Política Integrada de los Sistemas de Gestión

Política de Calidad

Con el fin de conseguir sus objetivos estratégicos, ofrecer un servicio eficaz y para conseguir la satisfacción de sus clientes la Dirección de Atos ha fomentado e implantado un Sistema de Gestión de la Calidad (SGC) conforme con la norma UNE-EN-ISO 9001:2015, complementado con otros modelos y prácticas como, las normas UNE-ISO/IEC 20000-1:2018 o ISO/IEC 33000. Esta política es conforme con la política de Calidad de Atos Global definida en el documento "Atos Quality Policy", publicada a través de la Intranet de la compañía.

En Atos, la Calidad por Diseño y la Mejora Continua de la Calidad son el valor que brindamos a nuestros clientes. La calidad está integrada en los productos, soluciones y servicios que ofrecemos, y nos esforzamos por mejorar la experiencia del Cliente en todo lo que hacemos.

La mejora de la calidad impulsa la experiencia del cliente.

Estamos comprometidos a brindar el más alto nivel de servicio a nuestros clientes y a desarrollar relaciones basadas en la responsabilidad y la confianza.
Escuchamos a nuestros clientes, actuamos en consecuencia para mejorar continuamente nuestros procesos y ofertas, y proponemos soluciones eficientes para satisfacer sus necesidades de negocio.
Nos esforzamos por la ejecución impecable de nuestros compromisos y por la facilidad para hacer negocios con nosotros.

La mejora de la calidad se incluye en cada paso de nuestros procesos. Nos comparamos con los mejores para lograr una excelencia operativa

Nos enfocamos en hechos y apuntamos a cero defectos en la entrega de servicios de principio a fin. Incluimos toda la cadena de suministro en este enfoque.
Involucramos a nuestros equipos y socios en el diseño de soluciones innovadoras para entregar valor a nuestros clientes y dirigimos nuestros centros de servicio y entrega basándonos en el pensamiento "lean".

La mejora de la calidad está integrada en nuestras prácticas de gestión y en los planes de desarrollo de nuestras personas trabajadoras.

Capacitamos y formamos a nuestras personas trabajadoras para facilitarles que hagan primeras entregas correctas y sean contribuyentes activos a la transformación digital del negocio de nuestros clientes.
Gestionamos nuestros equipos con objetivos específicos para garantizar nuestra rentabilidad y continuidad, la mejora continua de la calidad, con comportamientos profesionales de confianza, responsabilidad y proactividad como base de las relaciones con los clientes.
A través de nuestros programas de compromiso de las personas trabajadoras, nos esforzamos por hacer de Atos un gran lugar para trabajar, atrayendo y motivando a personas talentosas que dan lo mejor de sí y entregan valor a nuestros clientes.

Implementamos esta política a través del seguimiento y mejora continua del Sistema de Gestión Integrado de Atos (AIMS), y a la vez, con un pleno cumplimiento de las obligaciones contractuales y regulaciones locales.

Política de Seguridad de la Información

Atos es líder mundial en servicios digitales y como tal ha de proteger tanto sus activos como los activos de sus clientes (1) ante cualquier amenaza, ya sea interna o externa, deliberada o accidental.

Perímetro:

La Política de Seguridad de Atos aplica a todo el personal del Grupo Atos, así como a los contratistas y al personal temporal, y a cualquier tipo de información (2) en todos sus formatos (electrónico, papel, conversación, etc.), tanto la que es propiedad de la compañía, como la que, procedente de clientes, Atos utiliza o mantiene en custodia.

En este contexto, la seguridad física y la prevención de riesgos laborales (personas y sedes) son esenciales y contribuyen a reforzar la protección de los activos de Atos y de sus clientes.

Sistema de Gestión de la Seguridad de Atos:

Para apoyar la consecución de su objetivo de seguridad en la protección de la información, Atos ha elaborado e implantado un Sistema de Gestión de Seguridad de la Información (SGSI) acorde con la norma ISO 27001 que es el estándar de aplicación obligatoria para todas las actividades de negocio de Atos a nivel mundial.

Para apoyar la implementación local de las políticas globales de forma acorde con la legislación local, se generarán estándares, procedimientos y guías locales. Estas reglas locales definen el mínimo nivel de cumplimiento sobre seguridad para todo el personal (Nota ENS 1) (Nota ENS 2).

Más información en Atos SharePoint: Atos Group Security Home Page (3).

