Política del Sistema Integrado de Gestión, Gestión del servicio y Seguridad de la información

KEYTRON S.A. es una compañía especializada en proporcionar soluciones a las necesidades empresariales, en el ámbito de las tecnologías de la información y las comunicaciones.

Nuestra principal misión es ofrecer a los clientes soluciones con la mayor calidad.

Con más de 35 años de experiencia, KEYTRON S.A. aporta su conocimiento en el desarrollo de actividades en las distintas áreas: Infraestructuras de Sistemas, Redes y Comunicaciones, Soluciones de Negocio, Formación Técnica Especializada, Asistencia Remota, Seguridad y Servicio de Soporte Técnico.

Con el objetivo de la mejora continua del sistema de gestión de calidad y medioambiente, de la gestión del servicio y de la seguridad de la información, hemos desarrollado un programa que pretende asegurar el óptimo resultado del trabajo diario.

La Política del Sistema Integrado de Gestión, Gestión del servicio y Seguridad de la información tiene por objeto definir y establecer los principios fundamentales y compromisos de Keytron, así como asegurar el óptimo resultado en la realización de todas nuestras actividades diarias en materia de **calidad del servicio, sostenibilidad, protección del medioambiente, gestión del servicio y seguridad de la información**.

Se establecerán periódicamente objetivos de mejora alineados con la presente política y cuyo alcance para la ISO 9001 e ISO 14001 es el "**Desarrollo y prestación de servicios de venta, instalación y mantenimiento de hardware y software para sistemas, networking, telecomunicaciones, ciberseguridad y redes de cableado**", para la ISO 27001 es el "**Desarrollo y prestación de servicios de venta, instalación y mantenimiento de hardware y software para sistemas, networking, telecomunicaciones, ciberseguridad y redes**" y para la ISO 20000 es **"El sistema de gestión de servicios de Keytron que soporta la provisión de los siguientes servicios: mantenimiento para las áreas de sistemas, networking, telecomunicaciones y ciberseguridad, para todos los clientes desde su ubicación en Madrid de acuerdo con el catálogo de servicios".**

Este planteamiento de la política del sistema de gestión integrado (SIG) se fundamenta en los siguientes principios:

- Cumplir con las normas ISO, con el fin de cumplir con los requisitos de nuestros clientes, así como las disposiciones legales y reglamentarias vigentes.
- Integrar la mejora continua en el sistema de gestión de la calidad y medioambiente, gestión de los servicios y seguridad de la información en la estrategia de la compañía.
- Lograr la implicación activa y responsable de los empleados, mediante la formación continuada y favorecer su participación en las líneas de investigación y desarrollo que nos han dado personalidad entre los Integradores de Redes.
- Asegurar que los requisitos de los servicios prestados, incluidos los acuerdos de nivel de servicio (SLA), acordados con los clientes, se cumplen y se mantienen.
- Garantizar la satisfacción del cliente cumpliendo los acuerdos de nivel de servicio fijados.
- Gestionar los riesgos para la organización que puedan surgir en la prestación de los servicios.
- Asegurar la confidencialidad, disponibilidad e integridad de la información de la organización.

- Formar y concienciar a todos los empleados en materia de seguridad de la información.
- Satisfacer las expectativas y requerimientos de las partes interesadas.
- Fomentar el trabajo en equipo, el compromiso, y la innovación.
- Ofrecer una atención personalizada y altamente especializada a nuestros clientes, de forma que nos adecuemos a sus necesidades y ofrecer la mejor solución posible, al menor coste y en el mejor plazo.
- Garantizar el compromiso de prevención de la contaminación y protección del medioambiente por medio de formación y el establecimiento de buenas prácticas ambientales.

I. Política de Seguridad de la Información

La Política de Seguridad de la Información identifica responsabilidades y establece principios y directrices para una protección apropiada y consistente de los servicios y activos de información gestionados por medio de las Tecnologías de la Información y de las Comunicaciones (TIC).

La seguridad, concebida como proceso integral, comprende todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información y las comunicaciones, y debe entenderse no como un producto, sino como un continuo proceso de adaptación y mejora, que debe ser controlado, gestionado y monitorizado, implantando la cultura de la seguridad en Keytron.

