CONTENIDO

1. DECLARACIÓN DE LA ALTA DIRECCIÓN 2
2. OBJETIVO GENERAL 2
3. ALCANCE 3
4. PRINCIPIOS RECTORES 3
5. REFERENCIAS 3
6. DIRECTRICES GENERALES 4
6.1 SISTEMA DE GESTIÓN DE LA CALIDAD (ISO 9001) 4
6.2 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (ISO 27001) 5
6.3 Sistema de Gestión de Información de Privacidad (ISO/IEC 27701) 8
6.4 SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO (ISO 22301) 9
6.5 SISTEMA DE GESTIÓN DE SERVICIOS DE TI (ISO 20000) 11
6.6 SISTEMA DE GESTIÓN ANTISOBORNO (ISO 37001) 12
6.7 SISTEMA DE GESTIÓN DE RIESGOS (ISO 31000) 13
6.8 SISTEMA DE GESTIÓN DE INTELIGENCIA ARTIFICIAL (ISO 42001) 14
6.9 SISTEMA DE GESTIÓN DE RESPONSABILIDAD SOCIAL (ESR) 16
7. COMPROMISO INSTITUCIONAL 17
8. CUMPLIMIENTO Y SEGUIMIENTO 17
9. MEJORA CONTINUA 18
10. CONTROL DE CAMBIOS 19

1. DECLARACIÓN DE LA ALTA DIRECCIÓN

En Toka, la Alta Dirección asume el compromiso de garantizar que todas las operaciones, procesos y servicios se desarrollen bajo los más altos estándares de **calidad, seguridad, integridad, responsabilidad, gestión de riesgos y sostenibilidad**, asegurando en todo momento el cumplimiento de la normativa nacional, internacional y contractual aplicable.

La presente política integra, en un único marco rector, los principios, objetivos y directrices de nuestros sistemas de gestión, alineados a los estándares **ISO 9001, ISO/IEC 27001, ISO 22301, ISO 37001, ISO/IEC 20000-1, ISO 31000**, **ISO/IEC 27701**, **ISO/IEC 42001**, al estándar **PCI DSS** y a los principios **ESR**, consolidando así un **modelo integral de gestión y cumplimiento** que promueve la **eficiencia, la transparencia, la protección de activos, la resiliencia operativa, la anticipación y mitigación de riesgos, así como la mejora continua**.

2. OBJETIVO GENERAL

Establecer un marco unificado que permita:

- Garantizar la calidad de productos y servicios mediante procesos eficientes, controlados y evaluados de forma continua.
- Proteger la información y los datos personales asegurando su confidencialidad, integridad y disponibilidad, aplicando controles basados en riesgos y en las mejores prácticas internacionales.
- Asegurar la continuidad operativa frente a contingencias, mediante planes de recuperación, gestión de riesgos y asignación eficiente de recursos.
- Gestionar los servicios de TI con criterios de disponibilidad, capacidad, rendimiento y seguridad, alineados a acuerdos de nivel de servicio.
- Mantener un entorno ético, libre de soborno, con controles que prevengan conductas ilícitas y promuevan la integridad corporativa.
- Integrar la sostenibilidad y la responsabilidad social en las decisiones estratégicas y operativas, considerando el impacto económico, social y ambiental.

3. ALCANCE

La presente política es aplicable a:

- Todas las áreas y niveles jerárquicos de Toka.
- Proveedores y terceros que intervengan en procesos, servicios o proyectos estratégicos.
- Todos los activos físicos, tecnológicos, humanos y financieros gestionados por Toka.
- Procesos críticos, estratégicos y de soporte identificados en los sistemas de gestión.

4. PRINCIPIOS RECTORES

- **Cumplimiento normativo**: Operar en estricto apego a la legislación aplicable y a los estándares internacionales adoptados.
- **Eficiencia operativa:** Diseñar, ejecutar y supervisar procesos robustos, controlados y medibles que reduzcan riesgos y optimicen recursos.
- **Gestión basada en riesgos:** Identificar, evaluar y mitigar amenazas que puedan afectar la operación, la seguridad o la reputación.
- **Seguridad y resiliencia:** Proteger activos críticos y asegurar la recuperación oportuna de procesos y servicios ante incidentes.
- **Innovación y mejora continua:** Incorporar soluciones tecnológicas y prácticas de gestión que incrementen la calidad y el valor entregado a clientes y partes interesadas.
- **Integridad y transparencia:** Mantener conductas éticas y sistemas de control que fortalezcan la confianza interna y externa.
- **Responsabilidad social y sostenibilidad:** Adoptar prácticas que promuevan la eficiencia energética, la reducción de impactos ambientales y el bienestar social.

