APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por la Gerencia de GRUPO V3J, el día 23 de marzo de 2026.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

INTRODUCCIÓN

GRUPO V3J 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 seguridad (confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad) 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 confidencialidad, integridad, disponibilidad, 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 los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional 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.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC 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, en pliegos de licitación y en contratos para proyectos de TIC.

El personal debe estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

PREVENCIÓN

Los departamentos deben 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 los departamentos deben implementar las medidas mínimas de seguridad determinadas por el ENS, 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, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, los departamentos deben:

- 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.

DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuaren consecuencia.

Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

RESPUESTA

GRUPO V3J deberá:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en la organización o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, se desarrollará planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

ALCANCE

Esta Política será de aplicación y de obligado cumplimiento para toda la organización GRUPO V3J, a sus recursos y a los procesos afectados por el ENS, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Todos los miembros de GRUPO V3J, afectados por el alcance del ENS, tienen la obligación de conocer y cumplir esta “Política de Seguridad de la Información” y la normativa de seguridad correspondiente, siendo responsabilidad de GRUPO V3J disponer los medios necesarios para que la información llegue al personal afectado.

MISIÓN

GRUPO V3J tiene como misión el desarrollo, promoción y gestión de proyectos de generación de energía renovable y almacenamiento, proporcionando soluciones energéticas eficientes, sostenibles y seguras, garantizando en todo momento la protección de la información gestionada en el marco de su actividad.

La Dirección de GRUPO V3J, ha establecido en su organización un Sistema de Gestión de la Seguridad de la Información basado en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, atendiendo a los siguientes objetivos:

- Garantizar la protección de la información técnica, jurídica, económica y estratégica asociada a los proyectos de generación y almacenamiento energético.
- Asegurar la disponibilidad y continuidad de los sistemas de información que soportan la actividad de la organización.
- Cumplir con los requisitos legales, reglamentarios y contractuales aplicables, especialmente en materia de protección de datos, seguridad de la información y administración electrónica.

- Minimizar los riesgos derivados de incidentes de seguridad mediante una gestión sistemática del riesgo.
- Promover la concienciación y formación del personal en materia de seguridad de la información.
- Establecer mecanismos de control y mejora continua del Sistema de Seguridad de la Información.

MARCO NORMATIVO

El marco normativo en que se desarrollan las actividades de GRUPO V3J, y en particular la prestación de servicios electrónicos en el marco de su actividad empresarial y contractual está integrado por las siguientes normas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
- ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad
- Sistemas de gestión de la seguridad de la información. Requisitos
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPD).
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.
-

COMITÉ DE SEGURIDAD DE LA INFORMACION

Responsable de la Información/Servicio	JAVIER MUÑOZ CEVERA
Responsable de Seguridad	FLORENTINA AIDA CIOBOTARU
Responsable de Sistemas	MIGUEL IBAÑEZ CAMPOS

ROLES: FUNCIONES Y RESPONSABILIDADES

En GRUPO V3J, los roles de Responsable de la Información y Responsable del Servicio recaen en la Dirección.

- **RESPONSABLE DE LA INFORMACIÓN,** será quien determine los requisitos de los servicios prestados, en consonancia, tendrá las siguientes funciones:
  - Establecer y aprobar los requisitos de seguridad aplicables al servicio dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 3 de mayo, previa propuesta del Responsable de Seguridad y/o Comité de Seguridad de la Información.
  - Aceptar los niveles de riesgo residual que afecten al Servicio.
  - Aprueba la Política de Seguridad de la Información
  - Efectúa las valoraciones a las que se refiere el artículo 40 del ENS (categorías de seguridad), así como, en su caso, su posterior modificación
  - Recibe información sobre los incidentes y de las actuaciones realizadas para su resolución.
  - Determinación de los criterios para asignar y modificar a cada información el nivel de seguridad requerido, y será responsable de su documentación y aprobación formal
  - Establecer los requisitos/niveles de la información en materia de seguridad teniendo en cuenta la Política de seguridad.
  - Asumir la responsabilidad última de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
  - Aprueba el Plan de continuidad de Negocio

- Aprueba el sistema de gestión de la información
- Aporta los recursos financieros para la Seguridad de la Información

- **RESPONSABLE DEL SERVICIO,** será quien determine los requisitos de los servicios prestados, en consonancia, tendrá las siguientes funciones:
  - Establecer y aprobar los requisitos de seguridad aplicables al servicio dentro del marco establecido en el anexo I del Real Decreto 311/2022, de 3 de mayo, previa propuesta del Responsable de Seguridad y/o Comité de Seguridad de la Información.
  - Emprende y dirige la política de seguridad de la información.
  - Aporta los recursos financieros para la Seguridad de la Información
  - Efectuará las valoraciones a las que se refiere el artículo 40 (categorías de seguridad), así como, en su caso, su posterior modificación.
  - Será informado de los incidentes y de las actuaciones llevadas a cabo para su resolución
  - Establecer los requisitos/niveles del servicio en materia de seguridad teniendo en cuenta la Política de seguridad.

