Sistema de Gestión Integrado

# MANUAL DE GESTIÓN

Documento de uso interno

## CONTROL DE VERSIONES

| Revisión | Fecha | Motivo del Cambio |
|---|---|---|
| 1 | 09/05/2016 | Primera Emisión |
| 1.1 | 22/11/2016 | Actualizada para adecuarse al ENS |
| 1.2 | 29/12/2016 | Reemplazado cuadro de control de cambios. |
| 1.3 | 21/02/2017 | Realizados cambios para integrar el SGSI con la ISO 9001<br>Cambiado el nombre y el código |
| 1.4 | 20/03/2017 | Corrección de errores |
| 1.5 | 20/04/2017 | Añadidas referencias a los Propietarios del activo y del Riesgo en el apartado 4.6.2 |
| 1.6 | 1/06/2017 | Revisión - Corrección |

| | |
|---|---|
| Realizado y revisado<br>Miguel Gómez Laguna<br><br>Fdo.<br>Fecha 1-06-2017 | Aprobado<br>Comité de Gestión<br><br>Fdo.<br>Fecha 6-06-2017 |

# Contenido

# 1. Introducción

## 1.1 Presentación de la Organización

SPAI innova integra un grupo de profesionales conocedores de la administración local, especializados en el desarrollo e implantación de soluciones software, y en la prestación de los servicios asociados.

Protagonistas sin lugar a dudas de la informatización y modernización de la Administración Local española y en particular, de la implantación de Sistemas de Información Contable para la Administración Local (SICAL) de más de la mitad de los ayuntamientos y diputaciones, con soluciones contrastadas y de éxito desde 1992 hasta hoy.

Nos apasiona la creación de ambientes de trabajo con alta motivación y entusiasmo, vital para un equipo que acumula las mejores experiencias, con recursos financieros propios, además de nuevas oportunidades profesionales y laborales.

El objetivo de SPAI innova es ambicioso, pues además de ofrecer los productos de siempre existe un firme compromiso de mejora, ampliación e integración con nuevas soluciones demandadas por los clientes, junto a soluciones de Administración Electrónica exigidas por la legislación para la simplificación de procesos y la mejora de los servicios a los ciudadanos.

También es nuestro objetivo generar un ecosistema de trabajo y colaboración basado en las personas y en su desarrollo profesional. Un entorno estable y confiable, sostenible, comprometido, con un equipo motivado en armonía con nuestra orientación al cliente, que garantice respuestas a tiempo a los cambios a los que se enfrenta la administración, y a las necesidades del día a día de nuestros clientes y usuarios.

Con la experiencia de la cercanía a nuestros clientes, el trato humano, personal y profesional, nuestro sueño es ser el socio tecnológico de confianza para todas aquellas entidades y profesionales del sector público que valoren esta forma de entender el servicio.

Queremos ser los más cercanos y adaptables a sus necesidades, y que nuestro "sello" sea, además:

- La coherencia y contención en nuestras políticas de precios evitando las prácticas abusivas.
- La ética en nuestras relaciones con instituciones, clientes y empresas de nuestro entorno.
- Responsabilidad e implicación con la sociedad, nuestros colaboradores internos y externos, y nuestros clientes.
- Compromiso y agilidad ante los cambios.
- Cercanía para entender los problemas y tratar de dar las respuestas adecuadas.
- La mejor disposición para colaborar con otras empresas en beneficio del interés de nuestros clientes.

En SPAI entendemos la necesidad de trabajar con calidad, seguridad y responsabilidad y lo asumimos como constantes de nuestro trabajo diario. Por ello hemos adoptado un Sistema de Gestión que Integra la Gestión de la Calidad y de la Seguridad de la Información, con el fin de:

- Asegurar a nuestros clientes nuestro constante esfuerzo por cumplir y elevar los estándares de calidad de nuestros productos/servicios, para así satisfacer sus necesidades presentes y futuras.
- Identificar los procesos que desarrollamos con el fin de la mejora continua de los mismos.
- Dotar a la organización de una herramienta que especifique las responsabilidades de cada área de trabajo con el fin de evitar solapamientos en las competencias de las mismas.
- Disponer de una guía de actuación que prevenga la aparición de no conformidades y, si éstas ya se han producido, adoptar las medidas necesarias para la correcta resolución de las mismas.
- Contar con una descripción detallada de la empresa que permita la adopción de nuevas técnicas, procedimientos y personal que contribuyan a la mejora continua de los productos/servicios dispensados por la organización.

## 1.2 Importancia de los sistemas TIC y la seguridad de la información

SPAI INNOVA depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad, o trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios.

Esto implica que se deben aplicar medidas de seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

SPAI INNOVA debe cerciorarse de que la seguridad de la información es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

SPAI INNOVA debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Esquema Nacional de Seguridad y a la Ley Orgánica de Protección de Datos.

Esta Política de Seguridad sigue las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia.

## 1.3 Conceptos Generales

Se contemplan las siguientes dimensiones de seguridad:

- **Disponibilidad:** propiedad o característica de los activos consistentes en que las entidades o procesos autorizados tengan acceso a los mismos cuando lo requieran. Es necesario garantizar que los recursos del sistema se encontrarán disponibles cuando se necesiten, especialmente la información crítica.
- **Integridad:** propiedad o característica consistente en que el activo de información no sea alterado de manera no autorizada. La información del sistema ha de estar disponible tal y como se almacenó por un agente autorizado.
- **Confidencialidad:** propiedad o característica consistente en que la información ni se ponga a disposición, ni se revele a individuos, entidades o procesos no autorizados. La información sólo ha de estar disponible para agentes autorizados, especialmente su propietario.
- **Autenticidad:** propiedad o característica consistente en que una entidad sea quien dice ser o bien que garantice la fuente de la que proceden los datos. El sistema ha de ser capaz de verificar la identidad de sus usuarios, y los usuarios la del sistema.
- **Trazabilidad:** propiedad o característica consistente en que las actuaciones de una entidad puedan ser imputadas exclusivamente a dicha entidad.

Además, también se considerará:

- **Utilidad:** Los recursos del sistema y la información manejada en el mismo han de ser útiles para alguna función.
- **Posesión:** Los propietarios de un sistema han de ser capaces de controlarlo en todo momento; perder este control en favor de un usuario malicioso compromete la seguridad del sistema hacia el resto de usuarios.

El ciclo PDCA es el que se utilizará durante todo el ciclo de vida del SGI.

- **P (Planificar):** en esta fase se establecen las actividades, responsabilidades y recursos además de los objetivos a cumplir y cómo se van a medir estos objetivos.
- **D (Desarrollar):** se desarrollan los procesos y se implementan. Una vez implementados, hay que medir los resultados de la ejecución de dichos procesos.
- **C (Comprobar):** se analizan los resultados para comprobar si se han alcanzado los objetivos y si no es así, identificar las causas.
- **A (Actuar):** Se toman las acciones necesarias para corregir los fallos detectados en los procesos o para mejorarlos.

## 1.4 Prevención

SPAI INNOVA debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello implementará las medidas mínimas de seguridad determinadas por el ENS y la LOPD, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, van a estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, SPAI INNOVA debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

## 1.5 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, es preciso monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables, tanto regularmente, como cuando se produzca una desviación significativa de los parámetros que se haya prestablecido como normales.

## 1.6 Respuesta

SPAI INNOVA:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa un punto de contacto para las comunicaciones con respecto a incidentes detectados en otros Departamentos o en otros organismos.
- Establecer protocolos de intercambio de información relacionada con incidentes con clientes y proveedores.

## 1.7 Recuperación

Para garantizar la disponibilidad de los servicios críticos, SPAI INNOVA ha desarrollado planes de contingencia de los sistemas TIC como parte de su plan general de continuidad del servicio y actividades de recuperación.

## 1.8 Normas aplicables

Las normas que han servido de referencia para la elaboración del presente Manual de Gestión son las siguientes:

- **UNE/EN-ISO 9001** "Sistemas de Gestión de la Calidad. Requisitos."
- **Norma UNE/ISO-IEC 27001 Tecnología de la Información.** Especificaciones para los Sistemas de Gestión de Seguridad de la Información.
- **Real Decreto 3/2010**, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad** (ENS) en el ámbito de la Administración Electrónica, que en su artículo 11 establece la obligación para las Administraciones Públicas de disponer de una Política de Seguridad e indica los requisitos mínimos que debe cumplir.
- **Real Decreto 951/2015**, de 23 de octubre, de modificación del 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 Orgánica 15/99 de Protección de Datos de Carácter Personal (LOPD).
- **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 (LOPD).

# 2. Objeto y campo de aplicación

## 2.1 Objeto

Este Documento tiene como objetivo establecer las directrices que garanticen la calidad y la seguridad de la información de los servicios y productos de SPAI INNOVA a un nivel adecuado según el nivel de riesgo de los activos y nuestras necesidades y recursos.