5. REFERENCIAS

ISO 9001 – Sistemas de Gestión de la Calidad. Requisitos
ISO/IEC 27001 – Sistemas de Gestión de Seguridad de la Información. Requisitos
ISO/IEC 27701 – Sistema de gestión de información de privacidad (PIMS). Requisitos
Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), su Reglamento y Lineamientos
ISO 22301 – Sistemas de Gestión de la Continuidad del Negocio. Requisitos

ISO/IEC 20000-1 – Sistemas de Gestión de Servicios de Tecnologías de la Información. Requisitos.
ISO 37001 – Sistemas de Gestión Antisoborno. Requisitos
ISO 31000 - Sistemas de Gestión de Riesgos. Requisitos
ISO/IEC 42001 – Sistemas de Gestión de la Inteligencia Artificial. Requisitos
NMX-R-025-SCFI-2015, en Igualdad Laboral y No Discriminación
Responsabilidad Social Empresarial y Cambio Climático – Principios ESR y Adenda de Compromiso Climático.

6. DIRECTRICES GENERALES

6.1 SISTEMA DE GESTIÓN DE LA CALIDAD (ISO 9001)

En Toka, asumimos el compromiso de **mantener y mejorar la calidad** en todos nuestros productos y servicios, asegurando la **satisfacción de cada una de nuestras partes interesadas** y cumpliendo con los requisitos establecidos por clientes, autoridades y organismos certificadores.

Para lograrlo, hemos definido y documentado nuestros objetivos de calidad:

- Brindar un servicio de alta calidad generando la satisfacción de los clientes y usuarios.
- Implementar las herramientas innovadoras para mantener y mejorar la calidad de nuestros servicios.
- Incluir y reforzar la participación de los colaboradores en el SGC.
- Reforzar los procesos de la organización a través de la mejora continua.
- Tratar los riesgos propios de la actividad de la organización a través de controles preventivos, a efecto de mitigar el desvío al SGC.

Fomentando una **cultura organizacional orientada a la excelencia**, basada en principios de integridad, innovación, pasión, servicio y trabajo en equipo.

Este compromiso se ejecuta en estricto apego a:

- **Leyes, reglamentos y contratos aplicables**.
- Políticas, procedimientos, manuales y registros que forman parte del **Sistema de Gestión de la Calidad**.

El sistema debe **respetarse, mantenerse, cumplirse y mejorarse de manera continua**, asegurando su eficacia, adecuación y alineación con las mejores prácticas internacionales, para garantizar la **confianza, sostenibilidad y competitividad** de nuestra organización.

6.2 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (ISO 27001)

En Toka, asumimos el compromiso de proteger y gestionar de manera segura la información de nuestros clientes, usuarios, colaboradores, proveedores y de nuestras operaciones comerciales, asegurando su **confidencialidad, integridad, disponibilidad y autenticidad**, y cumpliendo con los requisitos establecidos por la normatividad aplicable, autoridades y organismos certificadores.

Para lograrlo, hemos definido y documentado nuestros objetivos de seguridad de la información:

Garantizar la Confidencialidad de la Información

- Asegurar que la información clasificada como privada y confidencial solo sea accesible para personal autorizado mediante la implementación de políticas de control de acceso, cifrado de datos y autenticación multifactor.

- Utilizar mecanismos de control de acceso basados en roles (RBAC) y cifrado AES-256 para proteger datos en tránsito y en reposo. Monitorear el acceso a la información para identificar y responder a posibles amenazas.

Mantener la Integridad de la Información

- Mantener la precisión y completitud de la información y sus procesos mediante la aplicación de controles para la gestión de cambios y la protección contra alteraciones no autorizadas.

- Implementar políticas de gestión de cambios que incluyan revisiones técnicas antes de cualquier modificación en sistemas críticos. Utilizar herramientas de integridad de archivos (FIM) para detectar modificaciones no autorizadas.

