Política de compliance

T-Systems ITC Iberia S.A.U.

Pública

Versión:	03.00	Válida desde:	30 de noviembre de 2020
Estatus:	Aprobada	Fecha de revisión:	17 de junio de 2025

INFORMACIÓN DEL DOCUMENTO

Autor/a	Revisado por	Aprobado por
T-Systems ITC Iberia S.A.U.	T-Systems ITC Iberia S.A.U.	Comité de Compliance Comité de Dirección (Board) Consejo de administración (Q2 2025)

Área de aplicación	Válida desde	Fecha aprobación
Todas las áreas	30.11.2020	30.11.2020

Versión	Última Revisión	Comentarios
01.00	30.11.2020	Redacción y publicación.
02.00	Mayo 2024	Actualización y ajustes varios.
03.00	17.06.2025	Revisión y actualización anual.

Departamentos implicados	Áreas implicadas	Referencia
Compliance	G&A	Todo el documento
Legal	G&A	Todo el documento

Contacto	Email
Compliance	Ask me! fmb.fmb-ts-ib-compliance-ask-me@t-systems.com

Resumen
Definición de la Política de compliance de T-Systems ITC Iberia S.A.U.

Lista de distribución y alcance
Personas trabajadoras de T-Systems ITC Iberia S.A.U. y su sucursal en Portugal.

ÍNDICE

1. OBJETO

La presente política de Compliance (en lo sucesivo, Política) tiene por objeto establecer los pilares sobre los que se asienta el Compliance Management System (en lo sucesivo, CMS) de T-Systems ITC Iberia, S.A.U. (en lo sucesivo, T-Systems) y presentar una visión general y estructural de su funcionamiento.

Así, la Política tiene cuatro objetivos:

- Informar sobre los objetivos y principios rectores del CMS, describiendo su funcionamiento y señalando sus líneas maestras en la prevención, detección y gestión de los riesgos de Compliance. En consecuencia, la normativa desarrollada en T-Systems en materia de compliance comparte unos objetivos y características comunes que se definen en la Política.
- Ayudar a las nuevas incorporaciones a conocer cuáles son las herramientas de las que dispone T-Systems en la lucha contra el delito y qué comportamiento espera T-Systems de todas ellas.
- Dar a conocer los principales rasgos característicos del modelo de prevención penal implementado en T-Systems y dar a conocer cómo a través del mismo la organización se compromete con el cumplimiento normativo.
- Evidenciar una cultura organizativa de respeto a la ley y la existencia de medidas razonables y proporcionadas para prevenir, detectar y gestionar los riesgos penales que afectan a la organización, todo ello conforme a lo exigido por el Código Penal, la UNE 19601 y la ISO 37001.

2. ÁMBITO SUBJETIVO

La Política aplica a las personas trabajadoras que presten servicios para T-Systems o para su sucursal en Portugal (en lo sucesivo, personas trabajadoras).

3. ÁMBITO TEMPORAL

La Política entrará en vigor el 30 de noviembre de 2020 y su vigencia será de 1 año, esto es, hasta el 30 de noviembre de 2021.

Llegado el plazo de vencimiento, la Política se prorrogará automáticamente por períodos de 1 año salvo decisión en contrario de T-Systems debidamente justificada.

4. MODIFICACIÓN DE LA POLÍTICA

T-Systems podrá modificar la Política en cualquier momento cuando lo considere necesario siempre que se justifique debidamente.

5. RESPONSABILIDAD

Las personas trabajadoras deben cumplir con la Política, así como con toda la normativa interna de T-Systems.

Las personas responsables de los diferentes departamentos deben divulgar el contenido de la Política entre el personal bajo su ámbito de responsabilidad y fomentar su cumplimiento.

Se prohíbe la comisión de cualquier infracción normativa.

Las personas trabajadoras deben identificar, analizar y evaluar los riesgos penales en su esfera de competencias y garantizar que se dispone de las medidas de Compliance necesarias para prevenirlos y gestionarlos.