La información y los procesos que la apoyan, son importantes activos para la empresa. La disponibilidad, integridad y confidencialidad de la información son esenciales para mantener la calidad de los servicios y la reputación e imagen de la empresa.

## 2.2 Alcance

Todas las pautas descritas en el presente documento serán efectivas para el conjunto de SPAI INNOVA, sus instalaciones y activos:

- A todos los departamentos, tanto a sus directivos como a empleados.
- A los contratistas, clientes o cualquier otra tercera parte que tenga acceso a la información o los sistemas de SPAI INNOVA.
- A bases de datos, ficheros electrónicos y en soporte papel, tratamientos, equipos, soportes, programas y sistemas.
- A la información generada, procesada y almacenada, independientemente de su soporte y formato, utilizada en tareas operativas o administrativas.
- A la información cedida dentro de un marco legal establecido, que será considerada como propia a efectos exclusivos de su protección.
- A todos los sistemas utilizados para administrar y gestionar la información, sean propios, alquilados o licenciados.

El alcance del Sistema de Gestión de Integrado de acuerdo a la normas ISO/IEC 27001, ISO 9001 y al Esquema Nacional de Seguridad es:

- Gestión de la Formación en Tecnología de la Información.
- Análisis, Diseño, Desarrollo, Mantenimiento y Soporte de aplicaciones en plataformas digitales.
- Servicio de Consultoría y Servicio de prestación en Cloud, para nuestros clientes. Se va a subcontratar un servicio, actualmente se presta desde los propios. Se alquilarán servidores.

**Localización**

**Sevilla:**

- Avda. Blas Infante, 8 Planta 3ª, módulos 16 y 17, 41400 – Écija.
- Teléfono: 955 314 020
- Email: info@spaiinnova.com

**Barcelona:**

- Avda. Castell de Barberà, 22-24, 08210 - Barberà del Vallès
- Teléfono: 935 193 834
- Email: info@spaiinnova.com

**Murcia**

Avda. de Juan Carlos I, Nº 59 (Edificio Torre Dimovil), Planta 5ª, Oficina 1, 30100 - Murcia

- Teléfono: 968 233 280
- Email: info@spaiinnova.com

## 2.3 Objetivos del Sistema de Gestión

SPAI INNOVA define el presente Manual de Gestión, de carácter obligatorio para todos sus empleados, teniendo un objetivo fundamental garantizar la calidad y la seguridad de la información y la prestación continuada de los servicios que proporciona, actuando preventivamente, supervisando la actividad y reaccionando con presteza frente a los incidentes que puedan ocurrir.

Uno de los objetivos de este documento es establecer las directrices que garanticen la seguridad de la información en SPAI INNOVA a un nivel adecuado según el nivel de riesgo de los activos y las necesidades y recursos de esta organización.

Este documento debe sentar las bases para que el acceso, uso, custodia y salvaguarda de los activos de información, de los que se sirve SPAI INNOVA para desarrollar sus funciones, se realicen, bajo garantías de seguridad, en sus distintas dimensiones: Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad.

Bajo estas premisas los **objetivos del Sistema de Gestión** serán:

- Asegurar que la plantilla conoce y comprende los requisitos del sistema de gestión y que asumen y son conscientes de sus responsabilidades en este tema.
- Proporcionar una guía para establecer los estándares, procedimientos, medidas de seguridad y cualquier otro medio que se estime oportuno para la gestión de la calidad y la seguridad de la información.
- Velar por la seguridad de la información, en sus distintas dimensiones.
- Cumplir los requisitos del negocio respecto a la seguridad de la información y los sistemas de información.
- Maximizar la calidad de los servicios prestados a nuestros clientes.
- Gestionar formalmente la seguridad, sobre la base de procesos de análisis de riesgos, para reducir o eliminar los riesgos inherentes a nuestras actividades por medio de la mejora continua del desempeño en seguridad en nuestros procesos, productos y servicios.
- Elaborar, mantener y probar los planes de contingencias y continuidad de la actividad que se definan para los distintos servicios ofrecidos.
- Realizar una adecuada gestión de incidentes que afecten a la seguridad de la información (ciberincidentes).
- Mantener informado a todo el personal acerca de los requerimientos de seguridad, y difundir buenas prácticas para el manejo seguro de la información.
- Proporcionar los niveles de seguridad acordados con terceras partes cuando se compartan o cedan activos de información.
- Garantizar que nuestras operaciones y procesos actuales y futuros cumplan con la legislación vigente en materia de seguridad de la Información.

Este Manual de Gestión:

- Se aprobará formalmente por la Dirección de SPAI INNOVA.
- Se revisará de forma anual, de manera que se adapte a las nuevas circunstancias, técnicas u organizativas, y evite la obsolescencia.
- Se comunicará a todos los empleados.
- El Responsable del Sistema de Gestión será el encargado de mantener esta manual, los procedimientos y de proporcionar apoyo en su implementación.
- Cada empleado es responsable de cumplir este manual y sus procedimientos según aplique a su puesto de trabajo.
- Los responsables de cada departamento serán los encargados de implementar esta Política y sus correspondientes procedimientos dentro de su área.
- Se mantendrá a disposición de las partes interesadas este manual así como los futuros desarrollos de la misma.

## 2.4 Plan de Mejora. Objetivos de Seguridad y Calidad

El Comité de Gestión establecerá y aprobará un Plan de Mejora con carácter anual en el que se definirán los objetivos de calidad y seguridad que se consideren necesarios en cada caso para cumplir con los objetivos indicados. Se deben establecer objetivos coherentes con las políticas de seguridad y calidad definidas, y proporcionar los recursos necesarios para su consecución, que serán definidos en el propio Plan de Mejora.

## 2.5 Exclusiones

**ISO 9001 - 7.1.5 Recursos de seguimiento y medición**: Dadas las características de los productos/servicios que la empresa suministra y los requisitos a él asociados, así como del desarrollo de las actividades de seguimiento y medición que se realizan durante el proceso de realización del mismo, no se considera necesario el uso de equipos de seguimiento y medición, por lo que este apartado se tratará como una exclusión permitida.

Los controles no aplicados del Anexo A de la Norma UNE/ISO-IEC 27001 se recogen en el Documento de Aplicabilidad en vigor.

**Esquema Nacional de Seguridad –op.exp.11 Protección de claves criptográficas:** De acuerdo con la guía de seguridad CCN-STIC 804 “Guía de Implantación”, el uso de claves criptográficas es condición de aplicabilidad de este control. Dado que la empresa no utiliza este tipo de claves se indica en el Documento de Aplicabilidad que esta medida no aplica.

## 2.6 Requisitos Legales

Con el objeto de satisfacer los compromisos establecidos de cumplir con la legislación y reglamentación aplicable a las actividades, productos y servicios de SPAI INNOVA, tiene establecido y mantiene el procedimiento **PG.03 Cumplimiento Legal** para la identificación y acceso a dichos requisitos legales y otros requisitos a los que la empresa se somete (acuerdos con autoridades públicas, códigos de buenas prácticas industriales y directrices o pautas no reglamentarias).

Según la legislación vigente, las leyes aplicables a SPAI INNOVA para las actividades dentro del alcance del Sistema de Gestión son:

- **Real Decreto 3/2010**, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad** (ENS) en el ámbito de la Administración Electrónica, que en su artículo 11 establece la obligación para las Administraciones Públicas de disponer de una Política de Seguridad e indica los requisitos mínimos que debe cumplir.
- **Real Decreto 951/2015**, de 23 de octubre, de modificación del 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 Orgánica 15/99 de Protección de Datos de Carácter Personal (LOPD).
- **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 (LOPD).
- Real Decreto Legislativo 1/1996, de 12 de abril, **Ley de Propiedad Intelectual**.
- Ley de Propiedad Industrial.
- Ley 34/2002, de 11 de julio, de **servicios de la sociedad de la información** y de comercio electrónico(LSSI).

# 3. Contexto de la organización

## 3.1 Organigrama

SPAI INNOVA se encuentra organizada en tres niveles, en el nivel más alto se encuentra la Gerencia de la empresa, y la mayoría de departamentos dependen directamente de la misma:

- Gerente
    - Departamento de Administración
        - Departamento de Recursos humanos
    - Departamento Comercial
    - Departamento de Consultoría
    - Departamento de Desarrollo
    - Departamento de Dirección de proyectos
    - Departamento de Soporte
    - Departamento TI
    - Comité de Gestión

## 3.2 Infraestructura informática

La red de SPAI Innova Astigitas dispone de un Data Center propio donde se alojan los servidores. El número total de puestos de trabajo aproximado es de 60. Utilizando principalmente Sistema Operativo Windows en los puestos de trabajo, en sus versiones Windows 7 y Windows 10. Respecto a la estructura de servidores; se utiliza un sistema de virtualización, disponiendo de servidores virtuales, con sistemas operativos tanto Windows como GNU/Linux.