Garantizar la disponibilidad de la información

- Garantizar que la información esté disponible para los usuarios autorizados cuando la necesiten, mediante la implementación de estrategias de alta disponibilidad, planes de continuidad del negocio y gestión de incidentes.
- Asegurar la redundancia de los sistemas críticos y realizar pruebas periódicas de los planes de continuidad del negocio y recuperación ante desastres (DRP). Monitorear los sistemas en tiempo real para detectar y mitigar incidentes que puedan afectar la disponibilidad.

Protección contra amenazas internas y externas

- Implementar medidas proactivas y reactivas para proteger la información contra amenazas tanto internas como externas, a través de la gestión de vulnerabilidades, detección de amenazas y respuesta a incidentes.
- Realizar análisis de vulnerabilidades y pruebas de penetración trimestrales. Utilizar soluciones EDR (Endpoint Detection and Response).

Cumplimiento con normativas y regulaciones

- Cumplir con todas las normativas y regulaciones aplicables, incluyendo ISO 27001, ISO 22301, PCI DSS, y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).
- Realizar auditorías internas y externas anuales para asegurar el cumplimiento. Mantener actualizadas las políticas y procedimientos conforme a los cambios en el entorno regulatorio y normativo.

Educación y concientización en seguridad

- Fomentar una cultura de seguridad de la información en toda la organización, asegurando que todos los colaboradores comprendan sus responsabilidades y el impacto de sus acciones en la seguridad de la información.
- Implementar programas de capacitación y concientización en seguridad de la información anuales, enfocados en políticas de seguridad, buenas prácticas, y respuesta a incidentes.

Gestión de riesgos de seguridad de la información

- Identificar, evaluar y gestionar de manera proactiva los riesgos relacionados con la seguridad de la información para minimizar el impacto potencial en la organización.
- Realizar evaluaciones de riesgos semestrales y cada vez que se produzcan cambios significativos en la infraestructura o procesos de negocio. Establecer y monitorear un plan de tratamiento de riesgos con controles específicos para mitigar los riesgos identificados.

Protección de datos personales y sensibles

- Asegurar la protección de los datos personales y sensibles mediante la implementación de medidas técnicas y organizativas adecuadas, en cumplimiento con la LFPDPPP y otras regulaciones aplicables.
- Aplicar técnicas de minimización de datos, anonimización y cifrado para proteger la información personal. Establecer procedimientos de respuesta y notificación ante incidentes de datos personales.

Fomentando así una **cultura organizacional orientada a la seguridad, resiliencia, confianza y responsabilidad compartida**, basada en principios de integridad, innovación, servicio y mejora continua.

Este compromiso se ejecuta en estricto apego a:

- Leyes, reglamentos y contratos aplicables.
- Políticas, procedimientos, manuales y registros que forman parte del Sistema de Gestión de Seguridad de la Información.

El sistema debe respetarse, mantenerse, cumplirse y mejorarse de manera continua, asegurando su eficacia, adecuación y alineación con las mejores prácticas internacionales, para garantizar la **confianza, sostenibilidad y competitividad** de nuestra organización.

6.3 Sistema de Gestión de Información de Privacidad (ISO/IEC 27701)

La **Dirección General**, en su carácter de Alta Dirección del Sistema de Gestión de Información de Privacidad (PIMS), establece su compromiso con la privacidad y la protección de los datos personales a través de la **PO-S-NO-SG-01 Política Integral de Gestión y Cumplimiento**, la cual constituye el marco rector de los sistemas de gestión implementados por Toka y establece los principios y compromisos institucionales aplicables en materia de cumplimiento, seguridad de la información, protección de datos personales y mejora continua.

En congruencia con dicha Política Integral, Toka establece dentro de ésta la **Política de Privacidad aplicable al Sistema de Gestión de Información de Privacidad (PIMS)**, alineada con el propósito y la dirección estratégica de la organización y utilizada como marco de referencia para el establecimiento y seguimiento de los objetivos de privacidad.