Son ellas las que mejor conocen la actividad de sus respectivos campos y las que se encuentran en mejor posición para detectar los riesgos penales que pueden producirse, así como para valorar la idoneidad y efectividad de las medidas existentes para enfrentarse a ellos.

Es por ello que el personal responsable de la gestión operativa reporta periódicamente al Compliance Officer sobre los riesgos penales que afectan a su ámbito de competencia.

De igual forma, el personal responsable de la gestión operativa recibirá apoyo en el ejercicio de sus funciones en materia de Compliance por parte del Compliance Officer.

Las relaciones con socios de negocios - proveedores, consultores, socios de ventas, socios estratégicos - pueden entrañar diversos tipos de riesgos. La verificación de integridad incluye la comprobación de las partes contratantes potenciales con respecto a los riesgos relacionados con el cumplimiento y la reputación, así como los posibles conflictos de intereses.

6. OBJETIVO DEL CMS

El CMS persigue el mantenimiento y fomento de la cultura de cumplimiento normativo, así como la prevención, detección y gestión de aquellos riesgos respecto de los cuales T-Systems pudiera ser responsable penal, conforme al artículo 31 bis del Código Penal.

Quedan excluidos aquellos riesgos de Compliance que tengan su origen en otras obligaciones de Compliance distintas de lo establecido en el Código Penal y la normativa extrapenal a la que éste haga referencia para completar el tipo delictivo, sin perjuicio de que dichas obligaciones se encuentran correctamente atendidas bajo otros sistemas de cumplimiento implementados en T-Systems.

Anualmente, y a propuesta del Compliance Officer, se fijan los objetivos de Compliance para el ejercicio. Durante el año el Comité de Compliance revisará que esos objetivos se han llevado a cabo de forma óptima y el Compliance Officer informará al Consejo de administración mediante la remisión de la Memoria anual en materia de Corporate Compliance.

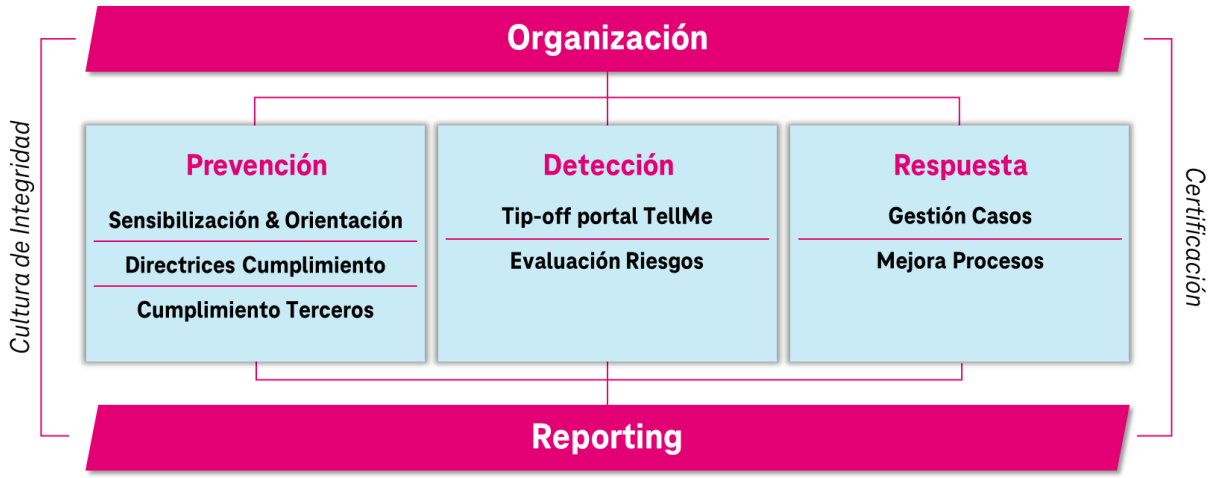
7. CMS

T-Systems dispone de un CMS compuesto por un elenco de normativas de obligado cumplimiento que pretende asegurar que todas las empresas del Grupo Deutsche Telekom (en lo sucesivo, Grupo) cumplen con el Código de Conducta.