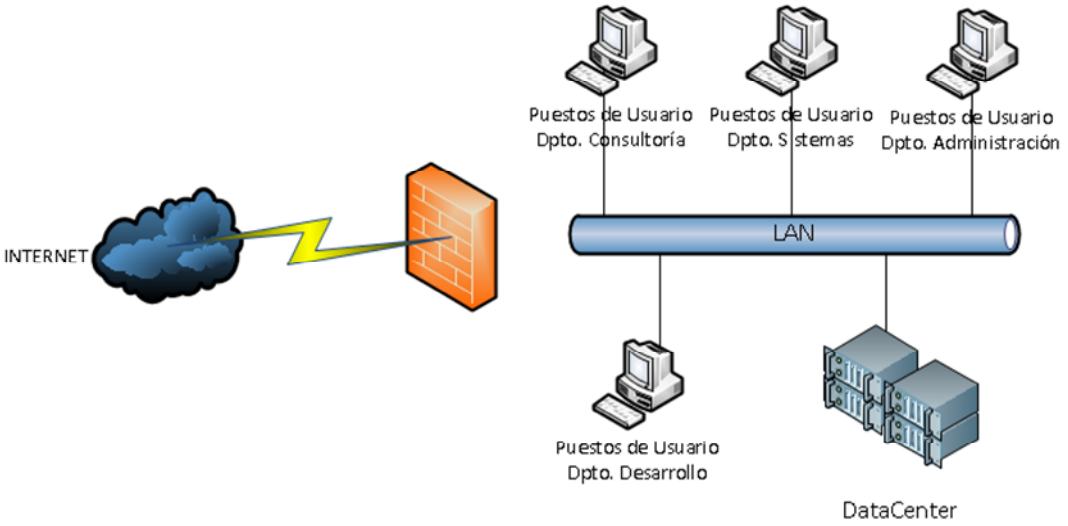
Se dispone de acceso a internet mediante Fibra Óptica, siendo Telefónica España y AireNetworks los proveedores del servicio. El acceso a internet está filtrado mediante Firewall corporativo así garantizar la seguridad de la organización.

Se dispone de una red organizativa: Directorio Activo para gestionar los permisos de acceso de los usuarios en los puestos de trabajos. La autenticación de los usuarios se realiza mediante uno o dos factores de autenticación, en función de las conclusiones de análisis de riesgos.

Las aplicaciones utilizadas en las estaciones de trabajo son (además del software propio desarrollado por la empresa) las siguientes: suite informática Office, herramientas de desarrollo de código abierto (como Eclipse), software desarrollado a medida (software de contabilidad, ERP), etc.

La información tratada por parte de los empleados de la entidad se almacena en servidores de ficheros destinados para ello, generándose copias de seguridad periódicas de la misma.

Todo el mantenimiento de infraestructura técnica se realiza por el personal especializado de la empresa.




## 3.3 Partes interesadas: Relaciones internas y externas

El sistema de gestión definido tendrá en cuenta las diferentes partes implicadas en el sistema de información siendo estas principalmente:

- **Clientes:** como parte fundamental del sistema, se velará por preservar la confidencialidad, integridad y disponibilidad, de la información intercambiada con los clientes, y necesaria para la prestación de los servicios señalados en el alcance, así como cualquier otra información (administrativa, de contacto…) necesaria para la prestación del servicio.
- **Proveedores:** Debido a la relevancia de los proveedores de servicios para el tratamiento de la información, especialmente en cuanto a los servicios de TI necesarios para la prestación de los servicios de SPAI INNOVA (como son los proveedores de las aplicaciones informáticas, o los encargados de las tareas de mantenimiento informático), se han establecido los requisitos necesarios para garantizar la seguridad y disponibilidad de sus servicios. Se deben de tener en cuenta igualmente los envíos de información realizados a las entidades bancarias.
- **Administración Pública:** Como destinatarios de los servicios prestados por SPAI INNOVA, con la finalidad de cumplir con las normas y leyes de aplicación, el envío de información se realizará, bien a través de los medios que dichos organismos ponen a disposición para tal fin (servicios web) o bien mediante medios alternativos como correo electrónico (mediante firma electrónica) o soportes magnéticos.
- **Trabajadores:** Como parte fundamental en el tratamiento de la información, los empleados deberán de conocer las normas y procedimientos de seguridad que se decidan aplicar en la organización para asegurar la confidencialidad, integridad y disponibilidad de los datos.

Se detalla a continuación las relaciones entre las diferentes partes interesadas que se incluyen dentro del alcance del SGI:

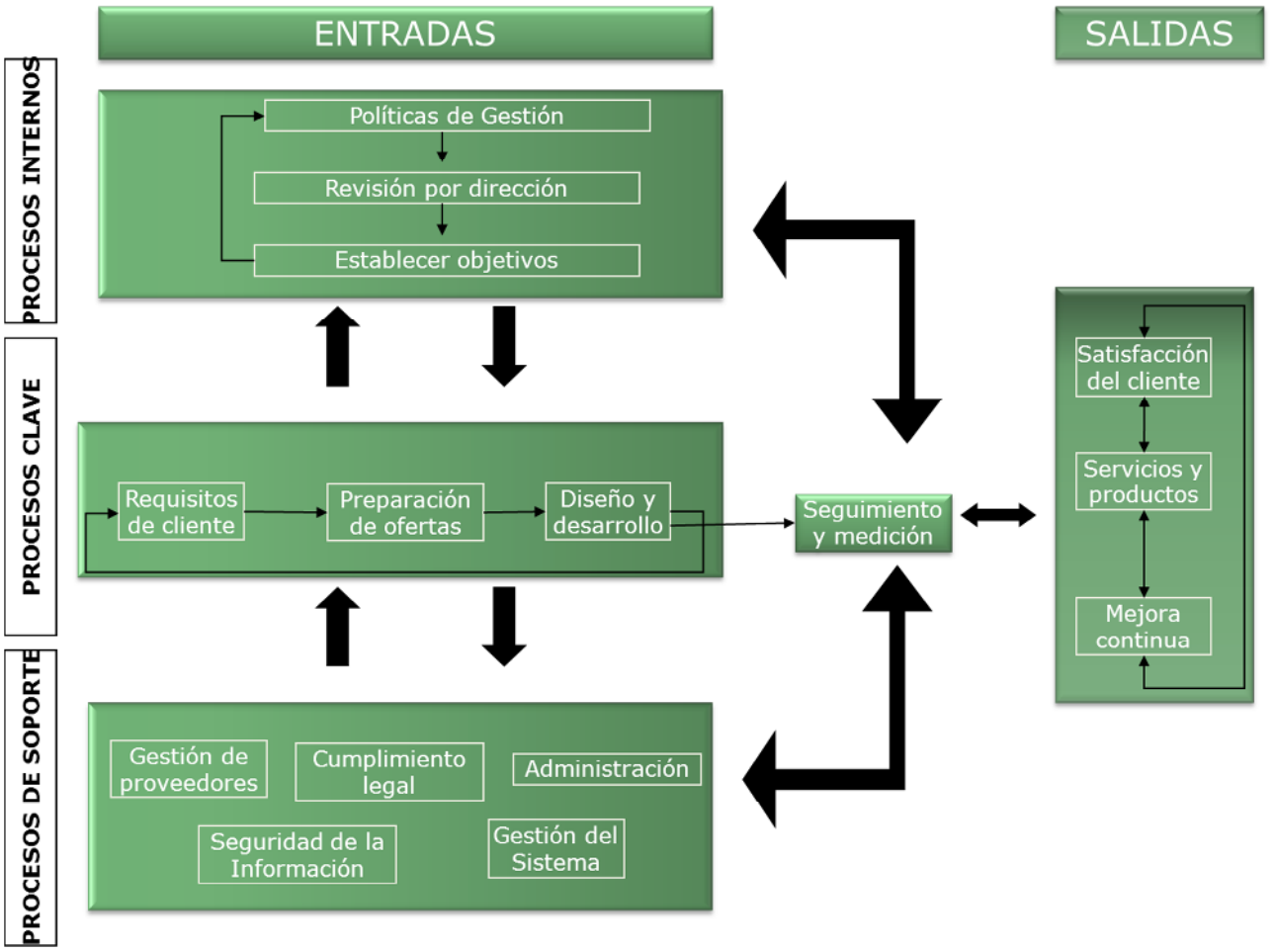
| Servicio | Sistema de tratamiento | Servicios subcontratados | Proveedores | Trabajadores | Clientes |
|---|---|---|---|---|---|
| Formación | [AP-02] Herramientas Ofimáticas<br>[AP-15] Windows Equipos Usuarios<br>[AP-07] Servidor web<br>[AP-08] SQL Server<br>[AP-09] Oracle<br>[AP-10] MySQL<br>[AP-11] POSTGRE-SQL<br>[AP-18] VMWare Horizon<br>[HW-01] Cluster Servidores Físicos<br>[HW-02] Servidores Virtuales<br>[HW-04] Cabina de discos de fibra<br>[HW-05] Cabina de discos i SCSI<br>[HW-06] Electrónica de red<br>[HW-08] Equipos Portátiles<br>[HW-09] Teléfonos Móviles | [CO-01] Fibra-Radioenlace<br>[CO-02] Fibra Alta Disponibilidad | Telefónica (Fibra Alta Disponibilidad)<br>Aire Networks (Fibra-Radioenlace | Departamento de Consultoría<br>Departamento de Soporte<br>Departamento comercial<br>Departamento de dirección de proyectos<br>Departamento TI | Administraciones publicas<br>Proveedores de AAPP |
| Desarrollo de aplicaciones | [AP-04] Eclipse Java<br>[AP-05] Power Builder<br>[AP-07] Servidor web<br>[AP-08] SQL Server<br>[AP-09] Oracle<br>[AP-10] MySQL<br>[AP-11] POSTGRE-SQL<br>[AP-14] KARAT | [CO-01] Fibra-Radioenlace<br>[CO-02] Fibra Alta Disponibilidad<br>[CO-08] VPN | Colt (Fibra Alta Disponibilidad)<br>Telefónica (Fibra Alta Disponibilidad)<br>Microsoft (Azure)<br>AZATY (Desarrollo)<br>ARION (Aplicaciones)<br>Duff and Phelps (Aplicaciones) | Departamento de desarrollo<br>Departamento comercial<br>Departamento de dirección de proyectos<br>Departamento TI | Administraciones publicas<br>Proveedores de AAPP |