Toka asume el compromiso de proteger la privacidad y los datos personales tratados en el desarrollo de sus actividades, productos y servicios, considerando las responsabilidades que le correspondan de acuerdo con su actuación como **Controlador o Procesador de PII**, según la naturaleza y características de cada actividad de tratamiento.
Toka se compromete a realizar el tratamiento de datos personales conforme a los principios de **licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad**, observando las finalidades determinadas o instruidas, según corresponda al rol que desempeñe en cada actividad de tratamiento.

Los datos personales serán obtenidos, utilizados, almacenados, compartidos, conservados y eliminados mediante mecanismos lícitos y bajo condiciones que permitan preservar su privacidad y protección durante su ciclo de vida, de conformidad con los **avisos de privacidad, contratos, instrucciones documentadas, políticas y procedimientos aplicables**, según corresponda.

Para el cumplimiento de este compromiso, Toka establece y mantiene medidas y controles **administrativos, técnicos y físicos** orientados a proteger los datos personales frente a pérdida, alteración, destrucción, uso, acceso, tratamiento o divulgación no autorizados, considerando los riesgos asociados a las actividades de tratamiento.

Asimismo, Toka se compromete a:

- cumplir los **requisitos legales, regulatorios, contractuales y organizacionales aplicables** en materia de privacidad y protección de datos personales;
- establecer y mantener un marco para la definición, seguimiento y evaluación de los **objetivos de privacidad**;
- respetar los derechos de los **Titulares o Principales de PII** y establecer mecanismos para su atención cuando corresponda;
- mantener identificadas y documentadas las actividades de tratamiento de datos personales y las responsabilidades de Toka como **Controlador o Procesador de PII**;
- gestionar los riesgos de privacidad y aplicar los controles que resulten necesarios de acuerdo con la naturaleza, contexto y finalidades del tratamiento;
- promover entre los colaboradores la **concientización, responsabilidad y cumplimiento** de sus obligaciones relacionadas con la privacidad y protección de datos personales;
- gestionar de manera adecuada la participación de **terceros, encargados, procesadores o subprocesadores** que intervengan en el tratamiento de datos personales, según corresponda; y
- **mantener y mejorar continuamente el Sistema de Gestión de Información de Privacidad**, asegurando su pertinencia, adecuación y eficacia**."**

La presente Política proporciona el marco para el establecimiento y revisión de los objetivos de privacidad de Toka y orienta la implementación, mantenimiento y mejora continua del PIMS.

La Política de Privacidad se mantiene como **información documentada** dentro de la **PO-S-NO-SG-01 Política Integral de Gestión y Cumplimiento**, es comunicada al interior de la organización y se encuentra disponible para las partes interesadas pertinentes, según corresponda.

6.4 SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO (ISO 22301)

En Toka, asumimos el compromiso de garantizar la **continuidad de nuestras operaciones críticas** aun en situaciones de interrupción o emergencia, asegurando la **confidencialidad, integridad y disponibilidad** de la información de clientes, usuarios, colaboradores y de nuestras propias actividades comerciales. Reconocemos que la capacidad de anticiparnos, resistir y recuperarnos frente a incidentes es un valor fundamental para la confianza y sostenibilidad de nuestra organización.

Para lograrlo, cumplimos con lo estipulado en las **leyes, reglamentos y contratos aplicables**, así como con los objetivos, políticas, manuales, procedimientos y demás elementos que integran nuestro Sistema de Gestión de Seguridad de la Información y Continuidad del Negocio, en estricto apego a la norma internacional **ISO 22301**.

Para asegurar la continuidad de nuestros servicios, fortalecer nuestra capacidad de respuesta y generar confianza en nuestras partes interesadas, hemos definido y documentado los siguientes objetivos:

- Garantizar la continuidad de los procesos críticos de la organización ante eventos disruptivos.
- Validar la efectividad de los planes de continuidad y recuperación mediante pruebas periódicas.
- Fortalecer la capacidad de respuesta y recuperación ante contingencias operativas o tecnológicas.
- Mantener actualizada la documentación del Sistema de Gestión de Continuidad del Negocio.
- Promover la cultura de continuidad del negocio en el personal involucrado en procesos críticos.
- Asegurar el cumplimiento de los requisitos normativos, regulatorios y contractuales aplicables.

Este compromiso se ejecuta en estricto apego a:

- Las **leyes, reglamentos y contratos aplicables** en materia de continuidad y seguridad de la información.
- Las **políticas, procedimientos, manuales y registros** que conforman el Sistema de Gestión de Continuidad del Negocio.