Ese CMS internacional está auditado y certificado de acuerdo con la norma IDW AssS 980, estándar de referencia en Alemania para la auditoría de modelos de cumplimiento.

T-Systems ha desarrollado e implementando diversas políticas, procedimientos e instrucciones de operación que complementan la normativa promovida por el Grupo. Parte de este cuerpo normativo se encuentra dirigido a la prevención, detección y gestión de los riesgos penales.

A continuación, se relaciona la estructura del CMS tanto a nivel internacional como local:



8. ESTRUCTURA DE CONTROL

8.1. Consejo de administración

El Consejo de Administración de T-Systems (en lo sucesivo, Consejo) es el principal impulsor del CMS, actuando con liderazgo en el compromiso con los valores de la empresa y promoviendo una cultura de cumplimiento con la ley, la normativa interna y los compromisos voluntarios adquiridos por la organización.

Asimismo, el Consejo es el responsable último del mantenimiento y mejora del CMS y debe garantizar que el mismo dispone de los recursos financieros, materiales y humanos adecuados y suficientes para su funcionamiento eficaz. Para ello, ha delegado las funciones del mantenimiento y mejora del CMS en el Comité de Compliance.

El Consejo debe de mostrar liderazgo y compromiso con el CMS implementado y con las normas que se derivan de éste y garantizar que las exigencias que emanan del CMS se incorporan en los procesos y procedimientos operativos de T-Systems.

8.2. Comité de Compliance

El Comité de Compliance de T-Systems (en lo sucesivo, Comité) es el órgano responsable de garantizar el correcto funcionamiento y el cumplimiento de las normas y pautas establecidas en materia de cumplimiento, tiene atribuciones en materia de cumplimiento normativo y prevención y control de los riesgos penales, y dispone de poderes autónomos de iniciativa y control en materia de Corporate Compliance.

El Comité está formado por los responsables de las áreas más relevantes y se reúne con carácter trimestral.

Las principales funciones del Comité son:

- Comunicar novedades de cumplimiento, posibles riesgos y medidas acordadas en unidades propias u operativas con las que estén en contacto.
- Promover el desarrollo y establecimiento de una cultura corporativa adecuada.
- Escalar, si es necesario, problemas de cumplimiento al Consejo.

El Comité está compuesto por las personas que en cada momento ostenten los siguientes cargos:

- VP Sales.
- VP Cloud Infrastructure & Security.
- VP Digital Solutions.
- VP Global Delivery Center.
- Head of TDU.
- Head of Procurement.
- Head of Corporate Finance.
- Head of Controlling.
- Head of Health Safety & Wellbeing.
- Head of Legal.
- Head of Marketing & Communication.
- Compliance Officer.
- Equipo Compliance.

8.3. Compliance Officer

El Compliance Officer es la posición clave para establecer el CMS y mantenerlo a largo plazo.

Realiza las funciones de Compliance en el día a día, junto a su equipo y es responsable de la implementación y desarrollo metodológico continúo de todos los procesos del CMS, basados en el diseño internacional y plazos establecidos.

Las funciones asignadas al Compliance Officer son las siguientes:

- Establecer el CMS y mantenerlo a largo plazo.
- Ejecutar las diferentes actividades de Compliance y mantener el contacto con las unidades internas requeridas de T-Systems.
- Informar de las correspondientes actividades de manera regular al Consejo o cualquier organismo supervisor necesario.
- Dirigir las reuniones periódicas del Comité como máximo responsable.
- Permanecer en contacto regular con la organización Group Compliance Management (en lo sucesivo, GCM) del Grupo.
- En caso necesario, ponerse en contacto con las personas que forman parte del Consejo.