| | | | | | |
|---|---|---|---|---|---|
| | [AP-15] Windows Equipos Usuarios<br>[AP-16] Windows Server<br>[AP-17] Linux<br>[AP-18] VMWare Horizon<br>[AP-19] VMWare VSPHERE<br>[AP-20] Gestor de Incidentes<br>[HW-01] Cluster Servidores Físicos<br>[HW-02] Servidores Virtuales<br>[HW-03] Servidor de Escritorios Virtuales<br>[HW-04] Cabina de discos de fibra<br>[HW-05] Cabina de discos i SCSI<br>[HW-06] Electrónica de red<br>[HW-07] Equipos de Usuario<br>[HW-11] Centralita Voz-IP | | Aire Networks( Fibra-Radioenlace | | |
| Cloud | [AP-16] Windows Server<br>[AP-17] Linux<br>[AP-08] SQL Server<br>[AP-09] Oracle<br>[AP-10] MySQL<br>[AP-11] POSTGRE-SQL<br>[AP-07] Servidor web | | Proveedor Cloud (Cloud para prestar servicio Nube)<br>Aire Networks (Fibra-Radioenlace<br>Telefónica (Fibra Alta Disponibilidad<br>UNIT4 (Cloud) | Departamento TI<br>Departamento comercial<br>Departamento de dirección de proyectos | Administraciones publicas<br>Proveedores de AAPP |

## 3.4 Sistema de gestión de la calidad y sus procesos

SPAI INNOVA tiene identificados y definidos los procesos principales relacionados con sus actividades y necesarios para el Sistema de Gestión de la Calidad, así como la secuencia e interacción de los mismos.

A continuación, se muestra el Mapa de Procesos donde quedan identificados los principales procesos para el Sistema de Gestión de la calidad y de forma global las interacciones de los mismos.




Igualmente, SPAI INNOVA tiene determinados los métodos y criterios para asegurar el funcionamiento efectivo y el control de los procesos, así como la disponibilidad de la información necesaria para apoyar el funcionamiento efectivo y el control de los mismos. Para ello, los procesos se miden, siguen y analizan, implantándose las acciones necesarias para lograr los resultados planificados y la mejora continua.

# 4. Liderazgo

## 4.1 Compromiso de la dirección

El presente Manual de Gestión es una línea de actuación clara, manifiesta y pública de SPAI INNOVA, por lo que la Dirección expresa su apoyo total a la misma y se compromete a mantener las directrices fijadas en el presente Documento. Asimismo, publicará y entregará a todos sus empleados y de la forma más apropiada las Políticas de Gestión, para que todos conozcan el objetivo establecido por el Comité de Gestión, las políticas, principios y normas adoptadas y su importancia para la seguridad de la empresa, las responsabilidades generales y específicas en materia de seguridad de cada miembro de la empresa y otras referencias a documentación que puedan ser útiles.

La Dirección está comprometida en la implantación, mantenimiento y mejora del Sistema de Gestión, por lo que:

- Se implica en comunicar a la organización la importancia de satisfacer los requisitos de los clientes, así como los legales y reglamentarios.
- Establece las Políticas de Calidad y Seguridad de la Información.
- Establece los Objetivos del sistema, así como la planificación, tal como se describe en el presente Manual.
- Lleva a cabo revisiones del Sistema de Gestión
- Se asegura la disponibilidad de los recursos.

## 4.2 Enfoque al cliente

La Dirección de SPAI INNOVA asegura que las necesidades y expectativas de los clientes están determinadas (incluyendo las obligaciones y requisitos legales y reglamentarios referidos a los servicios), son convertidas en requisitos y los requisitos son satisfechos con el propósito de lograr la satisfacción de los clientes y usuarios, tal y como se describe en los siguientes capítulos del presente Manual.

## 4.3 Requisitos de las Políticas del Sistema de Gestión Integrado

Las Políticas del Sistema de Gestión de SPAI INNOVA definida en los anexos del presente Manual, son establecidas por la Dirección, asegurando que:

- Son adecuadas al propósito de la organización y a la naturaleza de las actividades, productos o servicios.
- Incluyen de manera expresa el compromiso de satisfacer los requisitos de los clientes, de la mejora continua, de la protección de la información y de la entrega de servicios y productos.
- Incluyen de manera expresa un compromiso de cumplimiento con la legislación, la reglamentación aplicable y con otros requisitos que se estimen apropiados.
- Proporcionan un marco de referencia para establecer y revisar los objetivos del Sistema de Gestión.
- Son comunicadas y entendidas por los niveles apropiados de la organización;
- Son revisadas para conseguir una continua adecuación.
- La revisión de las Políticas se realizará de forma periódica, al menos en la Revisión por la Dirección del Sistema de Gestión (según lo establecido en el presente manual de gestión), y, de forma extraordinaria, siempre que la Dirección lo considere necesario.

Las Políticas de Gestión estarán documentadas y a disposición del público que la solicite y la Dirección se asegura que estas Políticas son entendidas, implantadas y mantenidas al día en la organización.

## 4.4 Política de Calidad

La Política de Calidad se recoge en el documento **SGI.01-01 Política de Calidad**.

## 4.5 Política de Seguridad de la Información

La política de Seguridad de la Información se recoge en el **SGI.01-02 Política de Seguridad**.

## 4.6 Roles, responsabilidades y autoridades en la organización

### 4.6.1 Comité de Gestión

El Comité de Gestión coordina la calidad y la seguridad de la información en SPAI INNOVA y está formado por:

- Responsable de la Información
- Responsable de los ficheros de LOPD
- Responsable del Servicio
- Responsable del Sistema de Gestión (Responsable de Calidad y Seguridad)
- Responsable del Sistema

El comité de Gestión se reunirá al menos una vez al año.

### 4.6.2 Roles: Funciones y Responsabilidades

Para gestionar de forma eficiente la Calidad y la Seguridad de la Información, cada uno de los departamentos de SPAI INNOVA deberá cumplir las normas y los procedimientos que correspondan. Todas estas normas y procedimientos estarán ratificados por la Dirección.

Los miembros del comité de gestión son los siguientes:

- **Responsable del Servicio, de la Información y de los ficheros de LOPD:** Director General.
- **Responsable del Sistema de Gestión:** Responsable del Departamento de Administración.
- **Responsable del Sistema:** Responsable del Departamento TI.

Las funciones y responsabilidades se detallan a continuación:

#### *4.6.2.1 Dirección*

La dirección de SPAI INNOVA se compromete a responder por las obligaciones inherentes a la seguridad de la información y proteger sus activos de información implementando las medidas de seguridad más apropiadas para conseguirlo de una manera efectiva con los recursos disponibles.

#### *4.6.2.2 Responsable de la Información*

Será el responsable de:

- Es el Propietario del Riesgo de toda la Información.
- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.

#### *4.6.2.3 Responsable de los Servicios*

Será el responsable de:

- Es el Propietario del Riesgo de todos los Servicios.
- Establecer los requisitos del servicio en materia de seguridad, incluyendo los requisitos de interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.

