CLASIFICACIÓN Y CONFIDENCIALIDAD

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

LISTA DE DISTRIBUCIÓN

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

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

TABLA DE CONTENIDO

1 OBJETIVO.

Establecer una política corporativa de seguridad de la información que apoye el cumplimiento de los objetivos de negocio del grupo Keralty y que sea aplicable para cualquiera de las empresas y países donde este tenga presencia.

2 ALCANCE.

La política corporativa de seguridad de la información aplica a todas las empresas del grupo Keralty, funcionarios, terceros y demás partes interesadas que por sus funciones custodian, procesan, transportan y/o almacenan información del grupo y/o de terceros.

3 DEFINICIONES

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

4 DECLARACIÓN GENERAL.

El grupo Keralty consciente de la importancia de proteger los activos de información que procesa, transporta, almacena y/o custodia sin importar su presentación ya sea física o digital, establece esta “Política Corporativa de Seguridad de la Información”, con el fin de salvaguardar la integridad, confidencialidad y disponibilidad de esta. La presente política está alineada al cumplimiento de los valores corporativos y de los requisitos legales, normativos, regulatorios y/o contractuales que deben cumplirse en cada uno de los países donde el grupo Keralty tiene presencia. Permitiendo así generar una cultura de debida diligencia en la protección de información, con el liderazgo y compromiso de la alta dirección, otorgando los recursos necesarios para la planeación, implementación, gestión, medición, verificación y mejora continua del sistema corporativo de gestión de seguridad de la información.

5 OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN.

A continuación, se describen los cinco (5) objetivos rectores del gobierno y del Sistema de Gestión Corporativo de Seguridad de la Información (SGSI) del grupo Keralty:

a) **SIG-SI-OBJ-01: Reducir la superficie de riesgo** mediante el diseño, implementación y seguimiento de controles de seguridad de la información de acuerdo con el tipo de activo, riesgo e información a proteger.

b) **SIG-SI-OBJ-02: Cumplir con los requisitos de seguridad de la información** definidos por el grupo Keralty y/o establecidos por la normativa, legislación, regulación vigente y/o acuerdo contractual mediante la vigilancia continua del contexto interno y externo del grupo y a través de procesos periódicos de validación y aseguramiento.

c) **SIG-SI-OBJ-03: Reducir el impacto de la materialización de riesgos de seguridad** de la información a partir del diseño, implementación y operación de un proceso holístico de gestión de incidentes de seguridad.

d) **SIG-SI-OBJ-04: Generar en todos los funcionarios, terceros y demás partes interesadas una cultura de protección de información** por medio de programas, capacitaciones y campañas de sensibilización en seguridad de la información y ciberseguridad.

e) **SIG-SI-OBJ-05: Mejorar las capacidades de Ciberresiliencia** del grupo Keralty a través de la incorporación de procesos, mejores prácticas internacionales, controles y tecnologías de ciberseguridad, alineadas a los procesos corporativos de negocio.

6 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN.

a) Como parte del proceso de diseño, implementación, operación, validación y mejora continua del Sistema de Gestión Corporativo de Seguridad de la Información del grupo Keralty, se han establecido un conjunto de políticas de

segundo nivel, las cuales se encuentran contenidas en el manual corporativo de políticas de seguridad de la información. Dicho manual presenta en detalle, los lineamientos específicos de seguridad de la información que han sido implementados para dar cumplimento a los requisitos establecidos por los estándares ISO/IEC 27001, ISO/IEC 27035 e ISO/IEC 27032, entre otras normativas; así como también al marco de gobierno y modelo controles establecidos en las mejores prácticas del Instituto Nacional de Estándares Americano (NIST) y el Centro de Seguridad de Internet (CIS).

