



Manual del sistema de gestión de la seguridad de la información

Manual del Sistema de Gestión de la Seguridad de la información

MAN-SI-01

Contenido

1 OBJETIVO Y CAMPO DE APLICACIÓN.....	3
Generalidades.....	3
Aplicación.....	3
2 TÉRMINOS Y DEFINICIONES	4
3 NORMAS PARA CONSULTAS	5
4 CONTEXTO DE LA ORGANIZACIÓN	7
Generalidades.....	7
Partes Interesadas, sus necesidades y expectativas.	8
Alcance del Sistema de Gestión de Seguridad de la Información.	10
CONTEXTO. ANÁLISIS DE LA SITUACIÓN DE PARTIDA	11
5 LIDERAZGO	13
Liderazgo y Compromiso.....	13
Política.....	13
Roles, responsabilidades y Autoridades en la organización	13
6 PLANIFICACIÓN	15
7 SOPORTE.....	18
Entrenamiento, Concienciación y Competencia.....	18
Comunicación	18
Información Documentada	18
8 OPERACIÓN	21
Apreciación de Riesgos de Seguridad de la Información	21
Tratamiento de riesgos de seguridad de la información.....	21
9 EVALUACIÓN DEL DESEMPEÑO	22
Auditorías Internas del SGSI.....	22
Revisión del SGSI por la Dirección	22
Salidas de la Revisión.....	23
10 MEJORA.....	24
Mejora Continua	24
No conformidad y Acción Correctiva.....	24

1 OBJETIVO Y CAMPO DE APLICACIÓN

Generalidades

El presente Manual de Gestión de la Seguridad de la Información (en adelante, MGSi), tiene por objeto establecer y desarrollar los requisitos para implementar, operar, monitorear, revisar, mantener y mejorar el Sistema de Gestión de la Seguridad de la Información para los servicios prestados por AL TEN, relativos a las áreas establecidas en el alcance del SGSi de la Política de Seguridad y en el presente manual.

Aplicación

Este MGSi desarrolla todos los requisitos establecidos en la Norma UNE-EN ISO/IEC 27001:2014 y el Esquema Nacional de Seguridad, para establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información dentro del contexto de la organización.

2 TÉRMINOS Y DEFINICIONES

Para el propósito de este documento son aplicables los términos y definiciones establecidos en las Normas:

- UNE-ISO/IEC 27001:2022 “Sistemas de Gestión de la Seguridad de la Información. Requisitos”
- UNE-ISO/IEC 31000:2018 “Gestión del Riesgo. Principios y Directrices”

3 NORMAS PARA CONSULTAS

El sistema de Gestión de Seguridad de la Información descrito en este Manual se ha desarrollado siguiendo las directrices y requisitos establecidos en los documentos citados a continuación:

- UNE-ISO/IEC 27001:2022 “Sistemas de Gestión de la Seguridad de la Información. Requisitos”
- UNE-ISO/IEC 27002:2022 “Código de prácticas para los controles de seguridad de la información”
- UNE-ISO/IEC 31000:2018 “Gestión del Riesgo. Principios y Directrices”
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

Para la implementación de nuestro SGSI se ha tenido en consideración de, al menos, las siguientes disposiciones:

- Reglamento (UE) 2016/679. RGPD – Reglamento General de Protección de Datos
- Reglamento (UE) 2016/679 del Parlamento Europeo, de 27 de abril de 2016, por el que se aprueba el Reglamento General de Protección de Datos.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- 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 59/2003, de 19 de diciembre, de firma electrónica
- Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Así como las siguientes disposiciones normativas que aplican en Portugal:

- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).
- Decreto-Lei n.º 7/2004 - Serviços da sociedade de informação, em especial do comércio electrónico (Transpõe a directiva 2000/31/CE).

- Lei n.º 51/2011 - Altera a Lei das Comunicações Electrónicas, que estabelece o regime jurídico aplicável às redes e serviços conexos e define as competências da Autoridade Reguladora Nacional neste domínio, transpondo as Directivas n.os 2002/19/CE, 2002/20/CE, 2002/21/CE, 2002/22/CE e 2009/140/CE.
- Lei n.º 58/2019 - Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
- Lei n.º 46/2012 - Transpõe a Diretiva n.º 2009/136/CE, na parte que altera a Diretiva n.º 2002/58/CE, do Parlamento Europeu e do Conselho, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, procedendo à primeira alteração à Lei n.º 41/2004, de 18 de agosto, e à segunda alteração ao Decreto -Lei n.º 7/2004, de 7 de janeiro.

Una empresa consultora externa de AL TEN proporciona soporte para la consulta de la legislación que afecta al desarrollo de las actividades en el campo de la seguridad de la información y se desarrolla mediante el *PO-ALT-18-Identificación-y-evaluación-requisitos-legales*.

4 CONTEXTO DE LA ORGANIZACIÓN

Generalidades

MARCO ORGANIZATIVO

ALLEN es una multinacional creada en Francia en el año 1988 que está presente en toda Europa.

ALLEN es el líder en Europa en Consultoría e Ingeniería Tecnológica en Altas Tecnologías.

Sus clientes son las grandes empresas de los sectores de Servicios, telecomunicaciones e industrial, y su oferta se compone de realización de estudios y proyectos abiertos, de gestión de proyectos, de proyectos con equipos y de proyectos cerrados, tanto en el ámbito del sector público como privado.