#### 4.6.2.4 Responsable del Sistema de Gestión

- Es el Responsable de Seguridad de la Información (incluidos los ficheros de LOPD).
- Es el Responsable de Calidad.
- Es el Propietario del Activo de todos los activos de la empresa en lo que respecta a la norma ISO 27001. En el inventario de activos podrá especificarse un Responsable del Activo, en el que el Propietario del Activo delega la toma de decisiones respecto a dicho activo.
- Es el responsable de la gestión y el mantenimiento del Sistema de Gestión.
- Asegura que los procesos del Sistema de Gestión están establecidos, implantados y mantenidos, de acuerdo con los requisitos de las normas aplicables.
- Informa a la Dirección del funcionamiento y eficacia del sistema para que ésta lleve a cabo la revisión, y como base para la mejora de la gestión de la empresa.
- Promueve el conocimiento de los requisitos de los clientes en materia de Calidad y Seguridad de la Información a todos los niveles de la organización.
- Colabora con la Dirección en la definición e implantación de las Políticas de Gestión de forma que sean fiel reflejo de la estrategia de la empresa.
- Planifica, programa y participa, cuando proceda, en las Auditorías internas y externas.
- Controla la elaboración, actualización, aprobación y distribución de la documentación de Gestión.
- Actúa como interlocutor con partes externas (clientes, proveedores, Administración, y demás partes interesadas) sobre aspectos del sistema de gestión.
- Controla la ejecución y eficacia de las acciones emprendidas para prevenir y gestionar No Conformidades, y valora las acciones a realizar tras la comunicación de una sugerencia de mejora.

#### 4.6.2.5 Responsable del Sistema

Será el responsable de:

- Es el Propietario del Riesgo de todos los activos, con excepción de los activos esenciales (Servicios e Información).
- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- La administración y gestión de las cuentas de los usuarios.
- Asegurarse de que sólo las personas autorizadas a tener acceso cuentan con él.

- Asegurarse de que los sistemas tienen los niveles de disponibilidad requeridos por la Organización.
- Incluir en los requisitos para nuevos desarrollos los aspectos de seguridad que apliquen.

#### 4.6.2.6 Propietario del Riesgo

El propietario del riesgo, asociado a uno o varios activos de información, tendrá las siguientes responsabilidades:

- Participar en el desarrollo del análisis y evaluación de riesgos realizada al menos con carácter anual
- Verificar la conformidad con los niveles de riesgo aceptable y colaborar en la aprobación de los mismos (que le afecten), así como la gestión de los riesgos asociado a los activos de información y los riesgos de los que es responsable.
- Asegurarse de que el personal le informa inmediatamente de cualquier violación de seguridad o mal uso de la información o los sistemas. El propietario del riesgo deberá informar a su vez al Responsable de Seguridad para tratar la incidencia.
- Informar al Responsable de Seguridad cuando ocurran cambios del personal, la organización, o del resto de los activos de información, que pueda implicar una revisión o actualización del análisis de riesgos, o de los permisos de acceso asignados.

#### 4.6.2.7 Propietario de Activos

El propietario de un activo, entendiendo por tal al responsable de dicho activo, tendrá las siguientes responsabilidades:

- Definir si el activo está afectado por la Ley de Protección de Datos y aplicarle en su caso, los procedimientos correspondientes.
- Asegurarse de que el software que se utiliza tiene licencia.
- Definir quiénes pueden tener acceso a la información, cómo y cuándo, de acuerdo con la clasificación de la información y la función a desempeñar.
- Asegurarse de que el activo cuenta con el mantenimiento adecuado
- Asegurarse de que el personal le informa inmediatamente de cualquier violación de seguridad o mal uso de la información o los sistemas. El propietario del activo deberá informar a su vez al Responsable de Seguridad para tratar la incidencia.
- Asegurarse de que la plantilla cuenta con la formación adecuada, conoce y comprende la Política de Seguridad y pone en práctica las directrices de seguridad.
- Asegurarse de que los soportes y equipos que contengan información son desechados según lo establecido.
- Implementar las medidas de seguridad necesarias en su área para evitar fraudes, robos o interrupción en los servicios.
- Mantener documentación actualizada de todas las funciones críticas para asegurar la continuidad de las operaciones en caso de que alguien no esté disponible.
- Informar al Responsable de Seguridad cuando ocurran cambios de personal que afecten al acceso de la información o los sistemas (cambio de función o departamento, causar baja en la empresa) para que se modifiquen apropiadamente los permisos de acceso.

- En los casos que aplique, asegurarse de que el personal y los contratistas tienen cláusulas de confidencialidad en sus contratos y son conscientes de sus responsabilidades.

#### *4.6.2.8 Personal*

- Conocer y comprender las Política de Calidad y Seguridad de la Información y los procedimientos que apliquen a su trabajo.
- Asegurarse de que sus acciones no producen ninguna infracción de seguridad.
- Informar al propietario del activo de cualquier incidencia de seguridad, real o sospechada, que detecte.

### 4.6.3 Procedimiento de Designación de Responsables

El Responsable del Sistema de Gestión será nombrado por Dirección a propuesta del Comité de Gestión.

El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

La Dirección designará también al Responsable del Sistema, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política.

### 4.6.4 Comunicación

SPAI INNOVA asegura la comunicación entre los diferentes niveles y funciones de la organización referente a los procesos del Sistema de Gestión y su efectividad. Dicha comunicación consiste en:

- Decidir y responder a las preocupaciones del personal en cuestiones relativas al Sistema de Gestión.
- Comunicación entre las diferentes áreas operativas de la organización, a fin de seguir la evolución de los procesos operativos del Sistema de Gestión y coordinar y unificar criterios de actuación.
- Comunicación a nivel de área, a fin de compartir entre sus miembros el conocimiento y las mejores prácticas adquiridas por la experiencia durante el desarrollo de los procesos correspondientes.
- Recibir, documentar y responder a las comunicaciones pertinentes de las partes interesadas de la organización, así como asegurar la comunicación interna entre los diversos niveles y funciones de la organización.
- Para asegurar dicha comunicación, se procede de la siguiente manera:
- El Responsable del Sistema de Gestión, mediante reuniones periódicas por departamentos con el personal, correo electrónico interno, etc., es responsable de dar a conocer las Políticas, los objetivos, las metas y la evolución del Sistema de Gestión en general y de la gestión de los requisitos del cliente en particular. Estas comunicaciones tendrán lugar siempre que dicho responsable lo considere oportuno y, en cualquier caso, tras las revisiones del sistema y las auditorías, con el fin de difundir los resultados y decisiones de carácter general y particulares derivadas de dichas actividades.

- Para asegurar que las informaciones puntuales de carácter urgente son comunicadas al personal afectado, la organización dispone herramientas de comunicación interna: correo electrónico, etc., que tienen un emisor y uno o varios destinatarios, y que sirven para comunicar informaciones referentes a, por ejemplo, cambios producidos en un pedido que ya había sido transmitido al personal afectado, incorporación de una nueva persona a la organización, recepción de una visita a la organización, etc.

Se ha definido un Plan de Comunicación, detallando las vías de comunicación entre las diferentes partes interesadas, en el documento **SGI.01-03 Plan de comunicación**.

## 4.7 Planificación

### 4.7.1 Información de entrada para la planificación

La Planificación de la Gestión se realiza para establecer el marco en el que se deben desarrollar y que debe regir las actuaciones de mejora de la empresa.

La Dirección SPAI INNOVA a través de las disposiciones del Sistema de Gestión establecido, identifica y planifica los recursos necesarios para:

- Alcanzar los Objetivos de Gestión.
- Garantizar que los cambios organizativos se efectúan de modo controlado y que el Sistema de Gestión mantiene su integridad durante estos cambios.
- La Planificación de la Gestión se lleva a cabo, de forma ordinaria en la Reunión de Revisión del Sistema, y de forma extraordinaria siempre que la Dirección así lo decida, quedando documentada, en cualquier caso, en las actas finales de dichas reuniones.

### 4.7.2 Resultado de la planificación. Planes de gestión

Como resultado de la planificación, la Dirección, de acuerdo con las Políticas definidas, establece los objetivos de la organización en materia de gestión para cada nivel relevante de la organización, que se recogen en el Plan de Gestión y el Plan de Seguridad, conteniendo:

- Los objetivos y metas aprobados,
- La asignación de responsabilidades en cada función y nivel relevante de la organización para el logro de los objetivos y metas,
- Los medios y el calendario en el tiempo en que han de ser alcanzados.

Los objetivos son medibles y se establecen (y revisan) considerando los requisitos de seguridad, las opciones tecnológicas y los requisitos financieros, operacionales y de la empresa, así como aquellos necesarios para satisfacer los requisitos para el producto/servicio y el compromiso de mejora continua, la opinión de los clientes y de las partes interesadas en general.

Para evaluar el grado de cumplimiento, y asegurar la adecuación y eficacia del sistema, los objetivos son revisados periódicamente, y las conclusiones de su seguimiento se tratan en las reuniones del Comité de Gestión, tal y como se detalla en el procedimiento aplicable. El seguimiento de los objetivos es documentado, registrado y aprobado por el Comité.

# 5. Apoyo

## 5.1 Recursos

El objeto de este capítulo es describir el modo en que SPAI INNOVA gestiona sus recursos en el marco de su Sistema de Gestión.