A continuación, una declaración breve de las políticas de segundo nivel:

I. **SIG-SI-CKE-PL02 Política corporativa de organización interna en seguridad de la información:** El grupo Keralty debe diseñar, implementar, gestionar, medir y mejorar de forma continua los controles referentes a los roles y responsabilidades en seguridad de la información, separación de deberes, comunicación con autoridades, contacto con grupo de interés y seguridad en gestión de proyectos, con el fin de garantizar una adecuada organización de seguridad de la información que permita el cumplimiento de los objetivos corporativos y del sistema de gestión.

II. **SIG-SI-CKE-PL03 Política corporativa de seguridad para el recurso humano:** El grupo Keralty debe diseñar, implementar, gestionar, medir y mejorar de forma continua los controles aplicables a los recursos humanos antes, durante y después del empleo con el fin de garantizar una adecuada operación del Sistema de gestión de seguridad y una cultura corporativa de protección de información.

III. **SIG-SI-CKE-PL04 Política corporativa de seguridad para la gestión de activos:** El grupo Keralty debe diseñar, implementar, gestionar, medir y mejorar de forma continua los controles referentes con el inventario, uso aceptable, clasificación de la información y el manejo de soportes para todos los activos de información que hacen parte del sistema de gestión de seguridad de la información.

IV. **SIG-SI-CKE-PL05 Política corporativa de control de acceso lógico:** El grupo Keralty debe diseñar, implementar, gestionar, medir y mejorar de forma

continua los lineamientos de control de acceso y sus responsabilidades referentes a redes, sistemas, aplicaciones y usuarios.

V. **SIG-SI-CKE-PL06 Política corporativa de criptografía:** El grupo Keralty debe diseñar, implementar, gestionar, medir y mejorar de forma continua los controles relacionados con el cifrado, la gestión de llaves y claves de acceso.

VI. **SIG-SI-CKE-PL07 Política corporativa de seguridad física:** El grupo Keralty debe diseñar, implementar, gestionar, medir y mejorar de forma continua los controles de seguridad física para áreas seguras, información y equipos informáticos.

VII. **SIG-SI-CKE-PL08 Política corporativa de seguridad en las operaciones:** El grupo Keralty debe diseñar, implementar, gestionar, medir y mejorar de forma continua los controles necesarios para garantizar la seguridad de las operaciones, protección contra código malicioso, copias de respaldo, registro y seguimiento de operaciones, sistemas operativos, vulnerabilidades técnicas y auditorías de sistemas de información.

VIII. **SIG-SI-CKE-PL09 Política corporativa de seguridad de las comunicaciones:** El grupo Keralty debe diseñar, implementar, gestionar, medir y mejorar de forma continua los controles relacionados con la gestión de seguridad de redes y la transferencia de información a través de estas.

IX. **SIG-SI-CKE-PL10 Política corporativa de seguridad para la adquisición, desarrollo y mantenimiento de los sistemas de información:** El grupo Keralty debe diseñar, implementar, gestionar, medir y mejorar de forma continua los controles de seguridad referentes a los requerimientos iniciales de seguridad, proceso seguro de desarrollo, soporte y datos de prueba.

X. **SIG-SI-CKE-PL11 Política corporativa de seguridad en relación con proveedores:** El grupo Keralty debe diseñar, implementar, gestionar, medir y mejorar de forma continua los controles de seguridad de la información en el relacionamiento con proveedores y la gestión de servicios prestados por terceros.

XI. **SIG-SI-CKE-PL12 Política corporativa de gestión de incidentes de seguridad de la información:** El grupo Keralty debe diseñar, implementar, gestionar, medir y mejorar de forma continua los controles para garantizar la gestión de incidentes de seguridad de la información planificando, preparando, detectando e informando, evaluando y decidiendo, respondiendo aprendiendo y mejorando con base en lecciones aprendidas.

XII. **SIG-SI-CKE-PL13 Política corporativa de seguridad en la continuidad de negocios:** El grupo Keralty debe diseñar, implementar, gestionar, medir y mejorar de forma continua los controles necesarios para que la operación de continuidad del negocio cumpla con los lineamientos mínimos de seguridad de la información ante un desastre.