En España, La sede central de ALLEN tiene su domicilio en Madrid, en c/ Vía de los poblados 3, edificio 5, planta 2, y en Portugal TECH ALLEN PORTUGAL LDA. Rui Júlio Dinis 242.

Edificio Les Palaces, Escritório 208 4050-318 PORTO contando con más centros a lo largo del territorio nacional. Todos los centros tienen una estructura similar con:

- Área Técnica
- Área Comercial
- Áreas de Soporte (Soporte Global en áreas de Compras, Formación, RR.HH. y Selección)

ALLEN está gestionada por cuatro direcciones generales que gestionan el área de Ingeniería, TIC y AAPP, Financiero y RRHH. De estas direcciones dependen un nivel intermedio de *management* compuesto por senior managers para el área comercial y gerentes de área para los departamentos transversales.

Con presencia en grandes empresas de diferentes sectores centra sus principales actividades en las áreas de:

- Soluciones e-Business
- Desarrollo de software
- Tecnología de Sistemas
- Integración y Gestión de procesos
- Business Intelligence
- Risk Management
- Prestaciones de personal con un perfil tecnológico de alto nivel, para participar en proyectos de ingeniería e I+D en los sectores y grandes empresas del país
- Desarrollo de estudios de ingeniería
- Desarrollo de aplicaciones informáticas a medida
- Asistencias Técnicas.
- Consultorías Tecnológicas
- Instalación y Mantenimiento de productos Oracle.
- Administración de Base de datos

La organización para la seguridad de los sistemas queda establecida en ALTEN a partir, de un lado, de la identificación y definición de las diferentes actividades y responsabilidades en materia de seguridad de los sistemas y, de otro, de la implantación de una estructura que las soporte. La estructura organizativa encargada de la gestión de la seguridad de la información del ALTEN está compuesta por los siguientes agentes: Responsable de Gestión del Sistemas, equipo del departamento de sistemas en los tres centros principales y el responsable de Calidad.

ALTEN es consciente de que la calidad de los servicios que presta a los clientes puede venir, en el medio plazo, condicionada, además de por cambios de naturaleza jurídica, por otros factores de muy diversa índole, como son las circunstancias económicas, las necesidades y exigencias, también cambiantes, de los propios profesionales, el conocimiento funcional, los avances tecnológicos o los nuevos modelos de gestión. Por ello ha determinado las siguientes cuestiones externas e internas que son pertinentes en el propósito de desarrollar su Sistema de Gestión de la Seguridad de la Información (en adelante SGSI);

- Peligros de la red por el aumento continuo de los ataques informáticos y accesos no autorizados, que obligan a tomar medidas para proteger la información, especialmente la sensible que maneja la entidad como organismo que se debe a sus partes interesadas.
- Los cambios continuos de la tecnología y la obligación, y correlativa preocupación, del ALTEN por mantener un constante estado del arte para alinear sus servicios a las nuevas necesidades.
- El también cambiante marco legal y regulatorio en el que se desarrollan las actividades de la entidad, tanto de naturaleza pública como privada.
- Las necesidades y expectativas de las partes interesadas de la entidad con el objeto de garantizar que toda la información perteneciente a las mismas que tenga el ALTEN deberá estar protegida en todas las dimensiones de seguridad.
- La alineación de las necesidades de los servicios de la información con la cultura, los procesos, la estructura y la estrategia de la organización.

Partes Interesadas, sus necesidades y expectativas.

ALTEN ha determinado las partes interesadas “relevantes” para el SGSI, que son las siguientes:

- Área Comercial
- Clientes
- Comité de Dirección
- Empleados
- Comité de Seguridad TIC
- Proveedores.
- ALTEN corporación (Accionistas e inversores)
- Administración Pública

ALTEN ha de adoptar cuantas medidas sean necesarias para garantizar que la información que gestiona en el desarrollo de las actividades que lleva a cabo para satisfacer las necesidades y expectativas de las partes interesadas antes mencionadas, en el ámbito de sus funciones, quede protegida en sus dimensiones de **disponibilidad, integridad, confidencialidad, trazabilidad y**

autenticidad tal y como señalan, básicamente, el Reglamento General de Protección de Datos (RGPD) y en ENS.

Objetivos estratégicos:

- **OBJETIVO 1.** MEJORAR LA POLÍTICA DE IMAGEN Y COMUNICACIÓN
- **OBJETIVO 2.** LOGRAR UN MODELO ECONÓMICO-FINANCIERO SUFICIENTE
- **OBJETIVO 3.** POTENCIAR Y ABRIR EL MARCO COMPETENCIAL-PROFESIONAL DE LA CONSULTORIA TECNOLÓGICA A LA SOCIEDAD
- **OBJETIVO 5.** IMPULSAR Y FOMENTAR EL DESARROLLO DE LAS PERSONAS
- **OBJETIVO 6.** DETECTAR NECESIDADES Y EXPECTATIVAS DE NUESTROS GRUPOS DE INTERES Y AUMENTAR SU GRADO DE SATISFACCIÓN
- **OBJETIVO 7.** ADECUAR LA PRESTACIÓN DE SERVICIOS A LAS NECESIDADES DEL ENTORNO CON EL OBJETIVO DE SITUAR A AL TEN EN UNA POSICIÓN DE EXCELENCIA
- **OBJETIVO 8.** AVANZAR EN PROYECTOS EN PREVISIÓN Y DESARROLLO

