REGISTRO DE ACTIVIDADES DE PLANIGER, S.A. (RAT) COMO RESPONSABLE DE TRATAMIENTO

Registro de Actividades de Tratamiento elaborados de acuerdo con los requisitos del art. 30 REGLAMENTO (UE) 2016/679 GENERAL DE DATOS PERSONALES (RGPD)

ÍNDICE

1. CONTROL DE CAMBIOS DEL REGISTRO DE ACTIVIDADES DE TRATAMIENTO

TRATAMIENTO MODIFICADO	MOTIVO DE MODIFICACIÓN	FECHA DE MODIFICACIÓN
Revisión general	Post-auditoría 2019	20/05/2019
Revisión tratamiento "Residentes" (ahora "usuarios de servicios asistenciales"	Ajustes relativos a la historia clínica	05/11/2019
Revisión general	Post-auditoría RGPD 2020	24/03/2021
Revisión general	Actualización tratamientos e inclusión de contenedores de información.	18/07/2022
Revisión general	Post- auditoria RGPD 2024	23/12/2024
Actualización del apartado de Marketing	Inclusión de nuevos destinatarios	02/06/2025

2. IDENTIFICACIÓN DEL RESPONSABLE DE TRATAMIENTO/

PLANIGER, S.A.	
DOMICILIO SOCIAL	C/ Infanta Mercedes 90, 2ª, 28020, Madrid.
DATOS DE CONTACTO	info@amavir.es / +34917451210
INSCRIPCIÓN REGISTRAL	Registro Mercantil de Madrid; Tomo 17.161, Folio 125, Hoja número M-293967
N.I.F.	NIF A-83151977
DELEGADO DE PROTECCIÓN DE DATOS (DPO)	SECURE & IT (B-85921625) C/ Chile, 8, Oficina 105, 28290 Las Rozas (Madrid) dpo@amavir.es

3. USUARIOS DE SERVICIOS ASISTENCIALES

USUARIOS DE SERVICIOS ASISTENCIALES (MIXTO)	
ENTIDAD RESPONSABLE	PLANIGER, S.A.
BREVE DESCRIPCIÓN	Tratamientos referidos a las personas titulares de las plazas residenciales y usuarios de otros servicios asistenciales (centros de día, etc.).
CATEGORÍAS DE DATOS	• **Datos identificativos básicos** (nombre y apellidos, DNI/NIE, nº Seguridad Social). • **Datos relativos a la salud (Historia Clínica)**: Documentación relativa a la hoja clínico-estadística; autorización de ingreso; informe de urgencia; anamnesis y la exploración física; evolución; órdenes médicas; hoja de interconsulta; informes de exploraciones complementarias; informe de anestesia; informe de quirófano; informe de anatomía patológica; evolución y planificación de cuidados de enfermería; aplicación terapéutica de enfermería; gráfico de constantes; informe clínico de alta. • **Datos contenidos en el PAI** (Programa de Actuación Individualizada): Características personales del residente desde el punto de vista médico, psicológico, funcional, cognitivo y social; necesidades dietéticas. • **Datos económicos y bancarios** • **Imagen personal** (ver tratamiento “Banco de imágenes”)
FINALIDAD Y BASE DE LEGITIMACIÓN	• Prestación de servicio residencial y asistencia geriátrica integral. Base de legitimación: Ejecución de contrato de prestación de servicios (art. 6.1 b) RGPD).

