

# Sistema de protección de datos implementado por ASOCIACIÓN AMANIXER

## 1. Registro de Actividades de Tratamiento:

---

### NOMBRE DEL FICHERO

PERSONAL

PERSONAL CON PREVENCIÓN

COMUNICACIÓN - WEB COMERCIAL - REDES

ATENCION AL LA USUARIA

GESTIÓN DE ASOCIADAS

### CLÍNICA

(El Registro de Actividades de Tratamiento, con información descriptiva adicional, forma parte de la documentación y protocolos de cumplimiento de ASOCIACIÓN AMANIXER con respecto de la legislación vigente en materia de protección de datos personales).

## 2. Existencia de documento de seguridad de tratamiento de datos personales:

---

La entidad cuenta con un documento de seguridad regulador del tratamiento automatizado de los datos personales obligatorio para todos los usuarios de los sistemas informativos.

El sistema de protección de datos será revisado y auditado periódicamente. La empresa colaboradora en esta tarea es la mercantil MA.SER LEGAL CONSULTORES S.L.P. con la que ASOCIACIÓN AMANIXER tiene contratado servicio de mantenimiento, seguimiento, consultoría y tramitación de obligaciones desprendidas del RGPD-UE y de la legislación vigente en materia de protección de datos personales.

Todos los usuarios de medios informativos serán informados anualmente acerca de sus obligaciones y responsabilidades respecto de los requisitos establecidos por el RGPD-UE y la Ley vigente de Protección de Datos, así como los establecidos por los reglamentos que la desarrollen.

### 3. Medidas de seguridad aplicadas:

---

El sistema de protección de datos ASOCIACIÓN AMANIXER establece una serie de estándares de seguridad de tipo organizativo y técnico-informático que deben ser cumplidos en el tratamiento de información de carácter personal. Entre otros, se resumen los siguientes:

**ACCESO LÓGICO AL TRATAMIENTO DE DATOS AUTOMATIZADO.** Sólo los usuarios autorizados por DIRECCIÓN deben acceder a los sistemas informáticos. Existe una relación actualizada de los usuarios que poseen permisos de acceso y tratamiento de la información. Dicha relación mantiene concordancia con los permisos establecidos a nivel informático.

**ACCESO LÓGICO AL TRATAMIENTO DE DATOS NO AUTOMATIZADO.** Sólo los usuarios autorizados por el documento de seguridad deben acceder a los sistemas informativos documentales. Existe una relación actualizada de los usuarios que poseen permisos de acceso y tratamiento de la información, aplicándose para ello medidas de seguridad en el acceso a los archivos documentales, los cuales se sitúan en zonas de acceso restringido al personal autorizado.

**ACCESO FÍSICO A LAS INSTALACIONES** en las cuales se encuentran los sistemas informáticos y los archivos de expedientes en papel. Sólo el personal autorizado por el documento de seguridad LOPD cuenta con autorización y permisos para el acceso a estas instalaciones.

**DESTRUCCIÓN DE SOPORTES.** Está prohibido el uso de soportes externos de grabación de información. Igualmente, no existe la posibilidad de uso de papel borrador por cara B. La entidad cuenta con un número adecuado de destructoras de papel de gran capacidad, las cuales están colocadas estratégicamente para facilitar la destrucción de documentos confidenciales por los usuarios autorizados. La situación de las destructoras en los locales de la entidad, así como la eficacia de las mismas, constituye un punto esencial en las auditorías de seguridad informática que la entidad lleva a cabo periódicamente.

**SALVAGUARDA DE FICHEROS.** La información automatizada cuenta con copia de salvaguarda diaria. Dicha copia de seguridad se almacena cifrada en centro alejado del centro de proceso de datos, lo cual garantiza su recuperación en caso de desastre.

Para más detalle acerca de las medidas de seguridad aplicadas por ASOCIACIÓN AMANIXER en cumplimiento de las exigencias normativas en materia de protección de datos personales, solicitar acceso a la parte procedimental de los documentos y protocolos de seguridad descritos en el punto 2.