Objetivos:

La política de seguridad de la compañía tiene como objeto asegurar que:

La información se proteja frente a cualquier acceso no autorizado, notablemente mediante "autenticación de dos factores" para todas las aplicaciones internas.
Se asegure la Confidencialidad de la información, se mantenga la Integridad de la información y se preserve la Disponibilidad de la información.
Se aplique una clasificación de los activos de información (Nota ENS 3).
Se lleve a cabo una gestión de riesgos de seguridad y privacidad por parte de los propietarios de los activos junto con los "security officers" y los "data protection officers" para identificar y evaluar los riesgos de seguridad y privacidad de forma que se tomen

las medidas preventivas adecuadas. Esto se realizará de acuerdo con la normativa aplicable. (EU GDPR)
Las vulnerabilidades de seguridad de tipo medio o alto que se identifiquen sean remediadas por los grupos de operaciones a la mayor brevedad.
Se cumplan los requisitos legales y reglamentarios vigentes del país, así como los requisitos contractuales sobre seguridad.
Todo el personal reciba una formación periódica sobre seguridad.

Roles y responsabilidades:

La responsabilidad de establecer la organización de seguridad y protección en Atos es del Head of Group Security. Es directamente responsable de actualizar esta política de seguridad y los objetivos de seguridad anuales, así como de proporcionar asesoramiento y asistencia en su implementación. Para esta misión, se basa en la organización de seguridad (Group Security).

Todo el personal de Atos es la primera línea de defensa en materia de seguridad, su colaboración y cumplimiento de las políticas de seguridad es esencial y obligatorio.

Todas las personas responsables directas de cada persona trabajadora (Internamente calificados como "line managers") son directamente responsables de la implementación de los Controles de Seguridad definidos por las Políticas en sus áreas de negocio y del cumplimiento por parte del personal a su cargo.

El personal debe comunicar inmediatamente cualquier incumplimiento o incidente de seguridad a su "security officer" correspondiente o a su "line mánager" (4), sin perjuicio que puede comunicar también mediante el Sistema Interno de Información de Atos local o Global (en adelante, "Sistema de Información") o en otras palabras llamado Canal de denuncias: https://atos.integrityline.com.

En el caso de que se produzca un incidente de seguridad, se deben tomar medidas inmediatas para reducir el riesgo y el impacto del daño para Atos y nuestros clientes.

Las excepciones a las Políticas de Seguridad requieren la aprobación del Head of Group Security.

Todo el personal es responsable de cumplir las Políticas de Seguridad de Atos y las normas, procedimientos y guías relacionados, incluyendo los principios denominados "Aide.Mémoire". Su incumplimiento puede dar lugar a medidas disciplinarias, que pueden incluir la finalización del contrato de trabajo.

Los procesos y procedimientos vigentes, publicados en el portal de conocimiento de la compañía se ajustarán en cada momento a la legislación y reglamentación vigente, siendo de aplicación a este Sistema de Gestión, en particular (sin limitación):

Legislación europea y española:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas (RGPD)
- Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos.
- Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18 —Comisaria de Protección de Datos vs Facebook Irlanda y Maximillian Schrems Adoptada el 23 de julio de 2020.
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales
- Ley 11/2022, de 28 de junio, General de Telecomunicaciones
- 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.
- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Ley 17/2001, de 7 de diciembre, de Marcas.
- Ley 24/2015, de 24 de julio, de Patentes (en vigor desde el 1 de abril de 2017)
- Real Decreto 316/2017, de 31 de marzo, por el que se aprueba el Reglamento para la ejecución de la Ley 24/2015, de 24 de julio, de Patentes
- Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de Información y Comercio Electrónico.
- Ley 59/2003, de 19 de diciembre, de firma electrónica
- Ley 1/2019, de 20 de febrero, de Secretos Empresariales
- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión Europea.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto – ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.
- Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.
- Real Decreto-Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones (ámbito específico).
- Lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4)- AEPD.
- Lista de tipos de tratamiento de datos que no requieren evaluación de impacto relativa a la protección de datos (art 35.5)- AEPD.
- Circular 1/2023, de 26 de junio, sobre la aplicación del artículo 66.1.b) de la Ley 11/2022, de 28 de junio, General de Telecomunicaciones (AEPD).