	• Servicio de recogida de medicamentos en farmacias. Base de legitimación: Existencia de consentimiento expreso del residente o de su representante legal/voluntario (art. 6.1 a) RGPD). • Gestión económica (cobros). Base de legitimación: Ejecución de contrato de prestación de servicios (art. 6.1 b) RGPD). • Gestión administrativa, fiscal y contable. Base de legitimación: Cumplimiento de obligaciones legales (art. 6.1 c) RGPD).
CATEGORÍAS DE INTERESADOS	• Residentes y usuarios de otros servicios asistenciales (centros de día, etc.).
CATEGORÍAS DE DESTINATARIOS	• Prestadores de servicios auxiliares externos con acceso a datos personales tales como prestadores de servicios IT. • Cesionarios tales como hospitales, servicio ambulancia, órganos de la Administración Pública, Juzgados, Fiscalía, Abogados y Procuradores, entidades bancarias, farmacias. • D.G. Servicios Sociales.
TRANSFERENCIAS INTERNACIONALES/DESTINO	NO
CONTENEDORES	Teléfono corporativo, Salesforce, Office 365, Servidor de ficheros, WhatsApp, OneDrive, intranet, SAP, RRSS (LinkedIn, Facebook, Instagram…), Centraliza virtual, Portátil, Sobremesa, IPADs, Pendrives, Sophon, Elastic, Mistery client.
PLAZO DE SUPRESIÓN	• Las historias clínicas y PAI se conservarán durante veinte años desde la extinción por cualquier causa de la relación contractual de prestación de servicios asistenciales.

	• Con carácter general, los documentos contractuales y los documentos de carácter económico relativos a cobros/pagos se conservarán durante seis años tras la extinción de la relación contractual de prestación de servicios asistenciales por cualquier causa. Este plazo se prorrogará por el tiempo necesario en los casos en los que esté vigente el plazo de prescripción de acciones por responsabilidad civil contractual (cinco años).
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Protección de documentación en papel mediante armarios bajo llave • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. La encriptación se aplicará a todas aquellas comunicaciones electrónicas que contengan datos personales relativos a la salud, especialmente en el caso de los PAIs y las historias clínicas, así como a los dispositivos electrónicos portátiles que contengan ese tipo de datos. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

4. REPRESENTANTES VOLUNTARIOS/LEGALES Y PERSONAS DE CONTACTO DE LOS RESIDENTES

REPRESENTANTES VOLUNTARIOS/LEGALES Y PERSONAS DE CONTACTO DE LOS RESIDENTES (MIXTO)	
ENTIDAD RESPONSABLE	PLANIGER, S.A.
BREVE DESCRIPCIÓN	Tratamientos referidos a los representantes y personas de contacto de los residentes.
CATEGORÍAS DE DATOS	• Datos identificativos básicos y datos de contacto.
FINALIDAD Y BASE DE LEGITIMACIÓN	• Establecimiento de comunicaciones con los familiares de los residentes. Base de legitimación: Existencia de interés legítimo (art. 6.1 f) RGPD) • Cumplimiento del deber de información y obtención del consentimiento en relación con los residentes representados. Base de legitimación: Cumplimiento de obligaciones legales (art. 6.1 c) RGPD).
CATEGORÍAS DE INTERESADOS	• Representantes legales/voluntarios. • Personas de contacto (familiares y amigos de los residentes).
CATEGORÍAS DE DESTINATARIOS	• Prestadores de servicios auxiliares externos con acceso a datos personales tales como prestadores de servicios IT. • Cesionarios tales como hospitales, servicio ambulancia, órganos de la Administración Pública, Juzgados, Fiscalía, Abogados y Procuradores, entidades bancarias.

TRANSFERENCIAS INTERNACIONALES/DESTINO	NO
CONTENEDORES	CRM y aplicación de servicio de correo electrónico
PLAZO DE SUPRESIÓN	Los datos se conservarán durante seis años tras la extinción de la relación contractual o, en su caso, tras la revocación o extinción de la representación. El plazo podrá prorrogarse respecto a los representantes legales o voluntarios mientras esté vigente el plazo de prescripción de acciones civiles (cinco años).
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Protección de documentación en papel mediante armarios bajo llave • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • •Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