Asimismo, a través de nuestra Política de Seguridad nos marcamos como **compromisos** que:

- La información y los servicios estén protegidos contra pérdidas de disponibilidad y contra accesos no autorizados, preservando, al tiempo, su confidencialidad e integridad.
- Se cumplan los requisitos legales de aplicación en esta materia en cada momento.
- Las incidencias de seguridad sean comunicadas y tratadas apropiadamente.
- Se establezcan procedimientos adecuados para facilitar el cumplimiento de esta política.
- El Responsable de Seguridad de la Información se encargue de salvaguardar esta política junto con los procedimientos dispuestos por el Comité de Dirección, así como de proporcionar apoyo en su implementación.
- El Comité de Seguridad de la información se encargue de implementar esta política y sus correspondientes procedimientos.
- Cada empleado se responsabilice de cumplir con esta política, así como con el Código de buenas prácticas y con sus procedimientos, de acuerdo con las características y exigencias propias de su puesto.

Se lleve a cabo un constante seguimiento del SGSI y del mantenimiento y adecuación al mismo de su Política de Seguridad.

Alcance del Sistema de Gestión de Seguridad de la Información.

AL TEN aplica su SGSI basado en la **ISO 27001**. El Alcance del Sistema de Gestión de Seguridad de la Información, de categoría MEDIA, para AL TEN comprende “EL SISTEMA DE INFORMACIÓN QUE DAN SOPORTE A LOS SERVICIOS DE CONSULTORÍA, TECNOLOGÍAS DE LA INFORMACIÓN Y SERVICIOS DE INGENIERÍA” según la Declaración de Aplicabilidad vigente, que aplica a sus sedes de Madrid, Lisboa y su centro de Alten Delivery Center Spain.

AL TEN aplica el **Esquema Nacional de Seguridad** sobre el sistema de información que dan soporte a los Servicios de Implantaciones Tecnológicas, Administración de Infraestructura, Soporte a Aplicaciones, incluido soporte a NEDAES. Según la Declaración de Conformidad vigente. Categoría MEDIA.

AL TEN aplica la **ISO 27701** dentro del sistema de gestión de privacidad de la información como responsable de los siguientes tratamientos de la empresa Alten:

- Gestión de clientes
- Gestión de proveedores
- Servicio PRL
- Gestión de RRHH
- Control de acceso de visitas y video vigilancia de las instalaciones de Alten

Encargado del tratamiento:

- 1) Los sistemas de información que dan soporte al proceso de gestión de la actividad comercial y la gestión de ofertas para proyectos del área de la administración pública,
- 2) Seguridad de la información de aquellos proyectos en los cuales se exija por parte del cliente requisitos de seguridad y privacidad sobre la ejecución del proyecto.

Según la declaración de aplicabilidad para protección de datos personales versión 1.0 y conforme al registro de actividad de tratamiento versión 1.0.

MARCO LEGAL

La definición de un sistema idóneo de gestión de la seguridad de la información en el AL TEN ha de pasar por la consideración de, al menos, las siguientes disposiciones normativas:

- Reglamento (UE) 2016/679. RGPD – Reglamento General de Protección de Datos
- Reglamento (UE) 2016/679 del Parlamento Europeo, de 27 de abril de 2016, por el que se aprueba el Reglamento General de Protección de Datos.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.
- 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 59/2003, de 19 de diciembre, de firma electrónica
- Real Decreto Legislativo 3/2011, de 14 de noviembre, por el que se aprueba el texto refundido de la Ley de Contratos del Sector Público.
- Ley 10/2021, de 9 de julio, de trabajo a distancia.

CONTEXTO. ANÁLISIS DE LA SITUACIÓN DE PARTIDA

El cambio que ha sufrido el propio concepto de “documento”, derivado, en buena medida, de la generalización de la información que hoy día se envía y recibe en formato electrónico, ha llevado, además, a establecer nueva regulación y novedosos procedimientos para la identificación, recogida y conservación del llamado patrimonio cultural digital, afectando este hecho incluso a la información institucional, organizativa y de planificación que las empresas de consultoría tecnológica, como parte del ámbito subjetivo de la ley 19/2013, de Transparencia, acceso a la información pública y buen gobierno, generan.

Conocido lo anterior, se ha de señalar que la estrategia TIC de AL TEN parte de una situación inicial, que se perfila a través del análisis de sus características internas (Debilidades y Fortalezas) y de su situación externa (Amenazas y Oportunidades) (análisis DAFO). Los resultados se presentan a continuación en un diagrama de matriz:

	Fortalezas	Debilidades
Análisis interno	<ul style="list-style-type: none"> Personal de la Gerencia de tecnologías con capacidad técnica experiencia profesional Alta dirección comprometida con la mejora de las TIC y su seguridad Objetivos claramente definidos 	<ul style="list-style-type: none"> Cultura organizacional con predisposición a la resistencia al cambio y tendencia a mantener funcionamiento y operativa tradicionales Entorno cambiante Dependencia de los fabricantes de los productos especializados Falta de concienciación de seguridad tanto de los usuarios como de los fabricantes Limitada infraestructura Limitaciones presupuestarias Problemas de motivación y formación del personal
	Oportunidades	Amenazas
Análisis externo	<ul style="list-style-type: none"> Gestionar y establecer mayor control sobre el uso de datos personales Control de delitos cibernéticos Regulación y legislación Conocimiento del ciudadano en el uso de las TIC Teletrabajo 	<ul style="list-style-type: none"> Vulnerabilidades Ausencia de soluciones de seguridad especializada Usuarios maliciosos Alta exposición (internet)

Esta estrategia contiene las líneas de actuación que surgen de combinar las fortalezas de la organización con las oportunidades externas, teniendo en cuenta las limitaciones que surgen de la combinación de debilidades.