El sistema debe **respetarse, mantenerse, cumplirse y mejorarse de manera continua**, con la participación activa de todo el personal, garantizando así la **sostenibilidad, resiliencia y éxito de nuestras operaciones** y relaciones con las partes interesadas.

6.5 SISTEMA DE GESTIÓN DE SERVICIOS DE TI (ISO 20000)

En Toka, asumimos el compromiso de **gestionar los servicios de Tecnologías de la Información (TI)** con criterios de **disponibilidad, capacidad, rendimiento, seguridad y mejora continua**, asegurando que estos respalden de manera efectiva la operación del negocio y satisfagan las necesidades de clientes, usuarios y partes interesadas.

Reconocemos que la gestión eficiente de los servicios de TI es un pilar estratégico para garantizar la continuidad operativa, la innovación tecnológica y la calidad en la prestación de nuestros productos y servicios.

Para lograrlo, cumplimos con lo estipulado en las **leyes, regulaciones y contratos aplicables**, así como con los **objetivos, políticas, manuales, procedimientos y registros** que forman parte de nuestro Sistema de Gestión de Servicios de TI, en estricto apego a la norma internacional **ISO/IEC 20000-1**.

Con este sistema, hemos definido y documentado los siguientes objetivos:

- Asegurar el cumplimiento de los niveles de servicio acordados. (mediante el seguimiento y evaluación del desempeño de los servicios tecnológicos).
- Fortalecer la satisfacción de los usuarios y clientes (mediante la atención de sus necesidades y la mejora continua de los servicios tecnológicos).
- Mantener una capacidad tecnológica adecuada para atender la demanda actual y prevista de los servicios.
- Fortalecer la gestión y evaluación de proveedores tecnológicos, asegurando su contribución al cumplimiento de los requisitos de servicio.

Este compromiso se ejecuta en estricto apego a:

- Las **leyes, reglamentos y contratos aplicables** en materia de Tecnologías de la Información.
- Las **políticas, procedimientos, manuales y registros** que conforman el Sistema de Gestión de Servicios de TI de Toka.

El sistema debe **respetarse, cumplirse, mantenerse y mejorarse de manera continua**, asegurando su eficacia, adecuación y alineación con las **mejores prácticas**

internacionales, y garantizando la **confianza, sostenibilidad y competitividad** de nuestra organización.

6.6 SISTEMA DE GESTIÓN ANTISOBORNO (ISO 37001)

En Toka, asumimos el compromiso de **prevenir, detectar y sancionar cualquier forma de soborno**, asegurando que todas nuestras relaciones comerciales, ya sean con clientes, proveedores, autoridades o colaboradores, se desarrollen bajo principios de **integridad, legalidad y transparencia**.

Se prohíbe de manera estricta a todos los colaboradores, directos e indirectos, **ofrecer, solicitar, recibir o aceptar sobornos, pagos, regalos, comisiones ilegales o cualquier beneficio indebido**, con la finalidad de obtener o mantener de forma impropia contratos, negocios, aprobaciones gubernamentales, beneficios fiscales, regulatorios o cualquier otra ventaja empresarial.

Nuestras políticas se fundamentan en el **cumplimiento estricto de la legislación vigente nacional e internacional**, aplicando controles especialmente rigurosos en todas las transacciones y operaciones con entidades privadas o públicas, sin importar su carácter dependiente o independiente.

La información complementaria se encuentra descrita en la **Políticas de Antisoborno**, la cual establece directrices, responsabilidades y sanciones aplicables para garantizar el cumplimiento.

Para dar cumplimiento a este compromiso, hemos definido y documentado los siguientes objetivos del Sistema de Gestión Antisoborno (SGA):

- **Asegurar la eficacia de los controles antisoborno**, garantizando que sean adecuados en su diseño y funcionamiento, mediante el seguimiento de su ejecución y los resultados obtenidos.
- **Obtener información relevante** que permita mejorar la apreciación y gestión de los riesgos de soborno.
- **Detectar oportunamente cambios** en el contexto interno y externo, incluidos los criterios y niveles de riesgo, que requieran ajustes en los tratamientos y prioridades de control.