El Compliance Officer es asimismo responsable del sistema interno de información de T-Systems, dando cumplimiento a la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

8.4. Equipo de compliance

El equipo compliance es responsable de la ejecución de las diferentes actividades de cumplimiento para garantizar la efectividad del CMS.

Recibe la asignación de tareas del Compliance Officer y le informa de los resultados.

8.5. Departamento de compliance

El Departamento de compliance está formado por el Compliance Officer y el equipo de compliance, que preparan los correspondientes informes para el Comité y el GCM.

Asimismo, con una frecuencia mínima anual, el Compliance Officer reporta al Consejo las actuaciones realizadas, los resultados en materia de Compliance, la Memoria anual del año anterior y el plan de medidas para el año en curso.

Todo ello sin perjuicio de que el Compliance Officer pueda reportar, de forma ad-hoc, al Consejo o al GCM en todos los casos en los que se considere necesario.

9. GESTIÓN DE RIESGOS

La identificación de los riesgos penales constituye la base para la implementación del CMS y su análisis y evaluación permite a la organización asignar recursos y establecer procesos idóneos para gestionar los riesgos identificados.

Por ello, el CMS establece que la gestión de riesgos debe contemplar la identificación, el análisis, la evaluación, el control, la monitorización y la revisión de los riesgos penales.

Para lo anterior, T-Systems dispone de dos herramientas de gestión de riesgos: Internal Control System (en lo sucesivo, ICS) y Compliance Risk Assessment (en lo sucesivo, CRA).

Ambos procesos se realizan periódicamente en todo el Grupo mediante un procedimiento estandarizado que permite la identificación de las actividades en cuyo ámbito pueden ser cometidos los delitos.

T-Systems analiza los riesgos de cumplimiento para cada unidad evaluándolos y estableciendo prioridades, así como planes de acción con medidas de mitigación de dichos riesgos.

9.1. ICS

La plataforma ICS aglutina riesgos operacionales y recoge el listado de riesgos por departamentos, así como el elemento de control diseñado conforme al riesgo a cubrir.

Incluye también la persona responsable del control.

9.2. CRA

La plataforma CRA se usa para el control y gestión de los riesgos de Compliance.

Esta plataforma es objeto de revisión periódica actualizándose la clasificación y valoración de los riesgos.

Así, a través del mapa de riesgos, se identifican potenciales riesgos que obedecen tanto a conductas indebidas por parte de T-Systems como por parte del personal y, por tanto, en perjuicio de T-Systems. En cada ejercicio se detectan los riesgos más relevantes y se establece un plan de acción para la mitigación de los mismos.

La metodología utilizada en CRA recoge los siguientes pasos para el proceso de identificación y evaluación:

- Determinación del contexto y alcance.
- Identificación de riesgos.
- Análisis de riesgos.
- Evaluación de riesgos.
- Control de riesgos.
- Monitorización.
- Comunicación y formación.
- Revisión del sistema.

9.3. Sistema de gestión antisoborno

T-Systems dispone de un Sistema de gestión antisoborno (en lo sucesivo, SdGA) que ayuda a la organización a prevenir y detectar riesgos en materia de soborno incluido en el mapa de riesgos del CRA, así como a cumplir con las leyes antisoborno y los compromisos voluntarios aplicables a sus actividades.

El SdGA es parte del CMS y los controles son ejecutados, mantenidos, revisados y mejorados de acuerdo con los requerimientos de la norma internacional ISO 37001.

10. PROTOCOLOS Y PROCEDIMIENTOS

El programa de cumplimiento tiene su máximo exponente en el Código de Conducta, que proporciona el marco de referencia y define la conducta empresarial de toda la plantilla del Grupo, basada en la integridad y cumplimiento de las leyes y reglamentos con respecto a clientes, socios de negocio, accionistas y público en general.