### 5.1.1 Provisión de recursos

SPAI INNOVA determina y proporciona, en el momento adecuado, los recursos necesarios para implantar y mejorar los procesos del Sistema de Gestión, y para lograr la satisfacción del cliente, la seguridad de la información y la entrega de los servicios.

### 5.1.2 Infraestructura

La Dirección está comprometida en la implantación, mantenimiento y mejora del Sistema de Gestión, por lo que identifica, proporciona y mantiene las instalaciones necesarias para lograr los objetivos de gestión incluyendo:

- Espacio de trabajo e instalaciones asociadas;
- Equipos, hardware y software;
- Servicios de apoyo.

La infraestructura necesaria para el desarrollo de las actividades de SPAI INNOVA se ha identificado en el análisis de riesgos.

### 5.1.3 Ambiente para la operación de los procesos

La Dirección está comprometida en la implantación, mantenimiento y mejora del Sistema de Gestión, por lo que se definen e implementan aquellos factores físicos y humanos del entorno de trabajo necesarios para lograr la conformidad del producto.

### 5.1.4 Recursos de seguimiento y medición

Dadas las características del propio producto/servicio que SPAI INNOVA suministra y los requisitos de medida a él asociados, así como del desarrollo de las actividades de seguimiento y medición que se realizan durante el proceso de realización del mismo, no se considera necesario el uso de equipos de seguimiento y medición, por lo que este apartado se tratará como una exclusión permitida. (Ver Exclusiones).

## 5.2 Personas

SPAI INNOVA tiene establecido, y mantiene al día, el procedimiento **PG.02 Gestión de Personal**, en donde se describen los criterios y responsabilidades asociadas para asegurar que aquel personal que tenga responsabilidades definidas en el Sistema de Gestión es competente basándose en la educación aplicable, formación, sensibilización, habilidades prácticas y experiencia.

La seguridad ligada al personal es fundamental para reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y servicios.

## 5.3 Comunicación

Se desarrollará un Plan de Comunicación en el que se establezcan las vías de comunicación que se producen entre las diferentes partes interesadas del sistema (ver documento **SGI.01-03 Plan de comunicación)**.

## 5.4 Información documentada

Para desarrollar este Sistema de Gestión se dispone de una estructura documental compuesta por:

- Manual de Gestión, el presente Manual: documento donde se establecen las bases del Sistema de Gestión de la empresa.
- Normativa, documentación donde se definen los usos permitidos o prohibidos en la organización.
- Procedimientos: describen las actividades requeridas para implementar el Sistema de Gestión para dar cumplimiento a requisitos exigidos por alguna de las normas aplicables.
- Instrucciones Técnicas: cualquier procedimiento que precise la intervención necesaria de determinados elementos y que requiera indicaciones específicas relacionadas con actividades críticas para satisfacer un objetivo se desarrollará en una instrucción técnica o de trabajo.

Los diferentes documentos tienen la extensión adecuada para asegurar el funcionamiento efectivo del Sistema y de la organización y el control de los procesos, en función de la complejidad del proceso, la interacción de los distintos procesos y la competencia del personal que intervenga.

### 5.4.1 Control de la documentación del Sistema de Gestión

SPAI INNOVA tiene establecido, y mantiene al día, el procedimiento **PG.01 Gestión del SGI** donde se describe cómo debe realizarse el control de la documentación del Sistema, donde se describen los criterios y responsabilidades asociadas al control de los documentos necesarios para el funcionamiento del Sistema de Gestión.

### 5.4.2 Documentación del Sistema

| ISO 9001 | ISO 27001 | ENS | Documento del Sistema |
|---|---|---|---|
| 4 Contexto de la organización | 4 Contexto de la organización | org.1 Política de seguridad | SGI.01 Manual de Gestión |
| 4.1 Comprensión de la organización y de su contexto | 4.1 Comprensión de la organización y de su contexto | | SGI.01 Manual de Gestión<br>SGI.01-01 Política de Calidad<br>SGI.01-02 Política de Seguridad<br>SGI.02 Categorización del Sistema<br>SGI.06 Análisis y Gestión de Riesgos<br>Gestión de riesgos |
| 4.2 Comprensión de las necesidades y expectativas de las partes interesadas | 4.2 Comprensión de las necesidades y expectativas de las partes interesadas | | SGI.01 Manual de Gestión |
| 4.3 Determinación del alcance del sistema de gestión de la calidad | 4.3 Determinación del alcance del sistema de gestión de seguridad de la información | | SGI.01 Manual de Gestión<br>SGI.03 Documento de aplicabilidad |
| 4.4 Sistema de gestión de la calidad y sus procesos | 4.4 Sistema de gestión de seguridad de la información | | SGI.01 Manual de Gestión<br>Políticas de Gestión |
| 5 Liderazgo | 5 Liderazgo | | SGI.01 Manual de Gestión |
| 5.1 Liderazgo y compromiso | 5.1 Liderazgo y compromiso | | SGI.01 Manual de Gestión<br>PG.01 Gestión del SGI |
| 5.2 Política | 5.2 Política | org.1 Política de seguridad | SGI.01-01 Política de Calidad<br>SGI.01-02 Política de Seguridad |
| 5.3 Roles, responsabilidades y autoridades en la organización | 5.3 Roles, responsabilidades y autoridades en la organización | org.1 Política de seguridad | SGI.01 Manual de Gestión |
| 6 Planificación | 6 Planificación | | SGI.02 Categorización del Sistema<br>SGI.03 Documento de aplicabilidad<br>SGI.06 Plan de Capacidad<br>SGI.06 Análisis y Gestión de Riesgos<br>PG.01 Gestión del SGI<br>PG.02 Gestión de Personal<br>PS.01 Análisis y Gestión de Riesgos |
| 6.1 Acciones para abordar riesgos y oportunidades | 6.1 Acciones para abordar riesgos y oportunidades | op.pl.1 Análisis de riesgos | SGI.04 Plan de Mejora<br>SGI.06 Análisis y Gestión de Riesgos<br>SGI.06-01 Informe de Análisis y Gestión de Riesgos |
| 6.2 Objetivos de la calidad y planificación para lograrlos | 6.2 Objetivos de seguridad de la información y planificación para su consecución | | SGI.04 Plan de Mejora |
| 6.3 Planificación de los cambios | | | SGI.02 Categorización del Sistema<br>SGI.06 Plan de Capacidad<br>SGI.06 Análisis y Gestión de Riesgos<br>SGI.06-01 Informe de Análisis y |

| ISO 9001 | ISO 27001 | ENS | Documento del Sistema |
|---|---|---|---|
| | | | Gestión de Riesgos<br>PG.02 Gestión de Personal<br>PG.05 Gestión de proveedores<br>PS.01 Análisis y Gestión de Riesgos<br>PS.02 Seguridad Lógica |
| 7 Apoyo | 7 Soporte | | |
| 7.1 Recursos | 7.1 Recursos | | SGI.02 Categorización del Sistema<br>SGI.06 Análisis y Gestión de Riesgos<br>SGI.06-01 Informe de Análisis y Gestión de Riesgos<br>PG.05 Gestión de proveedores |
| 7.2 Competencia | 7.2 Competencia | mp.per.4 Formación | PG.02 Gestión de Personal<br>SGI.04 Plan de Mejora |
| 7.3 Toma de conciencia | 7.3 Concienciación | mp.per.3 Concienciación | PG.02 Gestión de Personal<br>SGI.04 Plan de Mejora |
| 7.4 Comunicación | 7.4 Comunicación | | SGI.01 Manual de Gestión<br>SGI.01-03 Plan de comunicación |
| 7.5 Información documentada | 7.5 Información documentada | | SGI.01 Manual de Gestión<br>SGI.01-01 Política de Calidad<br>SGI.01-02 Política de Seguridad<br>PG.01 Gestión del SGI<br>PG.02 Gestión de Personal |
| 8 Operación | 8 Operación | | |
| 8.1 Planificación y control operacional | 8.1 Planificación y control operacional | | PG.04 Desarrollo de Software<br>PG.05 Gestión de proveedores<br>PC.01 Gestión Comercial<br>PC.02 Prestación de Servicios<br>PS.02 Seguridad Lógica<br>PS.03 Control de Accesos<br>PS.04 Gestión de Incidentes<br>PS.06 Seguridad Física<br>PS.08 Protección de Datos de Carácter Personal<br>PS.09 Protección de la Información |
| 8.2 Requisitos para los productos y servicios | | | SGI.01-03 Plan de comunicación<br>PG.04 Desarrollo de Software<br>PC.01 Gestión Comercial<br>PC.02 Prestación de Servicios |
| 8.3 Diseño y desarrollo de los productos y servicios | | | PG.04 Desarrollo de Software<br>PC.01 Gestión Comercial<br>PC.02 Prestación de Servicios |
| 8.4 Control de los procesos, productos y servicios suministrados externamente | | | PG.04 Desarrollo de Software<br>PC.01 Gestión Comercial<br>PC.02 Prestación de Servicios<br>PC.03 Satisfacción del cliente |
| 8.5 Producción y provisión del servicio | | | PG.04 Desarrollo de Software<br>PC.02 Prestación de Servicios |
| 8.6 Liberación de los productos y servicios | | | PG.04 Desarrollo de Software<br>PC.02 Prestación de Servicios |
| 8.7 Control de las salidas no conformes | | | PG.05 Gestión de proveedores<br>PC.03 Satisfacción del cliente |