XIII. **SIG-SI-CKE-PL14 Política corporativa de cumplimiento regulatorio:** El grupo Keralty debe diseñar, implementar, gestionar, medir y mejorar de forma continua los controles requeridos para el cumplimiento de los requisitos legales, regulatorios y/o contractuales, así como las revisiones de seguridad de la información.

XIV. **SIG-SI-CKE-PL15 Política corporativa de ciberseguridad:** El grupo Keralty debe diseñar, implementar, gestionar, medir y mejorar de forma continua los controles requeridos para la protección de los sistemas de información e infraestructura tecnológica frente a amenazas que puedan afectar la confidencialidad, integridad y disponibilidad de la información y datos contenidos en estas.

XV. **SIG-SI-CKE-PL16 Política corporativa de riesgos de seguridad de la información:** El grupo Keralty debe diseñar, implementar, gestionar, medir y mejorar de forma continua la gestión de riesgos asociada a la seguridad de la información.

b) El grupo Keralty podrá desarrollar otras políticas específicas de seguridad de la información para dar respuesta a requerimientos legales, normativos, regulatorios y/o contractuales específicos de cada compañía y/o país.

7 COMUNICACIÓN, ACTUALIZACIÓN Y ACEPTACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

a) La política corporativa de seguridad de la información del grupo Keralty debe estar disponible y ser comunicada para todas las partes interesadas según sea apropiado y aplicable.

b) La política corporativa de seguridad de la información, así como las políticas de segundo nivel y/o específicas, deben ser actualizadas como mínimo cada año y/o cuando se generen cambios en los objetivos de negocio, regulación, normativa existente y/o en el contexto interno o externo del grupo Keralty.

c) Los funcionarios y/o terceros según aplique, deberán conocer, aceptar y aplicar las políticas corporativas de seguridad de la información una vez empiecen a desarrollar actividades en la compañía, cada vez que éstas sean actualizadas y/o en el marco de aceptación anual de las políticas del sistema de gestión de seguridad de la información del grupo Keralty.

8 APROBACIÓN DE LA POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN Y POLÍTICAS DE SEGUNDO NIVEL.

La estructura de aprobación de las políticas corporativas de seguridad de la información, se establece en la **SIG-SI-CKE-PL01-MA01 Matriz Revisión - Aprobación Políticas.**

9 MEDICIÓN DEL DESEMPEÑO.

Para medir la eficacia y la efectividad tanto del gobierno corporativo de seguridad de la información, así como del sistema de gestión de la seguridad, se han establecido los siguientes indicadores estratégicos y operativos de desempeño alineados con los objetivos corporativos de seguridad:

a. **SIG-SI-KPI-000**: Nivel de reducción de superficie de riesgo de seguridad de la información

b. **SIG-SI-KPI-001** : Índice cierre de Planes de Tratamiento de riesgos de seguridad
c. **SIG-SI-KPI-002 :** Nivel de cumplimiento en los requisitos en seguridad de la información.
d. **SIG-SI-KPI-003 :** Nivel de atención de incidentes de seguridad de la información
e. **SIG-SI-KPI-004 :** Nivel de apropiación cultural en seguridad de la información
f. **SIG-SI-KPI-005 :** Nivel de madurez modelo de Ciberresiliencia organizacional
g. **SIG-SI-KPI-006** : Índice de Cierre de Vulnerabilidades Críticas y Altas
h. **SIG-SI-KPI-007 :** Índice de cumplimiento en la Gestión integral de usuarios

A continuación, se observa la relación entre los objetivos de seguridad, las áreas de interés del gobierno de seguridad de la información y los indicadores de desempeño del Sistema de Gestión Corporativo de Seguridad de la Información del grupo Keralty:

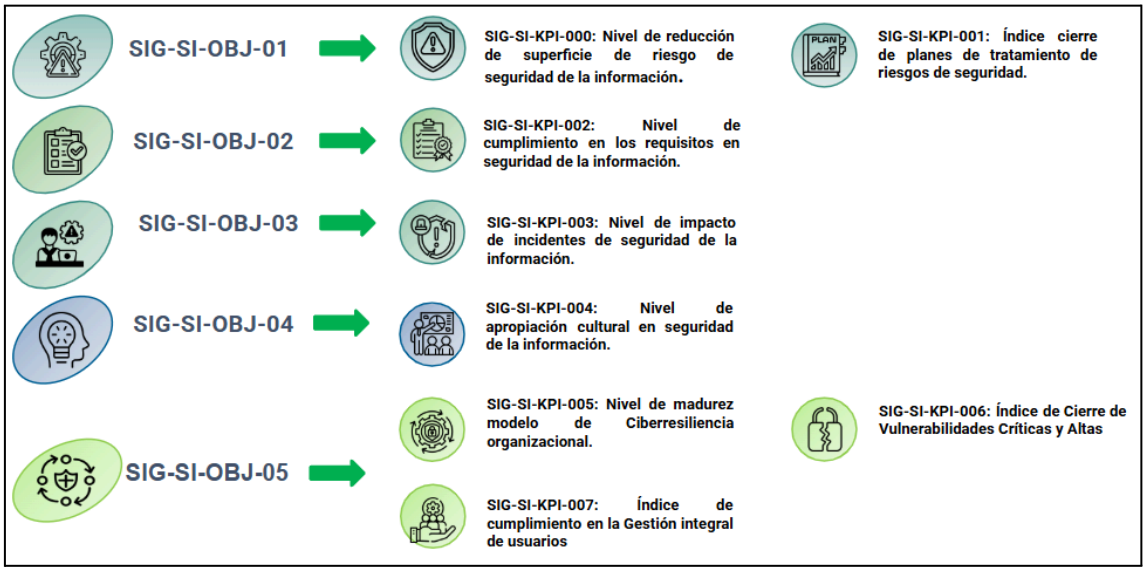

Figura 1 Relación entre objetivos y KPIs de seguridad de la información

El proceso para la definición, medición, seguimiento y análisis de los indicadores del Sistema de Gestión de Seguridad de la Información (SGSI), se encuentra definido en el documento **SIG-SI-CKE-PL01-PR03 Procedimiento para la gestión de indicadores del SGSI**

10 PILARES DEL GOBIERNO CORPORATIVO DE SEGURIDAD DE LA INFORMACIÓN DEL GRUPO KERALTY.

El gobierno corporativo de seguridad de la información del grupo Keralty, se ha diseñado y establecido bajo los siguientes pilares:

a) Predictivo: Permitiendo conocer de forma anticipada las amenazas a la seguridad de la información y su impacto en el negocio.

b) Personalizado: Diseñando e implementando controles de acuerdo con el tipo de activo, riesgo e información a proteger.

c) Participativo: Trabajando activamente con los grupos de interés en la protección de la información.

d) Preventivo: Monitoreando de forma proactiva y actuando de manera oportuna para reducir la superficie de riesgo.

e) Permanente: Asegurando constantemente los procesos, personas y tecnologías.

11 REFERENCIAS.

Para la elaboración del marco de políticas de primer y segundo nivel, lineamientos, procedimientos, estándares, guías e instructivos se han utilizado las siguientes normas y mejores prácticas de seguridad de la información y ciberseguridad.

