



Imper.ia

POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN

SEPTIEMBRE 2025

POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN			
Imper.ia			
	Elaborado	Revisa	Aprueba
Nombre	Piero Soto	Bryan Rivera	Bryan Rivera
Cargo	Control & Compliance Auxiliar	Control & Compliance Coordinador	Control & Compliance Coordinador
Fecha	12/09/2025	15/09/2025	15/09/2025
Uso de Inf.	Interno		
Código	POL-SIG-001		

Documento propiedad de IMPERIA SOLUCIONES TECNOLÓGICAS S.R.L. prohibido su reproducción total o parcial sin autorización. El ejemplar impreso es copia NO controlada de la información documentada del Sistema de Gestión Integrado de IMPERIA SOLUCIONES TECNOLÓGICAS S.R.L.

2024 - TODOS LOS DERECHOS RESERVADOS

I. ASPECTOS GENERALES

OBJETIVO

El objetivo de la presente Política de Sistema Integrado de Gestión es establecer el compromiso de Imperia con la calidad, la seguridad de información, la gestión eficiente de servicios de TI y la continuidad del negocio. Busca garantizar que todos los servicios y soluciones brindados respondan a los requisitos de nuestros clientes, así como a las obligaciones legales, regulatorias y contractuales, promoviendo una cultura organizacional basada en la mejora continua, la ética profesional y la resiliencia operativa.

ALCANCE

La política es aplicable a todos los procesos, áreas, colaboradores y niveles jerárquicos de Imperia, incluyendo tanto las actividades internas como las operaciones relacionadas con clientes, proveedores y demás partes interesadas. Abarca la planificación, provisión, soporte y mejora de los servicios de ciberseguridad y tecnologías de la información que ofrece la organización, así como la protección de la información y la gestión de la continuidad del negocio. Su cumplimiento es obligatorio y constituye el marco de referencia para el establecimiento de objetivos, programas y acciones de mejora alineadas con las normas ISO implementadas.

MARCO DE REFERENCIA

- ISO/IEC 27001:2022
- ISO 9001:2015
- ISO 37001:2016
- ISO 22301:2019
- ISO 20000-1:2018

DOCUMENTOS RELACIONADOS

- NO APLICA

TÉRMINOS Y DEFINICIONES

- **Sistema Integrado de Gestión:** Conjunto de políticas, procesos y prácticas implementadas en la organización para gestionar de manera unificada la calidad, la seguridad de la información, la gestión de servicios TI y la continuidad del negocio, bajo los lineamientos de normas internacionales
- **Calidad:** Grado en el que un conjunto de características inherentes de un servicio cumple con los requisitos establecidos por los clientes, la organización y la normativa aplicable.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de los activos de información, incluyendo además otros aspectos como autenticidad, trazabilidad y fiabilidad.

- **Continuidad de Negocio:** Capacidad de la organización para seguir operando y restablecer sus servicios críticos dentro de plazos aceptables tras una interrupción significativa.
- **Gestión de Servicios TI:** Conjunto de prácticas y procesos destinados a planificar, diseñar, entregar, operar y mejorar los servicios tecnológicos, asegurando que estos aporten valor a los clientes y partes interesadas.
- **Mejora Continua:** Actividad recurrente orientada a incrementar la capacidad de la organización para cumplir los requisitos de manera más eficaz, eficiente y segura, a través de revisiones periódicas, acciones correctivas y preventivas.
- **Partes Interesadas:** Personas u organizaciones que pueden afectar, verse afectadas o percibirse como afectadas por las decisiones y actividades de la organización (clientes, colaboradores, proveedores, entes reguladores, entre otros).

II. RESPONSABILIDADES

Rol	Responsabilidad
Alta Dirección	Definir, aprobar y revisar periódicamente la política y los objetivos del SGI, asignar recursos necesarios, garantizar el cumplimiento legal, regulatorio y contractual; promover la cultura de mejora continua y liderazgo.
Control & Compliance	Asegurar la implementación, mantenimiento y mejora de SGI; supervisar el cumplimiento de los requisitos de calidad, seguridad de la información, continuidad de negocio y servicio TI, coordinar auditorías y revisiones.
Responsables de Área / Jefaturas	Implementar y hacer cumplir la política dentro de sus procesos, asegurar que los colaboradores bajo su cargo conozcan y apliquen los lineamientos, reportar incidentes y oportunidades de mejora.
Colaboradores	Cumplir con los lineamientos de la política y los procedimientos asociados, proteger la información y los activos, participar activamente en capacitaciones, reportar incidentes, riesgo o desviaciones.
Proveedores y Contratistas	Cumplir con los requisitos de calidad, seguridad y continuidad establecidos contractualmente, colaborar en la protección de la información y en la prestación segura de servicios.

III. REVISIÓN

La presente política será objeto de revisión periódica por parte de la Alta Dirección, con el propósito de asegurar su continua pertinencia, adecuación y eficacia frente a los cambios en el entorno organizacional, los requisitos de clientes, las obligaciones legales y regulatorias, así como los avances tecnológicos y de la industria. La revisión deberá realizarse, como mínimo, una vez al año o con mayor frecuencia cuando se presenten cambios significativos en la organización, tales como la incorporación de nuevos servicios, modificaciones en el marco normativo aplicable, resultados de auditorías internas o externas, o la ocurrencia de incidentes relevantes que afecten la calidad, seguridad, continuidad o prestación de los servicios.