5. ATENCIÓN A USUARIOS DEL WEBSITE

ATENCIÓN A USUARIOS DEL WEBSITE (DIGITAL)	
ENTIDAD RESPONSABLE	PLANIGER, S.A.
BREVE DESCRIPCIÓN	Atención a las solicitudes de información
CATEGORÍAS DE DATOS	• Datos identificativos y de contacto.
FINALIDAD Y BASE DE LEGITIMACIÓN	• Atención de solicitudes de información. Base de legitimación: Existencia de consentimiento (art. 6.1 a) RGPD)
CATEGORÍAS DE INTERESADOS	• Usuarios del website solicitantes de información general.
CATEGORÍAS DE DESTINATARIOS	• Usuarios web
TRANSFERENCIAS INTERNACIONALES/DESTINO	NO
CONTENEDORES	Teléfono corporativo, Salesforce, Office 365, Servidor de ficheros, WhatsApp, OneDrive, intranet, SAP, RRSS (LinkedIn, Facebook, Instagram…), Centraliza virtual, Portátil, Sobremesa, IPADs, Pendrives, Sophon, Elastic, Mistery client, Altare.
PLAZO DE SUPRESIÓN	Los datos se suprimirán una vez resuelta la consulta

MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Protección de documentación en papel mediante armarios bajo llave • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • •Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad) • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

6. GESTIÓN DE PROVEEDORES

GESTIÓN DE PROVEEDORES (MIXTO)	
ENTIDAD RESPONSABLE	PLANIGER, S.A.
BREVE DESCRIPCIÓN	Tratamiento de datos personales referidos a proveedores (empresarios individuales) y representantes legales y comerciales relacionados con el suministro de bienes y prestaciones de servicios externos.
CATEGORÍAS DE DATOS	• Datos personales de contacto profesional. • Datos bancarios y económicos
FINALIDAD	• Ejecución del contrato mercantil. Base de legitimación: Necesidad para la ejecución de contrato mercantil (art. 6.1. b) RGPD. • Gestión fiscal, contable y administrativa derivada de transacciones mercantiles con los proveedores. Base de legitimación: Cumplimiento de obligaciones legales en materia fiscal y contable (art. 6.1 c) RGPD) • Tratamiento de datos personales de contactos profesionales pertenecientes a proveedores personas jurídicas con la finalidad de gestionar la relación contractual que vincula a las partes (art.6.1 f) RGPD)
CATEGORÍAS DE INTERESADOS c) RGPD)	• Proveedores (empresarios individuales) y representantes legales y comerciales.

CATEGORÍAS DE DESTINATARIOS	Prestadores de servicios auxiliares externos tales como gestorías, asesorías fiscales/legales, entidades financieras; cesionarios como órganos y organismos de las Administraciones Públicas, Juzgados y Tribunales, Auditores externos.
TRANSFERENCIAS INTERNACIONALES/DESTINO	NO
CONTENEDORES	SAP módulo finanzas, SAP módulo ISH, Repositorio en red, Teams, Plataformas de comunicación para subir las facturas a la APP, Office 365, Teléfono corporativo SIM corporativa, Portátil, Sobremesa.
PLAZO DE SUPRESIÓN	Los datos se conservarán durante el plazo de vigencia de la relación contractual y durante seis años tras su finalización.
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Protección de documentación en papel mediante armarios bajo llave • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico).

	• Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad) • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

7. GESTIÓN DE RECURSOS HUMANOS

GESTIÓN DE RECURSOS HUMANOS (MIXTO)	
ENTIDAD RESPONSABLE	PLANIGER, S.A.
BREVE DESCRIPCIÓN	Gestión de personal, selección de personal, prevención de riesgos laborales, asesoría jurídica laboral y labores administrativas.
CATEGORÍAS DE DATOS	• Datos laborales (identificativos y otros tales como nº de afiliación a la Seguridad Social • Datos económicos incluidos en la nómina, estado civil, nº de hijos, fecha de nacimiento): Ejecución de contrato laboral (art. 6.1 b) RGPD) • Datos curriculares (identificativos, académicos, profesionales) • Datos de carácter especial (grado de discapacidad)
FINALIDAD Y BASE DE LEGITIMACIÓN	• Gestión laboral (retribución, permisos, vacaciones, expedientes sancionadores, control de jornada laboral, etc.), formación, gestión de la Seguridad Social, gestión de prevención de riesgos. Base de legitimación: Cumplimiento de obligaciones legales derivadas de la relación contractual, y cumplimiento de obligaciones legales en relación con la Ley IRPF, Ley General de la Seguridad Social y Ley 31/1995, de Prevención de Riesgos Laborales y Estatuto de los Trabajadores, fundamentalmente. • Gestión de beneficios sociales. Base de legitimación: Necesidad para la ejecución del contrato laboral (art. 6.1 b) RGPD) • Selección de personal. Base de legitimación: Existencia de consentimiento (art. 6.1.b) RGPD)