MARCO ESTRATÉGICO

Misión

Corresponde a ALTEN, en el marco de los fines y funciones que legal y estatutariamente le han sido conferidos, la puesta en marcha y ejecución de, entre otras, las siguientes actuaciones:

- (i) Velar por la satisfacción de los intereses generales relacionados con el cliente.
- (ii) La representación exclusiva de esta profesión en el ámbito de su competencia.
- (iii) La defensa de los derechos e intereses profesionales de los trabajadores.
- (iv) La provisión de servicios que aporten elementos para el éxito de nuestros grupos de interés, propiciando, al mismo tiempo, el desarrollo permanente de la organización y de las personas vinculadas y relacionadas con ella.

Visión

Es objetivo esencial del ALTEN la prestación al cliente de un servicio excelente, innovador en técnicas y herramientas informáticas, que sea transparente en su gestión y responsable, respetuoso y comprometido con el medio ambiente. Con todo ello ALTEN aspira a dotar a sus profesionales de una formación continuada que les permita mejorar sus capacidades científico-técnicas.

5 LIDERAZGO

Liderazgo y Compromiso.

La Dirección de **AL TEN** adquiere el compromiso de definir, desarrollar e implementar y mantener el SGSI definido en este MSGSI, impulsando los siguientes puntos:

- Asegurar el establecimiento de una política, compromisos y unos objetivos de la seguridad de la información y su alineación con la dirección estratégica de la compañía
- Asegurar la integración de los requisitos del SGSI en los procesos de la organización, dentro del alcance del SGSI
- Asegurar que los recursos necesarios del SGSI estén disponibles
- Comunicar la importancia de una gestión de la seguridad de la información eficaz y conforme con los requisitos del SGSI
- Liderar, supervisar y asegurar que el SGSI consigue los resultados previstos
- Dirigir y apoyar a las personas, para contribuir a la eficacia del SGSI
- Promover la **mejora continua**
- Apoyar otros roles pertinentes de la Dirección, para impulsar el liderazgo en otras áreas de responsabilidad

Política

La Dirección de **AL TEN** ha definido el alcance y los límites del SGSI en su Política de Seguridad que:

- Incluye un marco de referencia para fijar objetivos y establece un sentido de orientación y principios generales de acción con respecto a la seguridad de la información;
- Toma en cuenta los requisitos legales o de regulación, y las obligaciones de seguridad contractuales;
- Está en línea con el contexto de gestión de riesgos estratégica de la entidad en el que tendrá lugar el establecimiento y mantenimiento del sgsi;
- Establece criterios con los cuales se evalúen los riesgos;
- Ha sido aprobada por la dirección general.

Por lo que la política del SGSI de la entidad cumple con los requisitos de la norma y está disponible como documento: ***POL-SI-01-Política-de-seguridad.***

Roles, responsabilidades y Autoridades en la organización

La Dirección de **AL TEN** adquiere el compromiso de desarrollar e implantar el SGSI definido en este MSGSI, así como de establecer un proceso de mejora continua.

Como bases fundamentales de este compromiso, la Dirección realiza las siguientes actividades:

- a) Establecimiento de la *Política de Seguridad de AL TEN*, en donde se asienta el compromiso de cumplir con los requisitos del SGSI en el alcance definido, así como los legales y reglamentarios aplicables. Asimismo, la difusión de dicha política, asegurando que es entendida por todos los miembros de **AL TEN**

- b) Asignar roles y las responsabilidades para la seguridad de la información
- c) Comunicar a la organización la conveniencia del cumplimiento de los objetivos de seguridad de la información y, conforme a la política de seguridad de la información sus responsabilidades legales y la necesidad de mejora continua
- d) Revisión anual del SGSI
- e) Establecimiento de los objetivos de la seguridad de la información
- f) Disponibilidad de recursos para el funcionamiento efectivo de los procesos del SGSI
- g) Criterios de aceptación de riesgos y niveles de riesgos aceptables
- h) Asegurar que se efectúen las auditorías internas del SGSI

6 PLANIFICACIÓN

ALTEN ha definido el enfoque de identificación, análisis y gestión de los riesgos que corren los activos incluidos en el alcance del SGSI llevando a cabo los pasos siguientes:

