CLASIFICACIÓN Y CONFIDENCIALIDAD

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

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 empresarial 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 empresarial Keralty.

3. RELACIONES CON PROVEEDORES.

3.1. Seguridad de la Información en las Relaciones con Proveedores.

3.1.1. 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, deben incluir los requisitos de seguridad de la información, ciberseguridad, protección de datos 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 seguridad (si aplica) .

b. Es responsabilidad de los dueños de la información y/o líderes integrales de los procesos de contratación en los diferentes negocios, 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, 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 Empresarial Keralty, con el fin de verificar el

cumplimiento de los requisitos de seguridad 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 Empresarial 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 Empresarial Keralty, deben cumplir con los requisitos de seguridad, ciberseguridad y privacidad definidos en las políticas corporativas de seguridad de la información.

f. Es responsabilidad del supervisor y/o gestor del contrato garantizar que el contrato que sea suscrito con terceros, tenga definidos los requisitos legales relacionados con la protección de datos personales, derechos de propiedad intelectual y derechos de autor.

g. Es responsabilidad del supervisor y/o gestor del contrato asegurar el cumplimiento de los requisitos de seguridad de la información, ciberseguridad, protección de datos y recuperación ante desastres (DRP) durante la ejecución del mismo.

3.1.2. 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 Empresarial Keralty, deben contar con un acuerdo de confidencialidad firmado que esté avalado por la Vicepresidencia Jurídica del Grupo Empresarial Keralty o 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 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 del Grupo Empresarial Keralty.

3.1.3. Cadena de suministro de las tecnologías de información y comunicaciones.

a. La Vicepresidencia Jurídica debe definir un acuerdo de confidencialidad en donde se tenga en cuenta todos los requisitos internos, legales y reglamentarios del Grupo Empresarial Keralty.

3.2. Gestión de la Prestación de Servicios de Proveedores.

3.2.1. Seguimiento y revisión de los servicios de los proveedores.

a. El líder integral es responsable de garantizar el cumplimiento de todos los requisitos de seguridad de la información, ciberseguridad y privacidad definidos en los contratos.

3.2.2. 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.

4. CONTROL DE CAMBIOS.

Tabla 1 Detalle del control de cambios

FECHA	CAMBIO	VERSIÓN
06/12/2021	Versión Inicial	1.0
28/10/2022	Se ajusta el documento de acuerdo a las observaciones del proceso de compras	
24/04/2023	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	

5. FLUJO DE APROBACIÓN.

Tabla 2 Detalle del flujo de aprobación

ELABORÓ	REVISÓ	APROBÓ
Nombre: Grupo de apoyo de seguridad de la información. **Cargo/Área/Proceso:** Gerencia de Seguridad de la Información. **Fecha:** 24/04/2023	**Nombre:** Rene Alejandro Riachi **Cargo/Área/Proceso**: Director de seguridad de la información. **Fecha**: 24/04/2023 **Nombre:** Diana Mendieta **Cargo/Área/Proceso:** Vicepresidente de compras **Fecha:** 26/07/2023 **Nombre:** Javier Galván. **Cargo/Área/Proceso:** Gerencia Corporativa de tecnología. **Fecha:** 26/07/2023 **Nombre:** Francisco Vega Ortiz **Cargo/Área/Proceso:** Director de contratación - Central Jurídica. **Fecha:** 26/07/2023	**Nombre:** Mikel Ruíz **Cargo/Área/Proceso:** CEPO - Ingeniería y Compras **Fecha:** 26/07/2023 **Nombre:** Diana Mendieta **Cargo/Área/Proceso:** Vicepresidente de compras **Fecha:** 26/07/2023 **Nombre:** Santiago Thovar. **Cargo/Área/Proceso:** Vicepresidente Global de Sistemas de Información (CIO). **Fecha:** 26/07/2023 **Nombre:** Alejandro Ramírez Romero. **Cargo/Área/Proceso:** Gerente Corporativo de Seguridad de la Información. **Fecha:** 26/07/2023