	• Registro de jornada laboral y control de accesos, tratamiento legitimado la necesidad para la ejecución de un contrato (art.6.1 b) RGPD) y en el interés legítimo (Art.6.1 f) RGPD) –respectivamente-, a la vez que concurre la excepción recogida en el art.9.2 b) para tratar datos de categoría especial (datos biométricos). • Consentimiento de uso de imagen y voz de los trabajadores: base de legitimación (Art.6.1 a RGPD)
CATEGORÍAS DE INTERESADOS	• Trabajadores asalariados • Candidatos • Becarios y estudiantes en prácticas
CATEGORÍAS DE DESTINATARIOS	Prestadores de servicios auxiliares externos tales como empresas de selección de personal, portales de empleo, gestorías, asesorías fiscales/legales, entidades financieras; entidades de formación; y cesionarios tales como FUNDAE, mutua de accidentes; inspectores de trabajo; Instituto de Seguridad e Higiene en el Trabajo y otros órganos y organismos de las Administraciones Públicas, Juzgados y Tribunales.
TRANSFERENCIAS INTERNACIONALES/DESTINO	NO
PLAZO DE SUPRESIÓN	Los datos curriculares de los candidatos se conservarán durante el plazo de un año, excepto si el candidato es contratado (en cuyo caso el CV pasará a formar parte del expediente laboral). Los datos relativos al registro de control horario de jornada se guardarán durante cuatro años, de acuerdo con el art. 34.9 del Estatuto de los Trabajadores. El resto de los datos se conservarán durante el tiempo necesario de acuerdo con los plazos legalmente establecidos, lo que incluye todo el tiempo que dure la relación laboral/profesional, más el tiempo adicional durante el cual se puedan derivar responsabilidades legales. Los documentos laborales que sean soporte contable se conservarán durante seis años.

CONTENEDORES	Carpetas compartidas alojadas en servidor de ficheros, Carpetas compartidas con centros alojadas en servidor de ficheros, Office 365, Epreselec (Infojobs), LinkedIn, Bolsa de empleos de ayuntamiento, Teams, Carpetas compartidas alojadas en servidor de ficheros, SAP módulo ISH, Portal del empleado, Teléfono corporativo, SIM corporativa, Portátil, Teamtailor, Aturnos, Cobee, Wagestram, Ctaima
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Protección de documentación en papel mediante armarios bajo llave • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad) • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

8. GESTIÓN SOCIETARIA

GESTIÓN SOCIETARIA (MIXTO)	
ENTIDAD RESPONSABLE	PLANIGER, S.A.
BREVE DESCRIPCIÓN	Tratamiento de datos personales referidos a socios, administradores y apoderados.
CATEGORÍAS DE DATOS	Datos identificativos y de contacto, datos económicos y transaccionales
FINALIDAD Y BASE DE LEGITIMACIÓN	Gestión de operaciones societarias y relaciones con los socios: Cumplimiento de obligaciones legales (Art. 6.1.c) RGPD) derivadas de Ley de Sociedades de Capital; ejecución de contrato de sociedad (Art. 6.1.b) RGPD)
CATEGORÍAS DE INTERESADOS	Socios, representantes legales y apoderados.
CATEGORÍAS DE DESTINATARIOS	Prestadores externos de servicios de IT, gestorías, asesorías fiscales/legales, entidades financieras, notarías, registros, órganos y organismos de las Administraciones Públicas, Juzgados y Tribunales.
TRANSFERENCIAS INTERNACIONALES/DESTINO	NO
CONTENEDORES	OneDrive de uso interno, OneDrive de uso externo, SAP módulo ISH, Correo electrónico, APP de gestión de impagados, Teams, SAP, Teléfono corporativo, SIM corporativa, Portátil, Abogados externos, Procuradores