- Identificación de las partes interesadas, sus dependencias y los responsables de su operativa diaria, a través del personal de las áreas implicadas.
- Valoración de las partes interesadas y su relación con los activos y sus dependencias respecto al grado de confidencialidad, integridad y disponibilidad, aportada por sus responsables y personal afectado directa e indirectamente por los mismos.
- Identificación y análisis de las amenazas y vulnerabilidades a las que están expuestos cada uno de los activos, así como el impacto que provocaría si éstas llegaran a materializarse. Se incluirá en esta identificación y análisis los activos relacionados con proyectos específicos sujetos a requisitos de seguridad de la información.
- Estimación de los niveles de riesgo a través del mapa de riesgo potencial e identificación de los riesgos residuales. Se incluirá en esta estimación de niveles de riesgo los relacionados con proyectos específicos sujetos a requisitos de seguridad de la información.
- Identificación del tratamiento de los riesgos, así como la selección de objetivos de control y controles para el mismo. Se incluirá en el tratamiento de los riesgos los relacionados con proyectos específicos sujetos a requisitos de seguridad de la información.
- Elaboración de la declaración de aplicabilidad y el plan de tratamiento de riesgos que incluye:
 - Los objetivos de control y los controles seleccionados;
 - Los objetivos de control y controles actualmente implementados; y
 - La exclusión de algún objetivo de control y de controles del anexo a de la norma y la justificación de esa exclusión.

En el caso de proyectos sujetos a requisitos de seguridad de la información, se elaborará una declaración de aplicabilidad y plan de tratamiento de riesgos específicos.

Los pasos mencionados están reflejados en los siguientes documentos: ***Identificación de Activos, Análisis de Riesgos, Declaración de Aplicabilidad, el Plan de Tratamiento de Riesgos y procedimiento para la elaboración de planes de seguridad de proyectos.***

1) Implementar y operar el SGSI.

ALTEN ha formulado, implementado y operado un *Plan de Tratamientos Riesgos* para alcanzar el nivel de madurez objetivo de cada control, partiendo del documento de *Declaración de Aplicabilidad*, describiendo las medidas organizativas y técnicas a desarrollar para cada uno de los controles de la norma que forman parte del alcance, y de esta manera, poder medir la efectividad de los mismos.

2) Monitorear y revisar el SGSI.

- **ALTEN** revisa y monitorea los procedimientos, normativas, instrucciones u otros controles del SGSI para:
 - Detectar, corregir y prevenir errores e incidentes de seguridad mediante la utilización de indicadores

- Determinar si las medidas tomadas para solventar deficiencias del SGSI, fueron efectivas
 - **AL TEN** revisa las evaluaciones de riesgos al cierre del período anual para actualizarlos y/o adaptarlos a los cambios que se presenten en la entidad (organización, tecnología, objetivos, amenazas, efectividad de los controles implementados y cambios legales).
- 3) Mantener y mejorar el SGSI.**
- AL TEN mantiene y mejora el SGSI de forma continua, a través de la figura del Responsable de Gestión de Seguridad junto con los responsables de los procesos del SGSI, y los cambios que se vayan detectando, se presentan al Comité de Calidad y Seguridad de la Información cuyos miembros los evalúan, y si así lo deciden, los aprueban para su implementación, de acuerdo a la Normativa de Organización de la Seguridad de la Información y el Procedimiento de Control y Gestión Documental y de los Registros.
 - AL TEN sigue el Procedimiento de Inventario y Valoración de Activos y la Instrucción Técnica de Análisis y Gestión de Riesgos para efectuar los cambios, actualizaciones y mejoras que se hayan detectado en la revisión anual de los riesgos, comunicando y ejecutando las acciones correctivas y preventivas indicadas en el documento del Plan de Tratamiento de Riesgos.
 - Objetivos de seguridad de la información y planificación para su consecución

AL TEN a través de su Dirección tiene establecido los objetivos de la seguridad de la información en las funciones y niveles pertinentes.

Para que los servicios ofrecidos por AL TEN se presten con eficacia, en términos de nivel de servicio, seguridad, disponibilidad y alcance, la Dirección de la empresa apuesta por una gestión basada en un cumplimiento estricto de cualquier requisito legal que le afecte, en la creación de valor para sus clientes y en la implantación de una serie de buenas prácticas, articuladas a través de modelos de referencia internacional, como son las Normas ISO.

Por este motivo, AL TEN ha decidido desarrollar su Política de Seguridad de la Información, que fija sus Objetivos de Seguridad alineados con las necesidades de negocio, el reconocimiento del valor añadido de los sistemas a proteger y una comprensión de los riesgos asociados a estos sistemas y expresados en los siguientes términos:

- Cumplimiento con los requerimientos de negocio.
- Protección de los activos afectados de las amenazas internas, externas, accidentales o deliberadas, accesos no autorizados, etc.
- Se analizarán los riesgos de seguridad de la información de todos los servicios prestados por la organización, incluidos en el alcance del sistema y se establecerán los controles asociados necesarios para mitigar los riesgos identificados. Estos controles de seguridad se desarrollarán de acuerdo a las directrices recogidas en la Normativa de Seguridad de la Información.
- Mantenimiento del riesgo al que está sometida la información por debajo del nivel exigido por AL TEN.
- Optimización de los costes y garantía de la seguridad en la prestación de servicios incluidos en el alcance, por parte de **AL TEN**, asegurando la confidencialidad de la información y manteniendo la integridad y la disponibilidad de la misma.