El proceso de revisión incluirá la evaluación de resultados de indicadores de desempeño, hallazgos de auditorías, retroalimentación de clientes y partes interesadas, análisis de riesgos y oportunidades, así como el cumplimiento de objetivos estratégicos. Las conclusiones derivadas de este proceso serán documentadas en las actas de revisión por la dirección y, en caso necesario, se dispondrán ajustes en la política, los objetivos o en los planes de mejora del SGI. La política revisada será comunicada de manera oportuna a todos los colaboradores y partes interesadas pertinentes, garantizando su difusión, comprensión y aplicación en toda la organización.

IV. PRINCIPIOS DE POLÍTICA

La Política del Sistema Integrado de Gestión de Imperia se fundamenta en los siguientes principios:

- Enfoque al cliente: Todas las acciones de la organización se orientan a comprender y satisfacer las necesidades de los clientes, superando sus expectativas y brindando soluciones de valor.
- Gestión de riesgo: La toma de decisiones se apoya en la identificación, evaluación y tratamiento de riesgos y oportunidades, con el fin de garantizar la seguridad, continuidad y calidad de los servicios.
- Mejora continua: Se promueve un ciclo permanente de aprendizaje y optimización de procesos, servicios y controles, con el objetivo de incrementar la eficacia y eficiencia de SGI.
- Ética y transparencia: Todas las actividades se desarrollan con integridad, responsabilidad y cumplimiento de las normas legales y contractuales, fortaleciendo la confianza de clientes y partes interesadas.
- Cultura organizacional: Se fomenta la capacitación, sensibilización y participación activa de los colaboradores, reconociendo que son el principal recurso para alcanzar los objetivos estratégicos.
- Innovación y resiliencia: La organización impulsa soluciones innovadoras y mantiene su capacidad de adaptación frente a cambios o incidentes disruptivos que puedan impactar la continuidad del negocio.

V. DIFUSIÓN Y COMUNICACIÓN

La política será comunicada a todos los colaboradores, proveedores, contratistas y partes interesadas relevantes mediante distintos canales de información, garantizando su comprensión y aplicación. Entre los mecanismos de difusión se incluyen la publicación en la intranet corporativa, la distribución por correo electrónico, la inclusión en programas de inducción y capacitaciones, así como su exposición en lugares visibles dentro de las instalaciones de la empresa. Control & Compliance será responsable de asegurar que la política sea entendida en todos los niveles de la organización, promoviendo espacios de sensibilización y asegurando que los colaboradores conozcan sus responsabilidades en el cumplimiento de los lineamientos establecidos. Asimismo, se fomentará la retroalimentación de las partes interesadas como mecanismo de mejora.

VI. VIGENCIA Y CONTROL DOCUMENTARIO

La presente política entra en vigencia a partir de su aprobación por la Alta Dirección y permanecerá vigente hasta que se determine su actualización o reemplazo, en función de cambios estratégicos, normativos, contractuales o de contexto que lo requieran.

El documento forma parte del sistema de gestión documentario de Imperia y será identificado con un código, versión y fecha de aprobación, garantizando su trazabilidad y control. El área de Control & Compliance es responsable de custodiar la versión vigente, asegurando que se encuentre disponible para todos los colaboradores y partes interesadas, mientras que las versiones obsoletas serán archivadas y controladas para evitar su uso indebido.

VII. COMPROMISO

En Imperia Soluciones Tecnológicas reafirmamos nuestro compromiso con la excelencia en la gestión, la seguridad de la información, la gestión eficiente de servicios de TI y la continuidad del negocio, garantizando el cumplimiento de los requisitos de nuestros clientes, legales, regulatorios y contractuales.

Nuestros compromisos son:

- Satisfacer las necesidades de nuestros clientes, brindando soluciones confiables que respondan a sus expectativas de calidad, seguridad, disponibilidad, continuidad y confianza.
- Cumplir con los acuerdos contractuales, asegurando la entrega de servicios y soluciones conforme a lo establecido en los compromisos asumidos.
- Mejorar continuamente las competencias de nuestros colaboradores, fortaleciendo la cultura de calidad, seguridad, ética, continuidad y servicio mediante la capacitación y sensibilización permanente.
- Cumplir con los objetivos de calidad, seguridad, disponibilidad y continuidad, brindando servicios de calidad, protegiendo la información, gestionando incidentes de manera oportuna y garantizando la resiliencia organizacional frente a interrupciones
- Cumplir con los objetivos de seguridad de la información, salvaguardando la confidencialidad, integridad y disponibilidad de los activos de información frente a amenazas internas y externas.
- Garantizar la continuidad del negocio, estableciendo planes, estrategias y pruebas periódicas que aseguren la recuperación de servicios críticos y la minimización de impactos en caso de incidentes disruptivos.
- Mejorar continuamente la eficacia del Sistema de Gestión Integrado (SGI), a través de la gestión de riesgos, revisiones periódicas y acciones de mejora, en concordancia con las normas ISO 9001, ISO 27001, ISO 20000-1 e ISO 22301.

Lima, 12 de septiembre del 2025