| ISO 9001 | ISO 27001 | ENS | Documento del Sistema |
|---|---|---|---|
| | 8.2 Apreciación de los riesgos de seguridad de información | op.pl.1 Análisis de riesgos | SGI.06 Análisis y Gestión de Riesgos<br>SGI.06-01 Informe de Análisis y Gestión de Riesgos<br>PS.01 Análisis y Gestión de Riesgos |
| | 8.3 Tratamiento de los riesgos de seguridad de información | op.pl.1 Análisis de riesgos | SGI.06 Análisis y Gestión de Riesgos<br>SGI.06-01 Informe de Análisis y Gestión de Riesgos<br>PS.01 Análisis y Gestión de Riesgos |
| 9 Evaluación del desempeño | 9 Evaluación del desempeño | op.mon.2 Sistema de métricas | |
| 9.1 Seguimiento, medición, análisis y evaluación | 9.1 Seguimiento, medición, análisis y evaluación | op.mon.2 Sistema de métricas | PG.01 Gestión del SGI<br>PC.03 Satisfacción del cliente |
| 9.2 Auditoría interna | 9.2 Auditoría interna | | PG.01 Gestión del SGI |
| 9.3 Revisión por la dirección | 9.3 Revisión por la dirección | | PG.01 Gestión del SGI |
| 10 Mejora | 10 Mejora | | |
| 10.1 Generalidades | | | PG.01 Gestión del SGI<br>SGI.04 Plan de Mejora |
| 10.2 No conformidad y acción correctiva | 10.1 No conformidad y acciones correctivas | | PG.01 Gestión del SGI<br>PS.04 Gestión de Incidentes |
| 10.3 Mejora continua | 10.2 Mejora continua | | PG.01 Gestión del SGI |

# 6. Operación

El objeto de este capítulo es describir el modo en que SPAI INNOVA gestiona sus procesos asociados a la realización del producto/servicio en el contexto de su Sistema de Gestión.

## 6.1 Planificación y control operacional

SPAI INNOVA tiene identificados y planificados los procesos y subprocesos que son necesarios para realizar el producto y prestar el servicio requerido y aquellas actividades que están asociadas con los aspectos de gestión significativos identificados, así como sus secuencias e interacciones.

Durante la planificación de la realización del servicio se determinan cuando sea apropiado, los siguientes puntos:

- Los objetivos de gestión, y los requisitos para el servicio.
- La necesidad de establecer procesos, documentos y de proporcionar recursos específicos para la ejecución del producto o servicio.
- Las actividades requeridas de verificación, validación, seguimiento e inspección específicas para el producto / servicio, así como los criterios para la aceptación del mismo.
- Los registros que sean necesarios para proporcionar evidencia de que los procesos de realización y el producto resultante cumplen los requisitos.

El Resultado de esta planificación se presenta de forma adecuada para la metodología de operación de la organización, reflejada en los procedimientos **PC.03 Gestión Comercial** y **PC.04 Prestación de Servicios**, y las Instrucciones Técnicas Asociadas.

## 6.2 Requisitos para los productos y servicios

### 6.2.1 Comunicación con el Cliente

SPAI INNOVA determina e implementa disposiciones eficaces para la comunicación con los clientes relativas a:

- La información sobre los servicios y productos.
- Las consultas, contratos o atención de pedidos, incluyendo las modificaciones.
- La retroalimentación del cliente, incluyendo sus quejas.

La comunicación con el cliente se desarrolla presencialmente, por teléfono, o a través del correo electrónico, para dar y recibir información y consultas, y del correo (postal o electrónico) para el envío de documentación. A lo largo de los proyectos se mantienen reuniones periódicas. Las quejas y reclamaciones pueden llegar por cualquier medio: presencialmente, teléfono, fax, correo electrónico o correo convencional.

### 6.2.2 Determinación de los Requisitos

SPAI INNOVA determina:

- Los requisitos especificados por el cliente, incluyendo los requisitos del contrato, los requisitos para las actividades de entrega y las posteriores a la misma.
- Los requisitos no establecidos por el cliente, pero necesarios para el uso especificado o para el uso previsto, cuando sea conocido.
- Los requisitos legales y reglamentarios relacionados con el servicio.
- Cualquier requisito adicional determinado por la empresa.

### 6.2.3 Revisión de los Requisitos

Esta revisión se efectúa antes de que la empresa se comprometa a proporcionar un servicio al cliente (ofertas, presupuestos, aceptación de contratos, aceptación de cambios en los contratos), garantizando que:

- Están definidos los requisitos del servicio, con claridad y sin ambigüedades, indefiniciones o contradicciones, resolviendo cualquier anomalía que resulte en la definición de dichos requisitos.
- Están resueltas las diferencias existentes entre los requisitos del servicio y los expresados previamente, en ofertas, presupuestos, etc.
- La organización tiene la capacidad para cumplir con los requisitos definidos en todos sus ámbitos (calidad, plazo, medios y recursos necesarios).
- Se mantienen registros de los resultados de la revisión y de las acciones originadas por la misma.
- Se confirman y documentan los requisitos del cliente antes de la aceptación, cuando éste no proporcione una declaración documentada de los mismos.
- Cuando se producen cambios en los requisitos del servicio, se modifica la documentación relevante y se informe al personal afectado.

### 6.2.4 Diseño y Desarrollo

SPAI INNOVA planifica y controla el diseño y desarrollo de los productos y servicios, determina los elementos de entrada relacionados con los requisitos del producto y servicio, proporciona resultados, revisa, verifica, valida y controla los cambios del diseño y desarrollo según lo descrito en los procedimientos **PC.03 Gestión Comercial** y **PC.04 Prestación de Servicios**, y las Instrucciones Técnicas Asociadas.

## 6.3 Control de los procesos, productos y servicios suministrados externamente

SPAI INNOVA tiene establecido y mantiene al día el procedimiento **PG.05 Gestión de proveedores** donde se describen los criterios y responsabilidades asociadas a los procesos de compra, contratación, evaluación, reevaluación y selección de los suministradores y de los productos adquiridos.

## 6.4 Producción y provisión del servicio

### 6.4.1 Control de la producción y de la provisión

Todos los servicios y productos ofrecidos por SPAI INNOVA están sometidos a control mediante la definición e implantación, entre otros, de:

- Indicadores y objetivos.
- Reuniones del Comité de Gestión.
- No Conformidades.
- Quejas/Reclamaciones de clientes y usuarios.
- Registros de los procedimientos relevantes.

Los métodos de control de la producción se describen en los procedimientos **PC.03 Gestión Comercial** y **PC.04 Prestación de Servicios**, y las Instrucciones Técnicas Asociadas.

### 6.4.2 Identificación y trazabilidad

SPAI INNOVA identifica, cuando es apropiado, el producto a través de las operaciones de producción y de servicio, utilizando para ello los métodos adecuados en cada caso.

Los criterios y responsabilidades asociadas a la identificación están referenciados en los procedimientos correspondientes, cuando sean necesarios.

En el caso de que la trazabilidad constituya un requisito para el producto, los criterios y responsabilidades asociados a la identificación única del mismo y su correspondiente registro, quedarán recogidos en los procedimientos correspondientes, cuando sean necesarios.

### 6.4.3 Propiedades del cliente o proveedores externos

SPAI INNOVA no suele custodiar bienes de los clientes o proveedores externos, a excepción de información que sea necesaria para la prestación de los servicios, como Datos de Carácter Personal o datos para la realización de pruebas. El uso de estos datos está regido por las estipulaciones contractuales y por el procedimiento **PG.03 Cumplimiento Legal**.

Si en algún momento se produjese alguna incidencia asociada a propiedades del cliente, motivada por la actuación de SPAI INNOVA que comportase deterioro sobre las mismas, o inadecuación para su uso, éstas serían debidamente registradas en un Informe de No Conformidad, y comunicadas al cliente de acuerdo con el documento **SGI.01-03 Plan de comunicación**.

### 6.4.4 Preservación

Con el fin de evitar el deterioro de la calidad o la seguridad durante las operaciones que se realizan encaminadas a la prestación de los servicios, se ha establecido y documentado una sistemática de actuación en los procedimientos de seguridad que deben seguirse rigurosamente para garantizar que se preserva en todo momento la información con la que se trabaja.

### 6.4.5 Validación de los procesos de producción y de la prestación del servicio

SPAI INNOVA valida los procesos de producción y de la prestación del servicio según lo descrito en los procedimientos **PC.03 Gestión Comercial** y **PC.04 Prestación de Servicios**, y las Instrucciones Técnicas Asociadas.