- Cumplimiento de los requerimientos legislativos y regulatorios.
- Elaboración, mantenimiento y prueba de Planes de Continuidad de Negocio.
- Establecer un Plan de formación y concienciación en materia de seguridad de la información que ayude al personal implicado a conocer y cumplir esta política, y a prevenir los riesgos identificados o potenciales.
- Gestión de todo tipo de incidentes de seguridad.
- Implantación de un sistema de mejora continua basado en un control permanente de la gestión y en la estrategia de gestión de riesgos adoptada por la empresa.

7 SOPORTE

La Dirección de AL TEN determina y provee los recursos necesarios para:

- a) Establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI.
- b) Asegurar que los procedimientos/normativas/instrucciones/políticas de seguridad de la información apoyen los requerimientos de las áreas afectadas por el alcance del SGSI.
- c) Identificar y establecer los requisitos legales, de regulación y las obligaciones de seguridad contractuales.
- d) Mantener la seguridad adecuada mediante la aplicación correcta de todos los controles implementados.
- e) Realizar revisiones cuando sea necesario, y reaccionar debidamente a los resultados de esas revisiones.
- f) Mejorar la efectividad del SGSI.

Entrenamiento, Concienciación y Competencia.

- Todo el personal de AL TEN afectado por el SGSI, está adecuadamente cualificado.
- Cada vez que se requiera, AL TEN realiza/coordina sesiones de formación y/o entrenamiento al personal de las áreas incluidas en el alcance del SGSI para asegurar que tenga las competencias adecuadas en el desempeño de las tareas en materia de la seguridad de la información. *Se dispone de un plan de formación con las necesidades estimadas que podría tener el personal afectado por el SGSI, y se incluye la formación anualmente.*
- A su vez, AL TEN ha ideado un *Plan de Sensibilización*, donde se recoge todas las acciones e iniciativas que realiza la compañía para sensibilizar a los empleados en materia de seguridad de la información.

Comunicación

La organización tiene establecido las necesidades de comunicación interna y externas pertinentes al SGSI, a través del procedimiento **Comunicación Interna y Externa del SGSI**, en vigor. El procedimiento se adaptará a lo estipulado en el procedimiento *PR-ALT-18 Procedimiento de Comunicación Externa e Interna*.

Información Documentada

1) Generalidades

El SGSI se estructura de la forma siguiente:

- Documentación emitida
 - Políticas (política de seguridad)
 - Normativas
 - Procedimientos
 - Procesos

- Instrucciones de trabajo
- Manuales
- Otros documentos (objetivos del SGSI, metodología e informes de evaluación de riesgos, plan de tratamiento de riesgos, declaración de aplicabilidad, orden del día de reuniones del comité...)
- Documentación recibida
 - Normativa ISO aplicable
 - Reglamentación aplicable
 - Posible información aplicable emitida por entidades externas y con repercusión en la prestación de los servicios que afectan al SGSI de AL TEN en el alcance establecido
 - Registros de seguridad de la información

2) Control de documentos

Los documentos requeridos por el SGSI deberán controlarse para garantizar que sólo se utiliza y está disponible la última edición aplicable.

El *Procedimiento PO-ALT-01-Control-de-la-Documentación* establece las medidas adoptadas para:

- a) Aprobar los documentos en cuanto a su adecuación antes de su emisión
- b) Revisar y actualizar los documentos cuando sea necesario, así como para llevar a cabo su re-aprobación
- c) Asegurar que se identifican los cambios y el estado de versión y revisión actual de los documentos
- d) Asegurar que las versiones pertinentes de los documentos aplicables se encuentran disponibles en los puntos de uso
- e) Asegurar que los documentos permanecen legibles e identificables
- f) Asegurar que los documentos de origen externo que AL TEN determina que son necesarios para la planificación y la operación del SGSI, se identifican y se controlan su distribución
- g) Evitar el uso no intencionado de documentos obsoletos, y para aplicarles una identificación adecuada en el caso de que se mantengan por alguna razón cualquiera

3) Control de los registros

Los registros de la seguridad de la información deberán permanecer legibles, fácilmente identificables y recuperables, ya que proporcionan evidencia de las actividades desempeñadas por las áreas afectadas dentro del alcance del SGSI de AL TEN.

El *procedimiento PO-ALT-02-Control-de-los-Registros* establece:

- Requisitos de identificación, legibilidad, almacenamiento, protección y recuperación (localización y acceso)
- Tiempo de retención
- Disposición de los registros de la seguridad de la información



8 OPERACIÓN

AL TEN tiene, implementado y controlado todos los procesos necesarios para cumplir los requisitos relacionados con la seguridad de la información dependiendo de cada responsable y se llevan a cabo a lo largo del año según las necesidades relacionadas con el SGSI, así como sus objetivos y planificaciones.

AL TEN tiene determinado los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.

AL TEN establece a través de los elementos de Revisión por la Dirección y Auditorías internas del SGSI el control y supervisión de los cambios del SGSI, tanto planificados como aquellos cambios no previstos y registrados.

Apreciación de Riesgos de Seguridad de la Información

AL TEN tiene establecido en el procedimiento *"IT-SI-01-Análisis-y-Gestión-de-Riesgos"* en vigor, la obligación de conservar información documentada de los resultados de las apreciaciones de riesgos de seguridad de la información.

Tratamiento de riesgos de seguridad de la información

AL TEN tiene establecido en el procedimiento *"IT-SI-01-Análisis-y-Gestión-de-Riesgos"* en vigor, la obligación de conservar información documentada del plan de tratamiento de riesgos de seguridad de la información.