# MEDIDAS TÉCNICAS Y ORGANIZATIVAS IMPLEMENTADAS POR

## ASOCIACIÓN AMANIXER

ESQUEMA DE MEDIDAS DE SEGURIDAD	EL RESPONSABLE DE TRATAMIENTO DE SE COMPROMETE AL CUMPLIMIENTO DE LAS SIGUIENTES MEDIDAS DE SEGURIDAD
<i>CONTROL DE ACCESOS FÍSICOS AL CENTRO DE PROCESO DE DATOS (SERVIDORES)</i>	Sito en zona de acceso restringido Emisión de llaves Cierre de puertas Revisión regular de permisos de acceso permanentes Sistema de control de acceso (lector de identificadores, tarjeta magnética, tarjeta con chip) Personal de seguridad, conserjes
<i>GESTIÓN DE SOPORTES (inventario actualizado de soportes)</i>	Inventario de soportes que contienen datos personales Inventario de soportes que tratan datos personales <i>(debe incluirse servidores propios y externos, computadoras, portátiles, discos externos, tarjetas de memoria, teléfonos móviles, etc.)</i>
<i>GESTIÓN DE SOPORTES (borrado seguro de soportes)</i>	Para reutilización y desecho, sistema de borrado de soportes implicados en el tratamiento redactado en procedimiento.
<i>CONTROL DE ACCESOS LÓGICOS A SISTEMA OPERATIVO Y APLICACIONES (Administradores y usuarios, segregación de funciones)</i>	Existencia de una política efectiva de gestión de permisos.
<i>CONTROL DE ACCESOS LÓGICOS A SISTEMAS OPERATIVOS Y APLICACIONES (políticas de contraseñas)</i>	Las pantallas en las zonas de acceso público están fuera de área visual del público. El proceso de asignación de contraseñas está recogido en un Procedimiento de Seguridad. Las contraseñas que validan los usuarios autorizados son personales e intransferibles. La contraseña requiere mínimo 8 caracteres. La contraseña exige al menos un número y una letra. La contraseña pide al menos una mayúscula y una minúscula. La contraseña contiene al menos un signo no alfanumérico. Las contraseñas de usuarios se renuevan al menos una vez al año. El sistema, al intento nº 3 no autorizado, bloquea el usuario.
<i>COPIA DE SEGURIDAD</i>	Copia de seguridad del volumen completo de los datos personales tratados. Copia de seguridad almacenada lugar seguro de acceso restringido. Copia de seguridad diaria. Copia de seguridad verificada en su contenido.
<i>PRUEBAS DE RESTAURACIÓN DE COPIAS PLANEADAS</i>	Copia de seguridad verificada periódicamente con simulacros de restauración.
<i>ELIMINACIÓN DE FICHEROS TEMPORALES</i>	Borrado periódico de las carpetas de intercambio temporales mediante script. Borrado programado de los ficheros con carácter temporal en los soportes que tratan datos personales.

# MEDIDAS TÉCNICAS Y ORGANIZATIVAS IMPLEMENTADAS POR

## ASOCIACIÓN AMANIXER

ESQUEMA DE MEDIDAS DE SEGURIDAD	EL RESPONSABLE DE TRATAMIENTO DE SE COMPROMETE AL CUMPLIMIENTO DE LAS SIGUIENTES MEDIDAS DE SEGURIDAD
<i>GESTIÓN DE INCIDENCIAS (registro y gestión de brechas de seguridad)</i>	Responsable encargado de gestión de incidencias (interno o externo). Procedimiento de gestión de incidencias: comunicación a responsables, registro, seguimiento e informe de resolución de incidencias.
<i>GESTIÓN DE INCIDENCIAS (notificación de brechas de seguridad)</i>	Procedimiento de notificación de brechas de seguridad de acuerdo con lo previsto en el RGPD.
<i>GESTIÓN DE VULNERABILIDADES DE SISTEMAS Y APLICACIONES</i>	Procedimiento de detección de vulnerabilidades de seguridad en sistemas de información informatizados. Procedimiento de detección de vulnerabilidades de seguridad en sistemas de información no informatizados.
<i>AUDITORÍA TÉCNICA DE SISTEMAS</i>	Auditorías anuales de seguridad de la información para datos informatizados. Auditorías anuales de seguridad de la información para datos no informatizados.
<i>CIFRADO EN EQUIPOS Y DISPOSITIVOS MÓVILES</i>	Garantía de contenido cifrado de equipos y dispositivos que contienen datos personales con ubicación itinerante y movilidad fuera de las instalaciones del encargado de tratamiento.
<i>SEGURIDAD EN ENTORNOS DE DESARROLLO Y TEST</i>	En los entornos de prueba y test existen datos personales generalmente no reales, pero se aplican las mismas medidas de seguridad que en el entorno de explotación.
<i>SEUDONIMIZACIÓN / ANONIMIZACIÓN DE DATOS PERSONALES</i>	Sustitución irreversible de identificativo de datos personales de los registros para su uso ulterior en otras actividades de tratamiento. Despojados de la información personal su uso está fuera de las obligaciones del RGPD. Reemplazo de campos de información personal dentro de un registro de datos por uno o más identificadores artificiales o pseudónimos, garantizando que cada registro de datos sea menos identificable mientras se queda apto para análisis de datos y procesamiento de datos.
<i>SEGREGACIÓN DE DATOS PERSONALES</i>	Aplicación de medidas para el tratamiento separado (almacenaje, modificación, eliminación, transferencia) de datos para fines distintos de los que son objeto.
<i>PRIVACIDAD DESDE EL DISEÑO</i>	Procedimiento de garantía de aplicación de la política de privacidad desde el diseño en los sistemas de información utilizados para el tratamiento de datos personales.
<i>INVENTARIO DE TRATAMIENTOS</i>	Existencia de un Registro de Actividades de Tratamiento conforme a lo exigido por el RGPD.
<i>DIFUSIÓN CORPORATIVA DE NORMAS DE CUMPLIMIENTO DEL RGPD</i>	Difusión de normas de confidencialidad entre empleados. Cursos informativos para los empleados con mayor implicación en el cumplimiento del RGPD.
<i>CONTROL DE SERVICIOS SUBCONTRATADOS</i>	Solicitud de autorización del Responsable de Tratamiento para la subcontratación de servicios que supongan un tratamiento de datos personales. Control de garantía de cumplimiento de las obligaciones RGPD por parte de la subcontrata.
<i>TUTELA EFECTIVA DE LOS DERECHOS DEL AFECTADO</i>	Comunicación inmediata al responsable de tratamiento de las solicitudes de ejercicio de los derechos.

<i>FIRMADO POR EL RESPONSABLE DE TRATAMIENTO</i>	<i>FIRMA</i>
ASOCIACIÓN AMANIXER	