En relación con el establecimiento de protocolos y procedimientos, T-Systems dispone de una cantidad elevada de políticas y procedimientos que concretan la conducta esperada por toda la plantilla en cuestiones diversas como el uso de los equipos corporativos, la seguridad de la información, la confidencialidad, la protección de los datos personales, normas en materia de prevención de la corrupción, defensa de la competencia, así como otras normas internas de aplicación en los distintos departamentos.

Con respecto al cumplimiento de los derechos humanos, el Board of Management de Deutsche Telekom aprobó en 2023 un nuevo Código de Derechos Humanos aplicable a todo el Grupo.

A través de dicho documento, el Grupo se compromete a respetar los derechos humanos y las preocupaciones medioambientales al implementar un proceso de due diligence mundial, así como a cumplir con los requisitos legales, las directrices y declaración de principios de la Organización para la cooperación y el desarrollo económico, la Organización Internacional del trabajo o el Pacto Mundial de las Naciones Unidas.

En caso de detectarse la necesidad de implementar una nueva norma o política, bien desde el Grupo o desde T-Systems, se inicia un proceso de desarrollo en el cual intervienen todos los departamentos implicados en su posterior aplicación. Una vez aprobada, se publica y comunica a toda la compañía y, especialmente, a aquellas personas que por su cargo o función deban aplicarla.

11. CONTROLES

Los controles implementados en T-Systems tienen diferentes características, en atención a su objetivo (prevención, detección o corrección) y sus rasgos de funcionamiento (soft[1] o hard[2], automáticos[3] o manuales[4]).

El CMS de T-Systems incluye controles con diferentes características para dotar al mismo de una mayor robustez.

11.1. Prevención

La mayor parte de los controles implementados se dirigen a prevenir la comisión de incumplimientos.

Son normas, procesos y procedimientos cuyo fin es establecer pautas de conducta que reduzcan significativamente la materialización del riesgo penal.

Los controles preventivos son comunicados a la plantilla afectada y, a su vez, se imparte formación para asegurar su total comprensión y aceptación, garantizando de esta forma su mayor efectividad preventiva.

Así mismo, T-Systems dirige controles de prevención, no solo frente a las personas trabajadoras, sino sobre sus socios de negocio.

11.2. Detección

Si bien la mayoría de los controles de Compliance se dirigen a prevenir la comisión de delitos, otros pretenden detectar la comisión de incumplimientos por elusión fraudulenta de los controles de prevención existentes.

11.3. Corrección

Una vez detectado o comunicado un incumplimiento, T-Systems cuenta con el Protocolo de gestión, investigación y respuesta de incumplimientos para investigarlo y, en determinados casos, informar de forma inmediata al Consejo, a fin de comprobar la realidad del incumplimiento y, de ser así, responder con las sanciones adecuadas que pueden alcanzar la denuncia ante las autoridades competentes.

A su vez, la gestión operativa competente y el Comité analizan y comprueban cómo ha podido producirse el incumplimiento y qué controles de prevención y/o detección deben ser modificados o añadidos para que no vuelva a producirse en el futuro.

En caso de ser necesario, se valora la posibilidad de realizar cambios en el CMS.

Implementados los nuevos controles, éstos se revisan periódicamente para comprobar que están funcionando correctamente y que, en efecto, el nuevo control corrige suficientemente la disconformidad producida anteriormente para que ésta no se vuelva a materializar.

[1] Controles soft: aquellos que de una forma más intangible dirigen la conducta de las personas trabajadoras, estableciendo pautas de comportamiento que deben ser seguidas por los integrantes de la organización.

[2] Controles hard: son tangibles y objetivos, por ejemplo, aquellas obligaciones de aprobación por más de una persona, autorizaciones, verificaciones o revisiones de resultados de una actividad.

[3] Controles automáticos: actúan sin necesidad de ser ejecutados por ningún miembro de la organización.

[4] Controles manuales: requieren para actuar de forma efectiva que la persona responsable del control ejecute el tipo de acción previsto en el control.