9 EVALUACIÓN DEL DESEMPEÑO

ALTEN tiene establecido los elementos necesarios a revisiones periódicas, para evaluar el desempeño de la seguridad de la información y la eficacia del SGSI, así mismo tiene articulado una sistemática de medición y supervisión de los objetivos e indicadores del SGSI a través del documento “Objetivos e Indicadores del SGSI” en vigor, estableciendo los protocolos adecuados para conservar la información documentada asociada.

Auditorías Internas del SGSI

El RGS establece el plan anual de auditorías internas del SGSI, que cubre todos los elementos del SGSI, con el objeto de determinar si está conforme con los requisitos de la norma, se ha implementado y se mantiene de manera efectiva; en caso contrario, se toman las medidas adecuadas para eliminar los incumplimientos detectados y sus causas.

ALTEN establecerá planes específicos para la realización de auditorías internas a proyectos a clientes conforme a lo marcado en los planes de seguridad aplicables.

Esa planificación de auditorías internas se realiza teniendo en cuenta el estado y la importancia de los dominios de control de la norma, procesos y áreas del alcance a auditar, así como los resultados de las auditorías previas. Se dispone de un plan estimado a tres años, que corresponden a los períodos de seguimiento para obtener y mantener la certificación del sistema.

La selección de los auditores y la realización de las auditorías asegura la objetividad e imparcialidad del proceso de auditoría, de modo que los auditores internos no auditarán actividades en los que ellos ejerzan alguna actividad.

El Procedimiento de Revisión y Mejora Continua, desarrolla en detalle el proceso anual de auditoría interna del SGSI.

Revisión del SGSI por la Dirección

Con el objeto de asegurar la consistencia, adecuación y eficacia del SGSI establecido, la Dirección revisa anualmente el SGSI.

Esta Revisión incluye la evaluación de las oportunidades de mejora, y la necesidad de efectuar cambios en el SGSI, incluyendo la política y los objetivos de la seguridad de la información.

La **NOR-SI-05-Normativa-de-organización-de-la-seguridad-de-la-información**, establece la estructura del Comité de la Calidad y Seguridad de la Información, su funcionamiento interno, periodicidad de reuniones, convocatorias, asuntos a tratar, toma de acuerdos, elaboración de actas, seguimiento de acuerdos, etc.

La información de entrada para la revisión por la Dirección incluirá información sobre:

- Resultados de las auditorías y revisiones del SGSI
- Retroalimentación de las partes interesadas
- Las técnicas, herramientas o procedimientos, que podrían usarse en la entidad para mejorar el desempeño y la efectividad del SGSI
- Resultados de las mediciones de eficacia
- Estado de acciones correctivas y preventivas

*El presente documento carece de validez por lo que se considera copia no controlada una vez descargado de la aplicación, por lo tanto, la versión en vigor se encuentra alojada en la aplicación DBDOC alojado en www.intranet.alten.es.

- Las vulnerabilidades o amenazas que no se enfocaron adecuadamente en la evaluación de riesgos previa
- Resultados de la medición a través de indicadores de seguridad de la información
- Medidas de seguimiento de revisiones anteriores
- Recomendaciones de mejoras

Además, en la reunión de revisión, se abordará la *Planificación de Operaciones y procesos del SGSI*, tratándose los siguientes asuntos:

- Previsión de cambios planificados que podrían afectar al Sistema de Gestión de la Seguridad de la Información
- Factores relacionados con el mercado, tales como la tecnología, la investigación y estrategias del mercado, así como otros factores que puedan tener impacto en la entidad, tales como condiciones financieras, sociales o medioambientales y cambios estatutarios o reglamentarios pertinentes
- Directrices genéricas de formación de los empleados de las áreas incluidas en el alcance del SGSI para el siguiente período
- Directrices genéricas de auditorías para el siguiente período
- Directrices genéricas sobre necesidades de recursos
- Seguimiento de la implantación y operación de los planes de seguridad
- Otros

Salidas de la Revisión

En la reunión de revisión del SGSI por la Dirección, a través del Comité de Calidad y Seguridad de la Información, se abordan los asuntos anteriores y se toman las acciones pertinentes, designando responsables y plazos de ejecución. Dichas acciones están encaminadas a:

- La mejora de la efectividad del SGSI y sus procesos (objetivos e indicadores de la seguridad de la información)
- Actualización de la evaluación de riesgos y el plan de tratamiento de riesgos
- Modificación de los procedimientos y controles de seguridad de la información, según sea necesario

El contenido de la revisión del SGSI, queda plasmado en el ***Informe de Revisión por Dirección***.

10 MEJORA

Mejora Continua

Los métodos y herramientas, a través de las cuales, AL TEN intenta mejorar continuamente la efectividad del SGSI, son las siguientes:

- Política de Seguridad de la Información
- Objetivos del SGSI
- Indicadores del SGSI
- Análisis de Riesgos
- Auditorías Internas
- Acciones Correctivas y Preventivas
- Revisión por la Dirección

No conformidad y Acción Correctiva.

El *PO-SI-11-Revisión-y-Mejora-Continua*, establece las acciones a tomar por la entidad para eliminar las causas de no conformidades con el objeto de prevenir su aparición.