- Informes, guías e instrucciones de la AEPD, CNPD, CEPD, Decisiones de la Comisión Europea sobre adecuación a la legislación de protección de datos de países u organizaciones.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 8/2011, de 28 de abril, por el que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).
- Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero ("DORA").
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).

La Política, así como los objetivos anuales en materia de seguridad se revisan al menos una vez al año, publicando en la intranet de Atos las últimas versiones.

(1) Según los compromisos contractuales.
(2) Ver "Atos Information Security Policy".
(3) Puede consultarse también la comunidad de Teams/Yammer "Espacio de protección de datos en Iberia".
(4) En incidentes relacionados con tratamiento de datos personales, se deberá informar también a su DPO.

Notas ENS: Para dar cumplimiento a los requisitos establecidos por el Esquema Nacional de Seguridad (ENS), en los servicios proporcionados por Atos que están incluidos en el alcance de dicha normativa (declarados en el portal https://gobernanza.ccn-cert.cni.es/certificados) se aplica adicionalmente*:*

(Nota ENS 1): En el documento local "Adaptaciones del SGSI para dar cumplimiento al ENS" se detallan las adaptaciones adicionales que se realizan sobre el Sistema de Gestión de la Seguridad de la Información de Atos, donde se incluyen aspectos como:
Identificación de los responsables de la información y de los servicios dentro del alcance y sus atribuciones
Requisitos mínimos de seguridad aplicables, en caso de no estar recogidos previamente en la política de seguridad global de Atos "Atos Information Security Policy"
Criterios para determinar los niveles de seguridad requeridos
Medidas de seguridad aplicables
Enlaces al detalle de la Normativa correspondiente (Real Decreto, Instrucciones Técnicas de Seguridad, Guías)

(Nota ENS 2) La coordinación general y resolución de conflictos se establece en el marco de las reuniones periódicas de Seguimiento de Seguridad, Protección de Datos y Calidad con la Dirección, así como en el Comité Ejecutivo Extendido con periodicidad mensual.

(Nota ENS 3) Además de Confidencialidad, Integridad y Disponibilidad, se consideran dos dimensiones adicionales: Trazabilidad y Autenticidad

Política Medioambiental

La Dirección de Atos considera que es su deber compatibilizar las dimensiones económicas, sociales y medioambientales de manera armónica y equilibrada en un modelo de desarrollo sostenible buscando la excelencia. Por ello se compromete a minimizar el impacto ambiental de sus actividades en toda la cadena de valor en todo el mundo; desde las operaciones de producción y las instalaciones de negocio hasta la logística y los productos y servicios, considerando la perspectiva del ciclo de vida completo.

Atos ha implantado un Sistema de Gestión Ambiental conforme con la norma UNE-EN ISO 14001:2015.

La Política Medioambiental está totalmente alineada con las ambiciones estratégicas del Grupo y con el programa de Responsabilidad Social Corporativa (RSC) del Grupo. Las principales ambiciones y compromisos de la Política Ambiental y del Programa Ambiental son compatibles con el contexto y las orientaciones estratégicas del Grupo.

El Grupo ha adoptado principios fundamentales o directrices genéricas de alto nivel para controlar y reducir su huella medioambiental. Todas las entidades y operaciones de Atos deberán cumplir con estos principios en los países donde operan.

Atos adopta los siguientes 8 principios de alto nivel para lograr sus compromisos:

1.Cumplimiento medioambiental. Identificar, supervisar y cumplir con todas las leyes, regulaciones y normas medioambientales vigentes y los requisitos de las partes interesadas, relacionados con los aspectos medioambientales de nuestras operaciones.
2. Retos Globales. Abordar nuestros retos medioambientales materiales [(2)] (emisiones de GEI, adaptación al cambio climático, uso de recursos, residuos y economía circular) fijando objetivos de reducción y creando resiliencia frente a los riesgos medioambientales.
3.Retos Locales específicos. Identificar y abordar los riesgos y retos medioambientales específicos de cada centro o país (productos, logística, gestión de residuos, reciclado, recuperación, agua, etc.).
4.Iniciativas y planes de acción. Poner en marcha y supervisar iniciativas, planes de acción y formación para todos los empleados del Grupo con el fin de avanzar de forma constante en aspectos y retos clave.
5.Protección del medioambiente. Prevenir la contaminación y proteger el medioambiente mediante un Sistema de Gestión Medioambiental para todo el Grupo y la Certificación ISO 14001 en los principales centros con procedimientos y controles adecuados.
6.Cadena de valor de Atos. Garantizar que los proveedores, contratistas y socios clave respetan esta Política y contribuyen activamente a nuestro progreso medioambiental mediante prácticas de contratación responsables, objetivos medioambientales y evaluaciones de resultados.
7.Control del rendimiento. Realizar un seguimiento anual de los indicadores clave de rendimiento y del avance respecto a los objetivos globales y locales, e impulsar la mejora continua mediante revisiones auditadas por terceros.
8.Sensibilización y Comunicación. Implicar a las partes interesadas mediante una comunicación transparente [e] informes alineados con las principales normas como CSRD, TCFD, GRI y EU Taxonomy.