- **Verificar el cumplimiento y los resultados previstos**, asegurando que las medidas de mitigación de riesgo se apliquen correctamente.
- **Incluir y reforzar la participación de los colaboradores** en el Sistema de Gestión Antisoborno, promoviendo la concientización y el compromiso con la integridad organizacional.

Este compromiso se ejecuta en estricto apego a:

- Las **leyes y reglamentos aplicables en materia de antisoborno**.
- Las **políticas, procedimientos, manuales y registros** que forman parte del Sistema de Gestión Antisoborno de Toka.

El sistema debe **respetarse, mantenerse, cumplirse y mejorarse continuamente**, asegurando su eficacia, adecuación y alineación con las mejores prácticas internacionales, para fortalecer la **confianza, transparencia y reputación corporativa** de la organización.

6.7 SISTEMA DE GESTIÓN DE RIESGOS (ISO 31000)

En Toka, asumimos el compromiso de **gestionar los riesgos de manera proactiva, sistemática y eficaz**, asegurando que nuestras decisiones estratégicas y operativas se fundamenten en un análisis integral de amenazas, oportunidades e impactos potenciales. Reconocemos que una adecuada gestión de riesgos es esencial para la **sostenibilidad, resiliencia y éxito de la organización**.

Nuestro enfoque de gestión de riesgos se alinea con los principios, el marco y las directrices establecidos en la **norma ISO 31000**, promoviendo una cultura organizacional orientada a la **anticipación, prevención y mitigación de riesgos** en todas nuestras actividades.

Para lograrlo, cumplimos con lo estipulado en las **leyes, regulaciones y contratos aplicables**, así como con los **objetivos, políticas, manuales, procedimientos y registros** que conforman nuestro Sistema de Gestión Integral.

En este sistema, nos comprometemos a:

- **Identificar y evaluar los riesgos** estratégicos, operativos, financieros, tecnológicos, ambientales y de cumplimiento, considerando el contexto interno y externo de la organización.
- **Definir y aplicar planes de tratamiento de riesgos**, estableciendo controles y medidas de mitigación proporcionales al nivel de exposición identificado.
- **Integrar la gestión de riesgos en la toma de decisiones**, asegurando que todas las iniciativas, proyectos y procesos consideren sus impactos potenciales en la operación y en las partes interesadas.
- **Monitorear y revisar continuamente los riesgos**, actualizando el mapa de riesgos y ajustando los planes de tratamiento ante cambios en el entorno o en la organización.
- **Fomentar la participación activa de los colaboradores**, fortaleciendo la cultura de gestión de riesgos mediante programas de sensibilización y capacitación.
- **Mejorar de forma continua el sistema de gestión de riesgos**, incorporando las lecciones aprendidas, resultados de auditorías, indicadores de desempeño y buenas prácticas internacionales.

Este compromiso se ejecuta en estricto apego a:

- Las **leyes, reglamentos y normativas aplicables en materia de gestión de riesgos**.
- Las **políticas, procedimientos, manuales y registros** que conforman el Sistema de Gestión de Riesgos de Toka.

El sistema debe **respetarse, cumplirse, mantenerse y mejorarse continuamente**, garantizando su eficacia, adecuación y alineación con las **mejores prácticas internacionales**, y contribuyendo a la **confianza, sostenibilidad y resiliencia organizacional**.

6.8 SISTEMA DE GESTIÓN DE INTELIGENCIA ARTIFICIAL (ISO 42001)

En **Toka**, la política de Tecnología de la Información e Inteligencia Artificial establece un marco integral para garantizar que el desarrollo, implementación y operación de soluciones basadas en IA se realicen bajo principios de calidad, seguridad, ética, sostenibilidad y cumplimiento normativo. Esta política aplica a todas las áreas, procesos, activos y terceros involucrados, y se alinea con estándares internacionales como ISO

9001, ISO/IEC 27001, ISO 22301, ISO 37001, ISO/IEC 20000-1, ISO 31000, ISO/IEC 42001, PCI DSS y los principios ESR. Su objetivo es asegurar la eficiencia operativa, la protección de datos, la resiliencia ante riesgos, la mejora continua y la responsabilidad social en el uso de tecnologías de IA, consolidando un modelo de gestión que fortalece la confianza, la transparencia y la competitividad organizacional.