12. CANALES DE COMUNICACIÓN

T-Systems dispone de los siguientes canales gestionados por el equipo de Compliance.

12.1. Ask me!

Con la finalidad de aclarar dudas respecto a la conducta adecuada en materia de Compliance, se dispone del buzón **Ask me**! (FMB TS IB COMPLIANCE ASK ME), en el cual se reciben consultas relevantes sobre el cumplimiento en relación a dudas sobre políticas y normativas.

12.2. Tell me!

Para avisar sobre la existencia de irregularidades o bien en caso de sospecha de que se hayan infringido las normas, la ley o los reglamentos y directrices internos existe el buzón **Tell me**! (FMB TS IB COMPLIANCE TELL ME).

Para garantizar el eficaz funcionamiento del buzón se dispone del Protocolo de gestión, investigación y respuesta de comunicaciones en el cual se regula el uso del buzón y la posterior investigación de los hechos.

Todas las personas trabajadoras tienen la obligación de notificar a sus superiores o a través del buzón de avisos **Tell me**! de inmediato y sin demora, cualquier irregularidad que tenga como potencial resultado un perjuicio económico o de cualquier otra naturaleza para T-Systems, sus personas trabajadoras, o las personas que forman parte del Consejo, así como cualquier incumplimiento de la ley o de la normativa interna.

También está a disposición el **portal del Grupo Tell me!** que permite reportar de forma anónima. Este portal está gestionado por una empresa externa, en contacto con el equipo de Compliance del Grupo.

Todas las comunicaciones recibidas que presenten una mínima verosimilitud serán investigadas con la autonomía e independencia necesaria para ello y, en todo caso, garantizando los derechos del comunicante y de las personas sobre los que versan los hechos objeto de comunicación.

Los datos serán tratados con el más estricto cumplimiento de la legislación sobre protección de datos de carácter personal, garantizando, en todo momento, que la identidad de las personas que hagan uso del mismo será tratada con la máxima confidencialidad y que no existirá ningún tipo de represalia contra ellos.

De demostrarse la veracidad del incumplimiento, la persona infractora se enfrentará a medidas disciplinarias que, conforme al Estatuto de los Trabajadores y el Convenio Colectivo aplicable, pueden llegar al despido disciplinario.

T-Systems anima a todas las personas trabajadoras a actuar de forma proactiva, comunicando cualquier potencial incumplimiento.

12.3. Intranet

La cultura corporativa de T-Systems está marcada por la integridad, la ética y la responsabilidad personal y se fundamenta en los Guiding Principles que representan los valores y convicciones del Grupo y proporcionan la orientación necesaria sobre cómo alcanzar los objetivos empresariales.

El Código de Conducta y otros contenidos relevantes en materia de Compliance están publicados en la intranet. El Código de Conducta es también de acceso desde el blog corporativo y en el área específica de responsabilidad corporativa. Todas las normas internas corporativas están disponibles en la intranet o en la aplicación de repositorio de políticas.

T-Systems incluye los Guiding Principles y la Política en el Pack Onboarding que reciben las nuevas personas trabajadoras en el momento de su incorporación.

Con carácter general, T-Systems comunica todas las políticas, procedimientos y procesos implementados a todas aquellas personas trabajadoras, socios de negocio o terceras personas ajenos a la compañía sobre los que éstas incluyan alguna obligación de observancia.

12.4. Formación

T-Systems imparte formaciones en materia de ética, cumplimiento normativo y respeto a las normas de conducta internas a toda la plantilla, poniendo especial foco a las nuevas incorporaciones con perfil de riesgo.

El formato puede ser presencial o e-learning.

13. ARCHIVO

La aplicación de los controles de Compliance genera una documentación cuyo archivo es primordial, tanto para la efectividad del CMS, como para disponer de evidencias del funcionamiento del concreto control.

Así, es obligatorio documentar y conservar todas las operaciones, controles y demás actuaciones desarrolladas por la gestión operativa y por el Comité.