Esta política es conforme con la política Medioambiental Global definida en el documento "Environmental Policy", publicada en SharePoint y en la web de Atos.

Política de Seguridad y Salud en el Trabajo

La Política de Atos establece el compromiso de proporcionar condiciones de trabajo seguras y saludables, con el fin de elevar los niveles de seguridad, salud y bienestar de la propia organización mediante la integración en la cultura de empresa de la prevención de lesiones y deterioro de la salud de las personas trabajadoras.
Esta política es esencial para garantizar que todas las personas trabajadoras desarrollan su actividad en un entorno, que no solo cumple con la normativa de seguridad, sino que también promueve una cultura de prevención y cuidado continuo, incorporando acciones específicas para la prevención de lesiones y mitigación del deterioro de la salud.
Con la finalidad de desarrollar una gestión eficaz e integrada de la seguridad y salud de sus personas trabajadoras, tanto propios como de empresas colaboradoras, la Dirección de Atos tiene definidos los principios rectores de su política, los cuales se aplican en todos los procesos y niveles de la empresa, así como de implementación de acciones correctivas y preventivas, para garantizar estos entornos de trabajo seguros y saludables.

De acuerdo con estos principios, Atos asume los siguientes compromisos:
Cumplir todos los requisitos legales y cualquier otros vigentes en materia de Prevención de Riesgos Laborales que sean de aplicación, así como, llevar a cabo de forma voluntaria acciones que garanticen la mejora de la promoción de la salud y bienestar de las personas trabajadoras.

Realizar una identificación de peligros potenciales y evaluar los riesgos asociados, estableciendo estrategias y procedimientos para prevenir lesiones y deterioros de la salud siempre teniendo en cuenta un análisis de género para que los puestos se adapten a las características particulares de las personas que los ocupan.

Desarrollar programas de formación y capacitación que aseguren que todas las personas trabajadoras estén adecuadamente informadas y capacitadas en prácticas de trabajo seguras.

Fomentar la participación dentro del Sistema de Gestión de Prevención de Riesgos Laborales de todas las personas trabajadoras que pertenecen a Atos, para incluir sus sugerencias de mejora, con objeto de fomentar la mejora continua y garantizar que las personas trabajadoras y sus representantes sean parte de la toma de decisiones en materia de Seguridad y Salud en el trabajo.

Garantizar la difusión tanto de la política de Prevención de Riesgos Laborales como del Plan de Prevención dentro de la organización mediante los canales corporativos de comunicación, así como poner a disposición la política de PRL a cualquier parte interesada (empresas colaboradoras, clientes etc…), a través de la web corporativa.

La revisión de esta política se llevará a cabo de forma periódica, con la finalidad de garantizar que sigue siendo adecuada a la actividad de Atos y con el propósito de trabajar bajo la mejora continua.

El éxito de la implementación de esta política requiere el pleno compromiso de todas las personas trabajadoras en todos los niveles de la organización

Política de Gestión de Servicio IT

El Sistema de gestión de servicios de IT es aplicable a todas las entidades de Atos y está alineado con los requisitos UNE-ISO/IEC 20000-1:2018 de acuerdo con las necesidades del negocio. La política se aplica a las ubicaciones incluidas en la Certificación de sitios múltiples AIMS, como se especifica en el certificado UNE-ISO/IEC 20000-1:2018.

El propósito de la Política de Servicios de Atos es buscar el mayor nivel de calidad y eficiencia operativa en los servicios que presta y, por lo tanto, obtener un mayor grado de satisfacción del cliente poniendo a las personas primero, como la base de la forma de trabajo y de su estrategia de crecimiento.

