

# POLÍTICA DE SEGURIDAD



## **1. INTRODUCCIÓN**

Es para ASTIVIA una prioridad, salvaguardar la seguridad de los datos de los clientes, ya sean de carácter personal o no. Es por ello que ASTIVIA publica y difunde este documento entre todos sus cliente para que sean conocedores de las medidas de seguridad que aplica, así como las políticas que ASTIVIA tiene por bandera e integra en su planificación estratégica.

Prueba de ello, es que ASTIVIA posee un sistema de gestión certificado bajo la norma ISO 9001, que obliga a salvaguardar los intereses del cliente, así como la norma ISO 27001, de seguridad de la información, que certifica que el sistema de gestión posee las medidas de seguridad que hacen posible que nuestros clientes se sientan seguros y confíen en que ISOTools, es una herramienta que no deja lugar a dudas para confiar en ella como elemento importante que garantiza la privacidad de los datos.

## **2. POLÍTICA DE SEGURIDAD**

ASTIVIA adquiere con sus clientes la responsabilidad de ofrecer servicios con un nivel adecuado de confianza, asegurando el cumplimiento de la legislación vigente.

Para alcanzar el citado nivel de confianza en el desarrollo de su actividad la Dirección de ASTIVIA es consciente de la importancia de aplicar una adecuada gestión de la seguridad de la información en sus tres dimensiones: confidencialidad, integridad y disponibilidad.

Los objetivos estratégicos del Sistema de Gestión de Seguridad de la Información que ASTIVIA se ha marcado son los siguientes:

- Desarrollar soluciones web libres de vulnerabilidades y dotadas de las medidas de seguridad acordes a las necesidades del cliente.
- Garantizar la disponibilidad y confidencialidad en el acceso remoto de sus clientes a las aplicaciones a través de la red.
- Dotar de las medidas necesarias para asegurar la integridad, disponibilidad y confidencialidad de la información de los clientes.

Mediante la presente política de seguridad, la Dirección adquiere el compromiso de asegurar la dotación de los recursos necesarios para implantar y mantener el proceso de mejora continua de la gestión de la seguridad con el fin de alcanzar los objetivos estratégicos. Asimismo, se compromete a proveer aquellos procesos de comunicación que aseguren la distribución de esta política.

## **3. MEDIDAS DE SEGURIDAD**

En virtud de los compromisos adquiridos por ASTIVIA, y prueba de ello es la certificación en ISO 27001, se recogen aquí las principales medidas de seguridad que se aplican, con el objeto de informarle de las garantías de seguridad de ASTIVIA.

### **3.1. Aspectos de la seguridad de ISOTools**

ASTIVIA basa la seguridad de los datos en los principios de:

- **Disponibilidad:** Asegura que los usuarios autorizados podrán acceder cuando lo requieran a la información
- **Integridad:** Garantiza la exactitud y completitud de la información y los métodos utilizados en su procesamiento
- **Confidencialidad:** Asegura que la información es accesible sólo por aquellos usuarios autorizados con un nivel de acceso determinado.

Además, identifica las amenazas entendiendo estas como: *“Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos”*, utilizado para el catálogo las amenazas propuestas por la norma ISO 27.001, además de otras propias.

### 3.2. Elementos de la seguridad de ISOTools

ASTIVIA, asegura que los datos del cliente se encuentran seguros, y por ello, en este punto detalla los elementos principales que permiten asegurarlo.