La Política de Seguridad de la Información pretende dar soporte al desarrollo, coordinación y racionalización de la normativa específica y a la actualización de los conceptos según la evolución de las TIC y de la legislación vinculante y alcanzar de esta forma un conjunto normativo equilibrado y completo.

II. Principios de la seguridad de la información

1. Principios básicos.

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

a) Alcance estratégico: La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de las iniciativas estratégicas de Keytron para conformar un todo coherente y eficaz.

b) Seguridad integral: La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual.

c) Gestión de Riesgos: El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad.

d) Proporcionalidad: El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.

e) Mejora continua: Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.

f) Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

2. Principios particulares

Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la Política de Seguridad de la Información y que inspiran las actuaciones de Keytron en dicha materia. Se establecen los siguientes:

a) Protección de datos de carácter personal: Keytron adoptará las medidas técnicas y organizativas destinadas a garantizar el nivel de seguridad exigido por la normativa vigente en relación con el tratamiento de los datos de carácter personal.

b) Gestión de activos de información: Los activos de información de Keytron se encontrarán inventariados y categorizados y estarán asociados a un responsable.

c) Seguridad ligada a las personas: Keytron implantará los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos.

d) Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.

e) Seguridad en la gestión de comunicaciones y operaciones: Keytron establecerá los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las TIC. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.

f) Control de acceso: Keytron limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.

g) Adquisición, desarrollo y mantenimiento de los sistemas de información: Keytron contemplará los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

h) Gestión de los incidentes de seguridad: Keytron implantará los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.

i) Gestión de la continuidad: Keytron implantará los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo con las necesidades de nivel de servicio de sus usuarios.

j) Cumplimiento: Keytron adoptará las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

III. Objetivos

La Dirección de KEYTRON, consciente del compromiso que contrae con sus clientes y con la seguridad, se ha basado en la ISO 27001 para la prestación de sus de servicios y operaciones, y perseguir por ello los siguientes objetivos:

a) Mantener al día la legislación aplicable y cumplir todos los requisitos legales y normativos, asociados a las actividades y aspectos que sean de obligado cumplimiento y también aquellos que suscribamos voluntariamente.

b) Asegurar que los servicios prestados y productos suministrados son seguros, fiables, cumplen con los pliegos de condiciones, normas e instrucciones aplicables, se adaptan a los requisitos y expectativas de sus clientes y mejoran continuamente.

c) Proteger la confidencialidad y disponibilidad de las comunicaciones de las personas que trabajan en la empresa, y la integridad de su información.

d) Conseguir y mantener el nivel de seguridad requerido para garantizar de forma adecuada la continuidad del negocio, incluso en situaciones adversas.

e) Asegurar la disponibilidad, confidencialidad e integridad de la información.

f) Implicar, motivar y comprometer al personal propio y aquel que trabaje en nombre de KEYTRON, con objeto de buscar su participación en la gestión, desarrollo y aplicación del sistema Seguridad de la Información implantado.

g) Establecer e implantar Planes de Formación y de Divulgación de Seguridad para mejorar la formación del personal.

h) Prevenir y tratar los incidentes de seguridad que puedan comprometer a la organización.

Es por ello por lo que desde Dirección se establece, dentro del programa de gestión, los planes y recursos necesarios para alcanzar los objetivos generales y la mejora continua. Esta política es revisada anualmente.

De igual modo la propia Dirección analiza los riesgos y vulnerabilidades en materia de seguridad que puedan afectar a KEYTRON, asumiendo y/o aceptando los mismos y proporcionando los medios necesarios para minimizarlos y asegura el buen funcionamiento del negocio.

Aspiramos a prestar un servicio de calidad, comprometido y flexible, de tal modo que nos convirtamos en partners o colaboradores de nuestros clientes en sus propios negocios.

Todo el personal perteneciente a KEYTRON tiene que cumplir la presente política, así como con el Sistema de Gestión, fundamentalmente las personas encargadas de la realización de las actividades comprendidas dentro del mimo, asumiendo las responsabilidades en materia de seguridad y sobre los activos de información.

34794880C EVA MARIA PRIETO (R: A78879285)

Firmado digitalmente por: 34794880C EVA MARIA PRIETO (R: A78879285)
ND: CN = 34794880C EVA MARIA PRIETO (R: A78879285) C = ES O = KEYTRON SA
Fecha: 2026.07.20 14:30:59 +01'00'

Eva Mª Prieto Martínez
Directora General
20/07/2026