Con este sistema, nos comprometemos a:

- **Cumplimiento normativo integral:** Operar en estricto apego a leyes nacionales, internacionales, estándares ISO, regulaciones de protección de datos y compromisos contractuales aplicables al uso de tecnologías de IA.
- **Calidad y mejora continua:** Desarrollar y mantener soluciones de IA que cumplan con altos estándares de calidad, fomentando la innovación, la eficiencia operativa y la mejora continua en todos los procesos.
- **Seguridad de la información y protección de datos personales:** Implementar controles robustos para garantizar la confidencialidad, integridad y disponibilidad de la información procesada por sistemas de IA, conforme a la LFPDPPP y la norma ISO 27001.
- **Gestión de riesgos y resiliencia operativa:** Identificar, evaluar y mitigar los riesgos asociados al uso de IA, asegurando la continuidad del negocio mediante planes de recuperación y respuesta ante incidentes.
- **Ética, integridad y transparencia:** Promover el uso responsable y explicable de la IA, evitando sesgos, prácticas discriminatorias o decisiones automatizadas no justificadas, en línea con la norma ISO 37001.
- **Responsabilidad social y sostenibilidad:** Integrar criterios de sostenibilidad en el diseño y operación de soluciones de IA, considerando su impacto ambiental, social y económico, conforme a los principios ESR.
- **Participación y formación del personal:** Involucrar a los colaboradores en la implementación y mejora de los sistemas de IA, brindando capacitación continua y fomentando una cultura organizacional basada en la ética, el servicio y el trabajo en equipo.

En este sentido, Toka establece los siguientes objetivos:

- Garantizar el uso responsable y ético de las herramientas de IA
- Proteger la confidencialidad, integridad y disponibilidad de los datos utilizados con herramientas de IA
- Asegurar la transparencia, trazabilidad y explicabilidad de los resultados generados por IA
- Evaluar y gestionar los proveedores de herramientas de IA de terceros

6.9 SISTEMA DE GESTIÓN DE RESPONSABILIDAD SOCIAL (ESR)

En Toka, reafirmamos nuestro compromiso con la **sostenibilidad, la mejora continua y la responsabilidad social**, integrando el análisis del **impacto del cambio climático** en nuestro sistema de gestión como un factor clave para la toma de decisiones estratégicas y operativas.

Como Alta Dirección, reconocemos que el cambio climático representa un desafío global que requiere una **acción inmediata, constante y coordinada**, por lo que nos comprometemos a:

- **Integrar el análisis de riesgos y oportunidades climáticas** en la planificación, implementación y mejora del sistema de gestión, alineándolo con las mejores prácticas internacionales y normativas vigentes.
- **Evaluar y gestionar los impactos del cambio climático** sobre nuestras operaciones, la cadena de valor y las partes interesadas, fortaleciendo la capacidad de adaptación y mitigación de la organización.
- **Promover la eficiencia energética y la reducción de emisiones**, adoptando tecnologías sostenibles e innovadoras que minimicen el impacto ambiental.
- **Sensibilizar y capacitar a colaboradores y partes interesadas**, fomentando una cultura organizacional orientada a la sostenibilidad y al compromiso activo frente al cambio climático.
- **Garantizar la transparencia y rendición de cuentas**, mediante la medición, monitoreo y comunicación continua de los avances en materia de sostenibilidad y acción climática.

- **Colaborar con organismos reguladores, asociaciones industriales y actores clave**, impulsando iniciativas que refuercen la sostenibilidad, la innovación responsable y la resiliencia frente al cambio climático.

Este compromiso se ejecuta en estricto apego a:

- **Leyes, reglamentos y estándares aplicables** en materia ambiental y de responsabilidad social.
- **Políticas, procedimientos, manuales y registros** que forman parte del Sistema de Gestión de Responsabilidad Social y Cambio Climático de Toka.

El sistema debe **respetarse, cumplirse, mantenerse y mejorarse de manera continua**, garantizando que Toka continúe operando con **integridad, innovación, responsabilidad ambiental y social**, contribuyendo al desarrollo sostenible y al fortalecimiento de la resiliencia organizacional.