	externos, Carpetas compartidas interna de financiero alojadas en servidor de ficheros, Office 365, Zoom, Teams, Teléfono corporativo, SIM corporativa, Dropbox, Wetransfer, Portátil, IPAD.
PLAZO DE SUPRESIÓN	Los datos personales de los socios, administradores y apoderados se conservarán durante el tiempo en que esté vigente la sociedad y, tras su extinción, mientras existan plazos en curso de prescripción de acciones judiciales. Plazo de conservación mínimo: seis años.
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Protección de documentación en papel mediante armarios bajo llave • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad) • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

9. MARKETING

MARKETING (DIGITAL)	
ENTIDAD RESPONSABLE	PLANIGER, S.A.
BREVE DESCRIPCIÓN	Tratamiento de datos personales relacionados con acciones comerciales de prospección (captación de nuevos clientes), comunicaciones y eventos, así como campañas dirigidas a clientes ya existentes.
CATEGORÍAS DE DATOS	Datos identificativos básicos y de contacto, imagen y voz
FINALIDAD Y BASE DE LEGITIMACIÓN	• Gestión de acciones comerciales. Base de legitimación: en relación con clientes potenciales, existencia de consentimiento expreso (art. 6.1. a) RGPD). En relación con clientes, existencia de interés legítimo (at. 6.1 f) RGPD). • El consentimiento de uso de imagen y voz de los trabajadores, con base de legitimación en su consentimiento expreso (art.6.1 a) RGPD)
CATEGORÍAS DE INTERESADOS	Clientes y potenciales clientes
CATEGORÍAS DE DESTINATARIOS	Empresas de marketing y publicidad, Agencias de comunicación, Imprentas, Autónomos colaboradores edición vídeo y fotografía, Plataformas de e-mailmarketing; prestadores externos de servicios de IT(Google, Meta); distribuidores oficiales; empresas del grupo Amavir en caso de consentimiento.
TRANSFERENCIAS INTERNACIONALES/DESTINO	NO

CONTENEDORES	Portátil Cointegra (RSC), Página web, Wordpress, Hotsuite (gestión de RRSS y web), Herramienta a medida SAU, Office 365, Carpeta compartida, Carpeta compartida alojada en servidor de ficheros de comunicación de crisis, Carpeta compartida alojada en servidor de ficheros compartida con dirección. Altare, Salesforce CRM de AMAVIR, Redes Sociales (Snapcht, X, Facebook, Instagram)
PLAZO DE SUPRESIÓN	Los datos de los clientes se conservarán con esta finalidad (marketing) mientras se mantenga la relación contractual y no haya sido revocado el consentimiento. En cuanto a los potenciales clientes, los datos se conservarán mientras el consentimiento no sea revocado. En ambos casos, los datos se eliminarán siempre que hayan quedado desactualizados y no puedan ser habilitados de nuevo.
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Protección de documentación en papel mediante armarios bajo llave • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad)

	• Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

10. CONTROL DE ACCESOS

CONTROL DE ACCESOS	
ENTIDAD RESPONSABLE	PLANIGER, S.A.
BREVE DESCRIPCIÓN	Tratamiento de datos personales referidos a visitantes a los centros residenciales y datos relacionados con el estado de salud
CATEGORÍAS DE DATOS	• Datos identificativos básicos • Datos de salud (temperatura)
FINALIDAD Y BASE DE LEGITIMACIÓN	• Seguridad. Existencia de interés legítimo (art. 6.1 f) RGPD). • Protección de intereses vitales del interesado o de otras personas físicas, (artículo 6.1 b) RGPD). • Obligación legal (artículo 6.1.c) RGPD).
CATEGORÍAS DE INTERESADOS	Visitantes (familiares, proveedores…)
CATEGORÍAS DE DESTINATARIOS	Asesoría legal, abogados, procuradores, Juzgados y Tribunales.
TRANSFERENCIAS INTERNACIONALES/DESTINO	NO
CONTENEDORES	