Este procedimiento define los requisitos para:

- Revisar las no conformidades
- Determinar las causas de las no conformidades
- Evaluar la necesidad de adoptar acciones, para asegurar que las no conformidades no vuelven a ocurrir
- Determinar e implantar las acciones necesarias
- Registrar los resultados de las acciones tomadas
- Revisar la efectividad de las acciones correctivas tomadas



BUREAU
VERITAS

Bureau Veritas Certification

Certificación

Concedida a

GRUPO ALTEN

CL VÍA DE LOS POBLADOS 3 EDIFICIO 5 PLANTA 2 PARQUE EMPRESARIAL CRISTALIA
- 28033 - MADRID - ESPAÑA

Bureau Veritas Certification certifica que el Sistema de Gestión ha sido auditado y encontrado conforme con los requisitos de la norma:

NORMA

ISO/IEC 27001:2022

El Sistema de Gestión se aplica a:

SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD QUE DA SOPORTE A LOS SERVICIOS DE CONSULTORÍA, TECNOLOGÍAS DE LA INFORMACIÓN Y SERVICIOS DE INGENIERÍA, A LOS PROCESOS DE GESTIÓN DE LA ACTIVIDAD COMERCIAL, LA GESTIÓN DE LAS OFERTAS PARA PROYECTOS DEL ÁREA DE LA ADMINISTRACIÓN PÚBLICA, ASÍ COMO DE LA SEGURIDAD DE LA INFORMACIÓN DE AQUELLOS PROYECTOS EN LOS CUALES SE EXIJA POR PARTE DEL CLIENTE REQUISITOS DE SEGURIDAD SOBRE SU GESTIÓN; SEGÚN LA DECLARACIÓN DE APLICABILIDAD DE V.3.1.

Número del Certificado:	ES151268 - 1
Aprobación original:	14-01-2016
Auditoría de certificación/renovación:	13-12-2024
Caducidad del ciclo anterior:	13-01-2025
Certificado en vigor:	14-01-2025
Caducidad del certificado:	13-01-2028

Este certificado está sujeto a los términos y condiciones generales y particulares de los servicios de certificación

Bureau Veritas Iberia S.L.
C/ Valportillo Primera 22-24, 28108 Alcobendas - Madrid, España





BUREAU
VERITAS

Certificación

Concedida a

GRUPO ALTEN

Bureau Veritas Certification

Emplazamiento	Dirección	Alcance
ALTEN DELIVERY CENTER, S.L.	CL VÍA DE LOS POBLADOS 3 EDIFICIO 5 PLANTA 2 PARQUE EMPRESARIAL CRISTALIA - 28033 - MADRID - ESPAÑA	SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD QUE DA SOPORTE A LOS SERVICIOS DE CONSULTORÍA, TECNOLOGÍAS DE LA INFORMACIÓN Y SERVICIOS DE INGENIERÍA, SEGÚN LA DECLARACIÓN DE APLICABILIDAD DE V.3.1.
ALTEN SOLUCIONES, PRODUCTOS, AUDITORÍA E INGENIERÍA, S.A.U.	CL VÍA DE LOS POBLADOS 3 EDIFICIO 5 PLANTA 2 PARQUE EMPRESARIAL CRISTALIA - 28033 - MADRID - ESPAÑA	SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD QUE DA SOPORTE A LOS PROCESOS DE GESTIÓN DE LA ACTIVIDAD COMERCIAL, LA GESTIÓN DE LAS OFERTAS PARA PROYECTOS DEL ÁREA DE LA ADMINISTRACIÓN PÚBLICA, ASÍ COMO DE LA SEGURIDAD DE LA INFORMACIÓN DE AQUELLOS PROYECTOS EN LOS CUALES SE EXIJA POR PARTE DEL CLIENTE REQUISITOS DE SEGURIDAD SOBRE SU GESTIÓN; SEGÚN LA DECLARACIÓN DE APLICABILIDAD DE V.3.1.
TECHALTEN PORTUGAL, UNIPESSOAL, LDA.	EDIFICIO ORIENTE, RUA MAR DA CHINA N°3 BLOCO B, PISO 4, PARQUE DAS NAÇÕES - 1990-183 - LISBOA - Portugal	SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD QUE DA SOPORTE A LOS PROCESOS DE GESTIÓN DE LA ACTIVIDAD COMERCIAL, LA GESTIÓN DE LAS OFERTAS PARA PROYECTOS DEL ÁREA DE LA ADMINISTRACIÓN PÚBLICA, ASÍ COMO DE LA SEGURIDAD DE LA INFORMACIÓN DE AQUELLOS PROYECTOS EN LOS CUALES SE EXIJA POR PARTE DEL CLIENTE REQUISITOS DE SEGURIDAD SOBRE SU GESTIÓN; SEGÚN LA DECLARACIÓN DE APLICABILIDAD DE V.3.1.

Número del certificado:	ES151268 - 1
Aprobación original:	14-01-2016
Auditoría de certificación/renovación:	13-12-2024
Caducidad del ciclo anterior:	13-01-2025
Certificado en vigor:	14-01-2025
Caducidad del certificado:	13-01-2028

Este certificado está sujeto a los términos y condiciones generales y particulares de los servicios de certificación

Bureau Veritas Iberia S.L.
C/ Valportillo Primera 22-24, 28108 Alcobendas - Madrid, España

