados con privacidad, derechos de propiedad intelectual y derechos de autor.

**g.** Es responsabilidad del líder integral del proceso o quien haga sus veces en los diferentes países, supervisor y/o gestor del contrato, asegurar el cumplimiento de los requisitos de seguridad de la información, ciberseguridad, privacidad y recuperación ante desastres (DRP) durante la ejecución del mismo.



### 4.1.2. Tratamiento de la Seguridad dentro de los acuerdos con proveedores.

**a.** Todos los terceros que accedan, manejen, procesen almacenen, transporten y/o custodien información confidencial del grupo Keralty, deben contar con un acuerdo de confidencialidad firmado que esté avalado por la vicepresidencia jurídica del grupo Keralty ó el área legal en cada país según aplique.

*Nota: Si la relación contractual con los terceros se formaliza a través de órdenes de compra o de contratos, estos deberán incluir la cláusula de confidencialidad correspondiente, adecuado a los términos y condiciones del negocio. En caso tal de que no lo incluya, se deberá hacer parte de los mismos a través de las condiciones generales de compra en calidad de anexo.*

**b.** Es responsabilidad de la vicepresidencia de compras o quien haga sus veces en los diferentes países incluir en las actas de entrega del proceso, las obligaciones de los gestores o líderes de los diferentes procesos contractuales, frente al cumplimiento

y alineación con las políticas corporativas de seguridad de la información y demás políticas de la Vicepresidencia Global de sistemas de información del grupo Keralty.

### 4.1.3. Cadena de suministro de las tecnologías de información y comunicaciones.

**a.** La vicepresidencia jurídica o quien haga sus veces en los diferentes países debe definir un acuerdo de confidencialidad en donde se tenga en cuenta todos los requisitos internos, legales y reglamentarios del grupo Keralty.

## 4.2. Gestión de la Prestación de Servicios de Proveedores.

### 4.2.1. Seguimiento y revisión de los servicios de los proveedores.

**a.** Es responsabilidad del líder integral del proceso, supervisor y/o gestor del contrato garantizar el cumplimiento de todos los requisitos de seguridad de la información y ciberseguridad definidos en los contratos.

### 4.2.2. Gestión de cambios en los servicios de los proveedores.

**a.** En el caso que el grupo Keralty realice cambios en las condiciones contractuales con los terceros, el área encargada de la supervisión del contrato, debe garantizar que los requisitos de seguridad de la información se mantengan vigentes y que los cambios propuestos no generen riesgos a los activos de información de la organización.

| HISTORIAL DE CAMBIOS | | |
|---|---|---|
| **VERSIÓN** | **FECHA** | **RAZÓN DEL CAMBIO** |
| 1 | 06/Dic/2021 | Versión Inicial |
| 2 | 28/Oct/2022 | Se ajusta el documento de acuerdo a las observaciones del proceso de compras |
| 3 | 24/Abr/2023 | Se realiza revisión de la política de organización interna de seguridad de la información, respecto a los lineamientos definidos en el nuevo estándar ISO/IEC 27001:2022.Dado que la Gerencia de Compras pasó a ser Vicepresidencia de Compras se toma la decisión de dejar el presente documento con Versión No.1 |
| 3 | 26/Abr/2024 | Se ajusta la nomenclatura del documento, donde se incluyen las siglas MKE; M: País México y KE: Compañía Keralty, de acuerdo a lo definido en el documento SIG-SI-MKE-PL01-PR01 Procedimiento de control de documentos.Se ajustan a nivel de forma y redacción de algunos numerales de la política.Se omite la palabra privacidad, dado que ya no está bajo el alcance de la Gerencia corporativa de seguridad de la información. |
| 3 | 26/May/2025 | En el apartado de definiciones se enlaza a la consulta del documento SIG-SI-MKE-PL01-FR06 Glosario de conceptos.Se ajusta el literal (e), del numeral 4.1.1 Política de seguridad de la información para la relación con proveedores |
| 3.3 | 20/Abr/2026 | Se Actualiza clasificación documental |



| ELABORÓ | REVISÓ | APROBÓ |
|---|---|---|
| **Nombre:** Daniel Fierro Sanchez<br>**Cargo:** Analista de Sistemas Seguridad de la Información<br>**Fecha:** 20/Abr/2026 | **Nombre:** Carlos Alfonso Tirado Zamudio<br>**Cargo:** Coordinador de Seguridad de la Información<br>**Fecha:** 20/Abr/2026 | **Nombre:** Francisco Javier Martínez<br>**Cargo:** Gerente de Seguridad de la Información<br>**Fecha:** 20/Abr/2026 |