- ISO/IEC 27001 Seguridad de la Información, Ciberseguridad y Protección de la Privacidad.
- ISO/IEC 27002 Estándar internacional - Seguridad de la Información, Ciberseguridad y Protección de la Privacidad.
- ISO/IEC 27005 Seguridad de la Información, Ciberseguridad y Protección de la Privacidad – Orientación sobre la gestión de los riesgos de seguridad de la información.
- ISO/IEC ISO 27035 Gestión de incidentes de seguridad de la información.
- ISO/IEC ISO 22301 Gestión de la Continuidad de Negocio.
- ISO/IEC ISO 31000 Gestión de riesgos.
- Marco de ciberseguridad NIST
- Modelo de controles CIS

12 CONTROL DE CAMBIOS

Tabla 1 Detalle del control documental

FECHA	CAMBIO	VERSIÓN
08/07/2021	Versión Inicial	1.0
18/03/2022	Se realiza ajustes a la codificación de las políticas de seguridad de la información	2.0
02/03/2023	Se realiza revisión de la política de seguridad de la información y ciberseguridad, respecto a los lineamientos definidos en el nuevo estándar ISO/IEC 27001:2022	3.0
28/02/2024	● Se omite la palabra Ciberseguridad del nombre de la "*SIG-SI-PL01 Política corporativa de seguridad de la información del Grupo Keralty*". ● Se incluye el numeral de definiciones en el documento. ● Se realizan ajustes de forma en la declaración de la política. ● Se ajusta la descripción de la política de gestión de incidentes de seguridad de la información. ● Se ajusta de forma el nombre de los objetivos de seguridad de la información. ● Se ajusta la versión para el estandar de ciberseguridad NIST 2.0. y para el Modelo de controles CIS V 8.0. ● Se ajusta la nomenclatura del documento, donde se incluyen las siglas CKE; C: País Colombia y KE: Compañía Keralty, de acuerdo a lo definido en el documento SIG-SI-CKE-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.	3.1
11/02/2025	● Se ajusta en la redacción el objetivo de la política.	3.2

	• Se agrega a la declaración de la política la palabra normativos y verificación. • Se agrega la palabra seguimiento al **SIG-SI-OBJ-01: Reducir la superficie de riesgo.** • Se agrega la palabra normativo al **SIG-SI-OBJ-02: Cumplir con los requisitos de seguridad de la información.** • Se agrega la palabra ciberseguridad al **SIG-SI-OBJ-04 cultura de protección de información.** • Se agrega la palabra negocio al **SIG-SI-OBJ-05: Mejorar las capacidades de Ciberresiliencia.** • Se agrega en el numeral 6 la palabra validación, normativa ISO/IEC 27035 y otras normativas aplicables. • Sobre el numeral 8 se enlaza el documento que contiene la aprobación de políticas corporativas y se elimina la imagen que asociaba el contenido. • Sobre el numeral 9 se realiza el cambio del código, nombre y cantidad de indicadores. • Se cambia la *Figura 1 Relación entre objetivos, KPIs de seguridad de la información y áreas de interés.* • Sobre el numeral 11 se retira sobre las normativas el año específico.	

13 FLUJO DE APROBACIÓN

Tabla 2 Detalle del flujo de aprobación

ELABORÓ	REVISÓ	APROBÓ
Nombre: Grupo de apoyo de la Gerencia Corporativa de Seguridad de la Información. **Cargo/Área/Proceso:** Gerencia Corporativa de Seguridad de la Información. **Fecha:** 11/02/2025	**Nombre:** Rene Alejandro Riachi. **Cargo/Área/Proceso:** Director de seguridad de la información. **Fecha:** 11/02/2025	**Nombre:** Alejandro Ramírez Romero **Cargo/Área/Proceso:** Gerente Corporativo de Seguridad de la Información (CISO). **Fecha:** 11/02/2025 **Nombre:** Integrantes de la Junta Directiva Matriz y Compañías del Grupo Keralty. **Cargo/Área/Proceso:** Junta Directiva Matriz y Compañías del Grupo Keralty. **Fecha:** 26/02/2025 **Nombre:** Santiago Thovar. **Cargo/Área/Proceso:** Vicepresidente Global de Sistemas de Información (CIO). **Fecha:** 07/04/2025