- Funciones y obligaciones del personal: El personal de administración y operación de sistemas de ASTIVIA ha recibido y aceptado un compromiso de confidencialidad, así como la formación necesaria recogida en el Manual de Acogida, para saber mantener los datos de una manera correcta que asegure la privacidad de los mismos. Además, toda la documentación del Sistema de Gestión de la Seguridad de la Información, ha sido difundida de manera correcta dependiendo de las responsabilidades de los recursos.
- Registro de incidencias: ASTIVIA comunicará las incidencias ocurridas que puedan afectar a la información del cliente, indicando el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se le comunica y los efectos que se hubiera derivado de la misma. Estas Incidencias están bajo el control del SGSI, lo cual asegura que el correcto tratamiento es revisado en las auditorías de terceras partes.
- Identificación y autenticación: ASTIVIA ha optado por dotar de medidas de seguridad que garantizan la correcta identificación y autenticación de los usuarios para acceder a la información, existiendo mecanismos que aseguran la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado. Debido a que el acceso se desarrolla a través de contraseñas, ISOTools incorpora una herramienta que asegura que el nivel de seguridad de contraseñas es el adecuado. Además, ASTIVIA tiene implantado y mantiene al día un procedimiento de asignación, distribución y almacenamiento de contraseñas internas que garantiza su confidencialidad e integridad.
- Control de acceso: Los empleados de ASTIVIA no tendrán acceso a los datos del cliente, siendo este acceso autorizado únicamente a los recursos necesarios para el desempeño de sus funciones de administración y operación con expreso consentimiento del cliente. El control de acceso se lleva a cabo bajo dominio seguro https, contando con certificado de VeriSign Secured®



- Control de acceso físico: Las dependencias donde se alberga la infraestructura que presta el servicio están equipadas con control de acceso y sistemas de monitorización y control para garantizar que únicamente accede a las mismas el personal autorizado.
- Gestión de soportes: ASTIVIA, tiene implantado y mantiene al día, un procedimiento de gestión de soportes e infraestructuras, contando con un inventario de los centros donde el Cliente puede alojar información o resultantes de la realización de copias de respaldo.
- Copias de respaldo y recuperación: ASTIVIA posee una política de backup y una dinámica de realizar copias de seguridad de la información del Cliente según se detalla en el procedimiento de backup. Realizándose copias de seguridad diariamente.
- Auditoría: ASTIVIA proporcionará información necesaria al Cliente para la realización de auditorías por parte del personal propio o por un tercero, siempre y cuando ello no suponga distorsiones en el desarrollo de ASTICIA en el desarrollo de sus actividad ordinaria, y tales informaciones o documentos tengan relación con los trabajos o servicios encargados y con los ficheros de los que fuera titular el Cliente.

### **3.3. Documento de seguridad**

El Reglamento de medidas de seguridad RD 994/99, establece que el responsable del fichero está obligado a la creación de un documento de seguridad con la descripción del fichero, funciones y obligaciones del personal, estructura del fichero, y otra serie de datos relativos al fichero, ASTIVIA proporcionará bajo demanda del cliente, los datos técnicos necesarios para la realización de ese documento de seguridad por su parte.

A la hora de declarar el citado documento de seguridad, conviene seguir la guía que la Agencia de protección de datos pone a disposición del público en general.

## **4. INFORMACIÓN SOBRE LA LOPD**

En lo referente a cumplimiento legal en materia de datos de carácter personal, y en virtud del uso de ISOTools para almacenar algunos datos de carácter personal, le proporcionamos la siguiente información relacionada con el servicio que tiene contratado con ASTIVIA.

La actual Ley Orgánica de Protección de Datos de Carácter personal, tiene por objeto “garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar”. Debemos mencionar, así mismo, el Real Decreto 1720/2007, que reglamenta a la LOPD, en ella encontramos que “tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos

fundamentales de las personas físicas, y especialmente de su honor e intimidad personal.

En el presente documento, ASTIVIA le comunica que si usa su herramienta de gestión informática ISOTools, para alojar datos de carácter personal es responsabilidad del tratamiento de los datos el propio Cliente, así mismo, la responsabilidad de darlos de alta en el Registro Nacional de Datos de Carácter Personal, es obligatorio por parte del Responsable del Fichero, sin que ASTIVIA interfiera en este proceso, ya que únicamente usará ISOTools como herramienta gestora de los datos. Si necesita más información al respecto, puede consultar en la página web de la Agencia Española de Protección de Datos [www.agpd.es](http://www.agpd.es).