PLAZO DE SUPRESIÓN	Los datos se conservarán durante el plazo máximo de un mes. Los datos obtenidos del documento de "Declaración responsable" entregado en el momento de acceso al centro serán conservados durante el tiempo recomendado por las Autoridades competentes para poder tener un control y seguimiento de los casos y contactos con personas contagiadas que se puedan producir.
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Protección de documentación en papel mediante armarios bajo llave • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • •Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad) • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

11. VIDEOVIGILANCIA

VIDEOVIGILANCIA (DIGITAL)	
ENTIDAD RESPONSABLE	PLANIGER, S.A.
BREVE DESCRIPCIÓN	Tratamiento de las imágenes captadas por las cámaras de videovigilancia, control laboral.
CATEGORÍAS DE DATOS	• Imagen.
FINALIDAD Y BASE DE LEGITIMACIÓN	• Seguridad. Base de legitimación: Interés público (art.6.1 e) RGPD) • Control Laboral del personal laboral. Base de legitimación ejecución de un contrato laboral, en vinculación con las facultades legales de control (art. 6.1 b) RGPD).
CATEGORÍAS DE INTERESADOS	Residentes, trabajadores y, en general, visitantes.
CATEGORÍAS DE DESTINATARIOS	Empresa de seguridad privada, abogados, procuradores, Juzgados y Tribunales.
TRANSFERENCIAS INTERNACIONALES/DESTINO	NO
CONTENEDORES	Queruplay, Servidores de Amavir, Securtias Direct
PLAZO DE SUPRESIÓN	Los datos se conservarán durante el plazo máximo de un mes desde su obtención.
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002:

	• Medidas de control de acceso físico a las instalaciones de la Organización • Protección de documentación en papel mediante armarios bajo llave • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

12. BANCO DE IMÁGENES

BANCO DE IMÁGENES (DIGITAL)	
ENTIDAD RESPONSABLE	PLANIGER, S.A.
BREVE DESCRIPCIÓN	Tratamiento de imágenes de personas para su utilización en acciones comerciales.
CATEGORÍAS DE DATOS	• Imagen personal
FINALIDAD Y BASE DE LEGITIMACIÓN	• Acciones comerciales. Base de legitimación: Existencia de consentimiento (art. 6.1 a) RGPD)
CATEGORÍAS DE INTERESADOS	• Personas físicas (identificadas o identificables) que autorizan el uso de su imagen para su utilización en acciones comerciales.
CATEGORÍAS DE DESTINATARIOS	Empresas de marketing y publicidad; plataformas de e-mailmarketing
TRANSFERENCIAS INTERNACIONALES/DESTINO	NO
CONTENEDORES	Cointegra (RSC), Página web, Wordpress, Hotsuite (gestión de RRSS y web), Herramienta a medida SAU, Office 365, Carpeta compartida, Carpeta compartida alojada en servidor de ficheros de comunicación de crisis, Carpeta compartida alojada en servidor de ficheros compartida con dirección.

PLAZO DE SUPRESIÓN	Los datos se conservarán mientras no conste la oposición del interesado y se suprimirán en todo caso cuando dejen de ser útiles para la finalidad para la que fueron recogidos.
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Protección de documentación en papel mediante armarios bajo llave • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