### 6.4.6 Control del producto o servicio no conforme

A través de los procedimientos **PG.01 Gestión del SGI**, así como el **PC.02 Prestación de Servicios** y **PC.03 Satisfacción del cliente**, se asegura que el producto o servicio que no es conforme con los requisitos, es identificado y controlado para prevenir una utilización o entrega no intencionada, e identifica y controla las no conformidades para reducir cualquier impacto adverso producido.

### 6.4.7 Tratamiento de los riesgos de seguridad de información

Analizar los posibles riesgos y elaborar una estrategia para gestionarlos adecuadamente es primordial para SPAI INNOVA ya que, únicamente si se conoce el estado de seguridad con evidencias racionales, podrán tomarse las decisiones adecuadas para solucionar los riesgos que surjan.

Cada activo tiene una valoración en términos de disponibilidad, integridad, confidencialidad, Autenticidad y Trazabilidad, que se realizará con los criterios detallados en el documento **SGI.02 Categorización del Sistema**.

Para la realización del análisis de riesgos se ha utilizado la herramienta PILAR, la cual utiliza la metodología MAGERIT ("Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información ") elaborada por el Consejo Superior de Administración Electrónica.

El nivel de riesgo aceptable se documentará en el documento **SGI.06-01 Informe de Análisis y Gestión de Riesgos**.

MAGERIT cubre las actividades de análisis y tratamiento de riesgos facilitando una gestión de riesgos informada. La gestión de esos riesgos implicará seleccionar e implantar las medidas técnicas y de organización, necesarias para impedir, reducir o controlar los riesgos identificados, de forma que los perjuicios que puedan causar se eliminen o, si esto no es posible, se reduzcan lo máximo posible.

La gestión de riesgos es el proceso integral de tratamiento de los riesgos descubiertos durante el análisis.

#### *6.4.7.1 Proceso Análisis de Riesgos*

- Se identificarán los activos de SPAI INNOVA. Estos activos están expuestos a una serie de Amenazas que, cuando ocurren, degradan el valor del activo, causando un cierto Impacto.
- Se listará una serie de amenazas que afectan directa o indirectamente al activo. Si estimamos la probabilidad de la amenaza, podemos concluir el riesgo en el sistema, o la pérdida a la cual está expuesto.
- La degradación y la probabilidad califican la vulnerabilidad del sistema frente a una amenaza.

#### *6.4.7.2 Proceso de Gestión de Riesgos*

La gestión de esos riesgos implicará seleccionar e implantar las medidas técnicas y organizativas necesarias para impedir, reducir o controlar los riesgos identificados, de forma que los perjuicios que puedan causar se eliminen o, si esto no es posible, se reduzcan lo máximo posible.

Se puede elegir entre las siguientes estrategias para mitigar el riesgo:

- **Asumir el riesgo:** aceptar el riesgo y no implantar controles para su disminución o eliminación.
- **Evitar el riesgo:** eliminar la causa o la consecuencia de dicho riesgo.
- **Disminuir el riesgo:** limitar el riesgo implementando controles que disminuyan el impacto.
- **Transferir el riesgo:** pasar el riesgo a otros, como por ejemplo una aseguradora.

Se desplegarán salvaguardas para hacer frente a las amenazas.

Las salvaguardas mitigan los valores de impacto y riesgo dejándolos reducidos a unos valores residuales, que serán asumidos por el Responsable de la Información o el Responsable del Servicio.

El Documento de Aplicabilidad correspondiente especificará para cada control de la ISO 27001 o el ENS, si se aplica o no y el motivo por el que se toma esa decisión.

Los riesgos y los controles adoptados tras el análisis de los riesgos deben ser revisados anualmente, así como siempre que las circunstancias lo aconsejen. Esto se considerará una parte más de la gestión de la seguridad.

# 7. Evaluación del desempeño

## 7.1 Seguimiento, medición, análisis y evaluación

El objeto de este capítulo es describir el modo en que SPAI INNOVA gestiona sus procesos asociados a las medidas y evaluaciones del producto y/o servicio, la capacidad de los procesos, la satisfacción de los asociados, la seguridad de la información, la gestión medioambiental y, en definitiva, cualquier otro elemento que pudieran requerir las partes interesadas en el contexto de su Sistema de Gestión.

### 7.1.1 Seguimiento y medición de los procesos

El seguimiento de procesos se realiza mediante la comprobación de una lista de indicadores aprobados por Dirección, que incluye la frecuencia del seguimiento, responsable de medición y responsable del análisis de los datos.

En el caso de que se detecte una desviación respecto a los resultados planificados en los indicadores, el Responsable del Sistema de Gestión deberá abrir una no conformidad con objeto de analizar la causa de la desviación y la posible toma de acciones correctivas.

### 7.1.2 Seguimiento y medición del producto

En cada uno de los Procedimientos Operativos o Instrucciones de trabajo están establecido los criterios para el seguimiento y medición del producto resultante en la fase que se encuentre /servicio prestado, los criterios de aceptación (tolerancias, etc.) /o de actuación y los registros asociados.

### 7.1.3 Satisfacción del cliente

Se recaba esta información por el personal de SPAI INNOVA en los contactos con los clientes y usuarios y mediante la realización de encuestas a los receptores de determinados servicios y productos, en las que se les consulta sobre el grado de satisfacción alcanzado con los mismos, según se detalla en el procedimiento **PC.03 Satisfacción del cliente**.

### 7.1.4 Análisis y evaluación

SPAI INNOVA determina, recopila y analiza los datos apropiados para demostrar la idoneidad y la eficacia del Sistema de Gestión y para evaluar dónde puede realizarse la mejora continua de dicha eficacia, incluyendo los datos generados del resultado del seguimiento y medición y de cualesquiera otras fuentes.

El análisis de datos proporciona información sobre:

- La mejora de la calidad.
- La mejora de la rentabilidad de la empresa.
- Las incidencias generadas por los proveedores.
- Las características y tendencias de los procesos y de los productos/servicios, incluyendo acciones correctivas y preventivas.
- La satisfacción del cliente.

## 7.2 Auditoría interna

El propósito del presente capítulo es describir los procedimientos y actividades para planificar y llevar a cabo auditorías internas del Sistema de Gestión.

El Responsable del Sistema de Gestión revisará el Manual y las Políticas anualmente o cuando haya cambios significativos que así lo aconsejen, y la someterá de nuevo a aprobación por la Dirección. Las revisiones comprobarán la efectividad de las políticas, valorando el origen, número e impacto de las incidencias registradas desde la puesta en marcha del SGI, el coste e impacto de los controles establecidos y las medidas de mejora adoptadas en la empresa y los efectos de los cambios tecnológicos. Estas revisiones incluirán los sistemas de información, a los proveedores de sistemas, a los propietarios de información y de activos de información, a los usuarios y también a la Dirección.

El Comité de Dirección de SPAI INNOVA será, en definitiva, el encargado de aprobar las modificaciones necesarias en el texto cuando se produzca un cambio que afecte a los activos evaluados originalmente y a las situaciones de riesgo establecidas.

El Sistema de Gestión Integrado se auditará según un plan de auditorías desarrollado por el Responsable del Sistema de Gestión. El SGI se auditará completamente cada tres años.

Este punto se desarrollará en los procedimientos de **PG.01 Gestión del SGI**.

### 7.3 Revisión por la Dirección

La Dirección realiza revisiones de su Sistema de Gestión Integrado para asegurar su continua consistencia, adecuación y eficiencia. La revisión efectuada evalúa la necesidad de realizar cambios en el Sistema de Gestión, incluyendo la política, objetivos y otros elementos a la vista de los resultados de la auditoría del sistema, las circunstancias cambiantes y el compromiso de mejora continua. Todo esto se recoge en el Procedimiento **PG.01 Gestión del SGI.**

Con los resultados de la Revisión se establece además el Plan de Gestión, que incluye los objetivos y metas para el siguiente ciclo de mejora.

## 8. Mejora continua

SPAI INNOVA está comprometido con la mejora continua del Sistema de Gestión. Para ello se apoya en las Políticas, los objetivos, los resultados de las auditorías internas, el análisis de datos, acciones correctivas y preventivas y la revisión por la dirección para facilitar la mejora continua.

### 8.1 Acción correctiva y preventiva

Con el fin de establecer un proceso para reducir o eliminar las causas de no conformidad al objeto de prevenir su reaparición, se ha establecido, y mantiene al día el procedimiento **PG.01 Gestión del SGI**, en donde se definen los criterios y responsabilidades asociados a:

- la identificación de las no conformidades, reales o potenciales (incluyendo las reclamaciones de los asociados y partes interesadas)
- la determinación de las causas de no conformidad
- la evaluación de la necesidad de adoptar acciones para asegurar que las no conformidades no vuelven a aparecer
- el registro de los resultados de las acciones adoptadas
- la revisión de que la acción correctiva/preventiva adoptada es eficaz.