7. COMPROMISO INSTITUCIONAL

Nuestro **Sistema Integral de Gestión y Cumplimiento** debe respetarse, mantenerse, cumplirse y mejorarse de manera continua, con la participación activa de todo el personal y el liderazgo de la Alta Dirección. Este compromiso transversal garantiza la sostenibilidad de la organización, el éxito de nuestras operaciones y la solidez de nuestras relaciones con clientes, socios, autoridades y demás partes interesadas, consolidando un modelo de gestión único, eficiente y alineado con las mejores prácticas internacionales.

8. CUMPLIMIENTO Y SEGUIMIENTO

El **Sistema Integral de Gestión y Cumplimiento** de Toka establece mecanismos claros y estructurados para asegurar que todas las políticas, procedimientos y lineamientos definidos se apliquen de manera efectiva en toda la organización.

- **Aplicación obligatoria:** El cumplimiento de este sistema es de carácter obligatorio para todos los colaboradores de la organización, independientemente de su nivel jerárquico o función, así como para proveedores, contratistas y terceros que participen en procesos, proyectos o servicios estratégicos de Toka.

- **Auditorías internas y externas:** Toka coordinará la realización de auditorías periódicas, internas y externas, con el fin de evaluar la eficacia, adecuación y mejora continua del sistema, asegurando su alineación con los requisitos normativos, contractuales y las mejores prácticas internacionales.

- **Sanciones y medidas correctivas:** El incumplimiento de las disposiciones establecidas dará lugar a sanciones conforme a los reglamentos internos y a la legislación vigente, incluyendo la implementación de medidas correctivas y preventivas que fortalezcan el control, la transparencia y la confianza en los procesos.

El seguimiento al cumplimiento se llevará a cabo de manera sistemática, garantizando que los resultados obtenidos se analicen, comuniquen y traduzcan en oportunidades de **mejora continua**. De esta forma, se consolida un sistema integral robusto, capaz de responder a las necesidades de la organización, de sus partes interesadas y de su entorno regulatorio.

9. MEJORA CONTINUA

El **Sistema Integral de Gestión y Cumplimiento** de Toka se sustenta en el principio de la mejora continua, garantizando que sus políticas, procesos y controles evolucionen de manera constante para responder eficazmente a los retos estratégicos, operativos, regulatorios y tecnológicos de la organización.

- **Revisión anual de la política integral:** La Alta Dirección revisará de manera formal la política integral al menos una vez al año, con el objetivo de confirmar su pertinencia, eficacia y alineación con los valores corporativos, la estrategia institucional y las mejores prácticas internacionales.

- **Incorporación de resultados de auditorías, indicadores y análisis de riesgos:** Los hallazgos derivados de auditorías internas y externas, el comportamiento de los indicadores clave de desempeño (KPI) y los resultados de los análisis de riesgos serán considerados como insumos fundamentales para identificar áreas de mejora, priorizar acciones y fortalecer el sistema integral.

- **Inclusión de retroalimentación de clientes, proveedores y partes interesadas:** Se recopilarán y analizarán de manera sistemática las sugerencias, observaciones y

expectativas de clientes, proveedores, colaboradores y demás partes interesadas, integrándolas al proceso de mejora como un elemento clave para elevar la calidad, seguridad y sostenibilidad de los servicios y operaciones.

Este enfoque asegura que el sistema integral se **respete, mantenga, cumpla y perfeccione de manera continua**, consolidando la **resiliencia, competitividad y confianza** de Toka frente a las demandas del entorno y las necesidades de sus partes interesadas.

10. CONTROL DE CAMBIOS

Revisión	Fecha	Cambio	Motivo	Responsable	Aprobó
00	23/10/25	Se integra el sistema de gestión de la Inteligencia Artificial, en el numeral 6.7. Cambio de imagen institucional, incorporado una nueva clave que sustituye a **PO-SG-01 política integral de gestión y cumplimiento.**	Mejora	Sistemas de Gestión	Dirección General
01	12/02/26	Se agrega el concepto "Regalos" en el numeral **6.6. Sistema De Gestión Antisoborno (ISO 37001)** Adicional se hace un reajuste en su codificación	Mejora	Sistemas de gestión	Dirección General
02	03/08/26	Se actualizo el documento en el punto **6. DIRECTRICES GENERALES**	Mejora	Sistemas de gestión	Dirección General