De acuerdo con la visión de Atos "Ser un socio confiable para las empresas que crean su firma del futuro y el mejor lugar para trabajar para empleados y nuevos talentos" que se resume a continuación:

Ser un socio de confianza para nuestros clientes.
Ser reconocido como un jugador global de TI con una amplia cartera de servicios.
Innovar continuamente para que nuestros clientes puedan progresar y tener éxito.
Ser el mejor lugar para trabajar. Aspiramos a atraer y nutrir jóvenes talentos para crear un ambiente de trabajo dinámico y diverso. Se motiva a nuestros ingenieros a su desarrollo y crecimiento.
Liderar con el ejemplo.

En línea con esta visión, Atos ha decidido que el cumplimiento de la norma UNE-ISO/IEC 20000-1:2018 es vital para brindar nuestros servicios.

Esto implica contar con un sistema integral de gestión de servicios (SMS) para dirigir y controlar todas las actividades de gestión de servicios. En el caso de Atos el SMS se llama ITSMS (IT Service Management System).

Junto con el Sistema de Gestión de Calidad (QMS), el sistema de Seguridad de la información (SGSI) y el Sistema de Gestión Ambiental (EMS), el Sistema de Gestión del Servicio (ITSMS), constituye el Sistema Integrado de Gestión de Atos (AIMS).

La misión del ITSMS es impulsar proactivamente, junto con todas las unidades de ingeniería y entrega, la mejora continua, la eficiencia, la satisfacción del cliente y la integración en la entrega de los servicios a nuestros clientes.

La Visión para lograr esta Misión es:

Impulsamos un cambio (de cultura), de la "complacencia" a la "organización que se guía a sí misma y se mejora a sí misma" centrada en los resultados.
Impulsamos una organización donde los procesos se valoran como vehículos para conducir resultados de forma controlada y predecible.
Nos esforzamos por lograr mejoras basadas en la "lógica de madurez", es decir, resolver problemas de forma controlada y gradual para garantizar la sostenibilidad.
Nos esforzamos por la optimización, los resultados y el valor de extremo a extremo en todos los silos (práctica, GEO, organización del cliente) a través de un sistema de gestión integrado.

Los Objetivos de ITSMS son:

Mejora continua en la prestación de servicios, calidad y seguridad.
Cumplimiento de los requisitos del servicio.
Consecución de los objetivos de gestión del servicio.
Excelencia operativa.
Reducción de riesgos.
Satisfacción de los clientes.

La prestación de servicios está alineada con las necesidades del cliente, los objetivos de la empresa y los compromisos acordados. Los servicios se entregan de acuerdo con la calidad definida en los servicios, procesos y contratos estándar del cliente. Existe una cartera de servicios y está en continuo desarrollo y mantenimiento como base para la prestación de servicios y las actividades de Gestión de servicios. Se definen SLA y KPIs a diferentes niveles de la organización, así como otros específicos relacionados con contratos y acuerdos con clientes.

Para gestionar de forma eficaz todos los servicios, existe un enfoque de gestión de servicios basado en procesos. Todos los procesos requeridos se definen, comunican y mejoran en función de las necesidades de negocio y los comentarios de las partes interesadas involucradas. Todos los roles y responsabilidades de la gestión de servicios (incluidos los roles como parte de ITSMS) están claramente definidos. Existen procesos y políticas específicos, según se considere necesario.

Los servicios y los procesos de gestión de servicios se mejoran continuamente. Los comentarios de las partes interesadas se utilizan para la mejora del portfolio, agregando valor y calidad a los servicios. Se mejora la gestión de los servicios entregados en base al monitoreo continuo del desempeño de los procesos, sus indicadores y efectividad. Las mejoras se registran y gestionan para maximizar su aportación.

La dirección de Atos está comprometida con esta política y su implementación. Proporcionan en su ámbito específico de responsabilidad, los recursos necesarios para implementar y mejorar la Gestión del Servicio, cumplir con todos los requisitos legales y contractuales y aumentar la satisfacción de nuestros clientes.

Es responsabilidad de todo el personal aplicable, así como de los contratistas y el personal temporal, adherirse a la Política de gestión del servicio y los procesos, instrucciones de trabajo y pautas relacionados. Los planes de gestión de servicios específicos de la unidad

de negocio describen los detalles para garantizar que la creación, implementación, operación, mantenimiento y mejora continua del sistema de gestión de servicios (ITSMS) de Atos se logren de acuerdo con la política y los requisitos de la norma UNE-ISO/IEC 20000-1:2018.