13. GESTIÓN DE DERECHOS DE LOS INTERESESADOS Y REGISTRO DE VIOLACIONES DE SEGURIDAD

GESTIÓN DE DERECHOS DE LOS INTERESADOS Y REGISTRO DE VIOLACIONES DE SEGURIDAD (MIXTO)	
ENTIDAD RESPONSABLE	PLANIGER, S.A.
BREVE DESCRIPCIÓN	Gestión de peticiones de ejercicio de derechos de los interesados en materia de protección de datos personales y gestión de violaciones de seguridad
FINALIDAD Y BASE DE LEGITIMACIÓN	Gestión de peticiones de ejercicio de derechos de los interesados en materia de protección de datos personales y gestión de violaciones de seguridad. Base de legitimación: cumplimiento legal (art. 6.1 c) RGPD)
CATEGORÍAS DE INTERESADOS	• Interesados que soliciten alguna petición de ejercicio de derechos en materia de protección de datos personales dirigida al Responsable de Tratamiento (clientes, proveedores, miembros de órganos societarios, empleados, estudiantes en prácticas, trabajadores externos y otros) • Interesados implicados o referidos en los hechos objeto de un procedimiento de gestión de violación de seguridad.
CATEGORÍAS DE DATOS	• Datos básicos identificativos • Datos de contacto • Datos personales adicionales que sean objeto del derecho cuyo ejercicio se solicita • Datos personales adicionales vinculados a la violación de seguridad objeto de gestión
CATEGORÍAS DE DESTINATARIOS	• Prestadores de servicios IT con acceso a datos personales

	• Agencia Española de Protección de Datos • Juzgados y Tribunales de Justicia • Secure&IT (Delegado de Protección de Datos)
TRANSFERENCIAS INTERNACIONALES/DESTINO	No
PLAZO DE SUPRESIÓN	Los datos se conservarán mientras esté vigente el plazo de prescripción de tres años establecido en el art. 78 LOPD-GDD y, en su caso, durante el tiempo adicional mientras existan procedimientos sancionadores en curso.
CONTENEDORES	Carpetas compartidas alojadas en servidor de ficheros, OneDrive de uso interno, OneDrive de uso externo, SAP módulo ISH, Correo electrónico, APP de gestión de impagados, Teams, SAP, Teléfono corporativo, SIM corporativa, Portátil, Abogados externos, Procuradores externos, Sharepoint.
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Protección de documentación en papel mediante armarios bajo llave • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico).

	• Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), • Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

14. RECONOCIMIENTO FACIAL DE RESIDENTES

RECONOCIMIENTO FACIAL DE RESIDENTES (AUTOMATIZADO)	
ENTIDAD RESPONSABLE	PLANIGER, S.A.
BREVE DESCRIPCIÓN	Sistema de reconocimiento facial para prevenir las salidas de las instalaciones del centro de residentes con patologías o enfermedades neurodegenerativas o psiquiátricas.
FINALIDAD Y BASE DE LEGITIMACIÓN	Base de legitimación el art. 6.1. a) y d) del RGPD, que concurre con las excepciones previstas del art. 9.2 a) y c) del RGPD.
CATEGORÍAS DE INTERESADOS	• Residentes
CATEGORÍAS DE DATOS	• Datos básicos identificativos • Plantilla biométrica (facial)
CATEGORÍAS DE DESTINATARIOS	• Prestadores de servicios IT con acceso a datos personales • Agencia Española de Protección de Datos • Juzgados y Tribunales de Justicia
TRANSFERENCIAS INTERNACIONALES/DESTINO	No

PLAZO DE SUPRESIÓN	Plantilla biométrica: Los datos se conservarán mientras el residente o su representante legal no retire el consentimiento y, mientras se mantenga esté vigente la relación contractual. Eventos (imágenes de eventos detectados por la herramienta): durante el plazo de un mes.
CONTENEDORES	En el propio grabador (PC).
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Protección de documentación en papel mediante armarios bajo llave • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), • Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

15 . COMITÉ BIOÉTICO

COMITÉ BIOÉTICO	
ENTIDAD RESPONSABLE	PLANIGER, S.A.
BREVE DESCRIPCIÓN	Comité en donde se evalúan casos complejos y consultas relacionadas con los residentes, familiares, temas relacionados con la ética y moralidad, dentro de GRUPO AMAVIR.
FINALIDAD Y BASE DE LEGITIMACIÓN	Base de legitimación el art. 6.1. e) del RGPD, interés público.
CATEGORÍAS DE INTERESADOS	• Residentes • Familiares • Trabajadores
CATEGORÍAS DE DATOS	• Datos básicos identificativos • Datos especialmente protegidos
CATEGORÍAS DE DESTINATARIOS	• Miembros del comité • ciudadanos
TRANSFERENCIAS INTERNACIONALES/DESTINO	No
PLAZO DE SUPRESIÓN	Los datos se conservarán el tiempo necesario para resolver las consultas y poder llevar a cabos la resolución de las cuestiones planteadas dentro del comité.

	Los datos personales que no sean necesarios se suprimirán de manera inmediata.
CONTENEDORES	
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Protección de documentación en papel mediante armarios bajo llave • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), • Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

16. SERVICIO DE ATENCIÓN AL USUARIO

SERVICIO DE ATENCIÓN AL USUARIO	
ENTIDAD RESPONSABLE	PLANIGER, S.A.
BREVE DESCRIPCIÓN	Se trata de un sistema implantado dentro de la propia página web de GRUPO AMAVIR, en donde se lleva a cabo la recopilación de recomendaciones, quejas de residentes, de familiares, se envían encuestas de satisfacción etc..
FINALIDAD Y BASE DE LEGITIMACIÓN	Base de legitimación el art. 6.1. b) y f) del RGPD,) relación contractual e interés legítimos prevalentes del responsable o de terceros a los que se comunican los datos.
CATEGORÍAS DE INTERESADOS	• Residentes • Familiares • Solicitantes de información vía Web
CATEGORÍAS DE DATOS	• Datos básicos identificativos del interesado. • Datos de contacto.
CATEGORÍAS DE DESTINATARIOS	• Residentes • Familiares
TRANSFERENCIAS INTERNACIONALES/DESTINO	No

PLAZO DE SUPRESIÓN	Los datos se conservarán plazo máximo de 3 años desde el último contacto con el potencial cliente.
CONTENEDORES	
MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Protección de documentación en papel mediante armarios bajo llave • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), • Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.

17. SERVICIO DE CENTRALITA

SERVICIO DE ATENCIÓN AL USUARIO	
ENTIDAD RESPONSABLE	PLANIGER, S.A.
BREVE DESCRIPCIÓN	Sistema de recepción y gestión de llamadas de potenciales clientes. Se gestiona dentro de la infraestructura de Grupo AMAVIR.
FINALIDAD Y BASE DE LEGITIMACIÓN	Base de legitimación el art. 6.1. a) del RGPD, consentimiento expreso y el art. 6.1 f) del RGPD interés legítimo.
CATEGORÍAS DE INTERESADOS	• Potenciales clientes personas físicas • Familiares de potenciales residentes
CATEGORÍAS DE DATOS	• Datos básicos identificativos • Datos de contacto
CATEGORÍAS DE DESTINATARIOS	NO APLICA
TRANSFERENCIAS INTERNACIONALES/DESTINO	No
PLAZO DE SUPRESIÓN	Los datos se conservarán en un plazo máximo de 3 años desde el último contacto con el potencial cliente.
CONTENEDORES	

MEDIDAS DE SEGURIDAD	Medidas de seguridad adoptadas conforme a la norma ISO 27002: • Medidas de control de acceso físico a las instalaciones de la Organización • Protección de documentación en papel mediante armarios bajo llave • Control de acceso lógico (aplicaciones, sistemas operativos, etc.) mediante encriptación y configuración de seguridad de contraseñas con nivel alto, asignadas de forma unívoca. • Segregación de grupos, roles y permisos de acceso lógico (estructura de red, dominio, aplicaciones) a la información en función del rol desempleado en la organización. • Mecanismos de protección de acceso a redes (cortafuegos perimetrales, empleo de túneles privados VPN) • Gestión de copias de seguridad de la información (cloud + soportes de almacenamiento físico). • Mecanismos de protección ambiental del centro de proceso de datos (incendios, temperatura, humedad), • Centro de Operaciones de Seguridad asociado al CPD con personal 24 horas, 7 días a la semana, con vigilancia continua de condiciones ambientales, sistemas de ingeniería y mediciones de energía. • Protección antivirus de los equipos de los empleados, controlados mediante consola centralizada.