- **RESPONSABLE DE SEGURIDAD,** será quien tome las decisiones adecuadas para satisfacer los requisitos de seguridad de la información y de los servicios. Dispondrá de las siguientes funciones:
  - La determinación de la categoría de seguridad del sistema, con base en las valoraciones de los Responsables de la Información y del Servicio
  - Elaborar y aprobar la Declaración de Aplicabilidad, atendiendo a los requerimientos del Responsable de la Información y del Servicio
  - Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en su ámbito de responsabilidad.
  - Determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios, supervisará la implantación de las medidas necesarias para garantizar que se satisfacen los requisitos y reportará sobre estas cuestiones
  - Formalización y aprobación de las medidas seleccionadas del Anexo II en la Declaración de Aplicabilidad, incluyendo las medidas compensatorias o complementarias de vigilancia y su correspondencia con las medidas del Anexo II antes citado.
  - Comprobar que las medidas de seguridad de la información han sido adecuadamente implementadas por el Responsable del Sistema.
  - Análisis de los informes de Auditoria de primera, segunda o tercera parte que se refieran a los sistemas de su ámbito competencial, y presentación de sus conclusiones al Responsable del Sistema y, en su caso, al Comité de Seguridad de la Información.
  - Aprobación explicita de los cambios que impliquen un riesgo de nivel ALTO con carácter previo a su implantación protección de datos que sean fijados por el responsable o por el encargado del tratamiento, contando con el asesoramiento del DPD.
  - Participar en la elaboración y en la propuesta de la Política de Seguridad de la Información y los procedimientos, normativas e instrucciones en aplicación del ENS.
  - Analizar los riesgos antes del despliegue de los sistemas de inteligencia artificial en la entidad, atendiendo a las valoraciones del Responsable de la Información y del Servicio y, en su caso, del Delegado de Protección de Datos y supervisar su despliegue.
  - Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
  - Cuando el sistema trate datos personales, el Responsable de la Seguridad velará por la correcta integración de los requisitos establecidos por la normativa de protección de datos.
  - Realizar o promover las autoevaluaciones o auditorías periódicas que permitan verificar el cumplimiento del ENS.
  - En la gestión de los ciberincidentes, contando con los responsables de la entidad, de la información y de los servicios, calificará la peligrosidad de estos de acuerdo a la Guía CCN-STIC 817, actuando como punto de contacto con las autoridades competentes en materia de seguridad y, en función de los roles asignados en la Política podrá notificar los mismos, en su

caso, al CCN-CERT. Cuando fuese precisa la notificación al CSIRT de referencia está deberá realizarse sin dilaciones indebidas y con carácter inmediato, sin perjuicio de la remisión de información ampliada de forma paulatina.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema, que podrá ser proporcionado por elementos específicos, tales como herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para la alta dirección del GRUPO V3J, incluyendo los incidentes más relevantes del periodo.
- Por otro lado, el Responsable de la Seguridad colaborará con el Delegado de Protección de Datos de la Entidad en la gestión de los incidentes que afecten a datos personales y, en su caso, a la notificación a las autoridades de control y a las personas afectadas.

- **RESPONSABLE DE SISTEMAS**, dentro de sus áreas de actuación, tendrán asignadas las siguientes funciones:
  - Paralizar o dar suspensión al acceso a información o prestación de servicio si tiene el conocimiento de que estos presentan deficiencias graves de seguridad.
  - Desarrollar, operar y mantener el sistema de información durante todo su ciclo de vida.
  - Elaborar los procedimientos operativos necesarios.
  - Definir la topología y la 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.
  - Prestar al Responsable de Seguridad asesoramiento para la determinación de la Categoría del Sistema.
  - Colaborar, si así se le requiere, en la elaboración e implantación de los planes de mejora de la seguridad y, llegado el caso, en los planes de continuidad.
  - Llevar a cabo las funciones del administrador de la seguridad del sistema:
    - La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de la actividad desarrollada en el sistema y su correspondencia con lo autorizado.
    - Aprobar los cambios en la configuración vigente del Sistema de Información.
    - Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
    - Asegurar que son aplicados los procedimientos aprobados para manejar el Sistema de Información.
    - Dar de alta o baja los usuarios.
    - Lleva el registro de entrada y salida de soportes.

PROCEDIMIENTOS DE DESIGNACIÓN

La responsabilidad general de la seguridad de la información recaerá sobre el **Responsable de Seguridad**, siendo la responsabilidad última del Comité de Seguridad de la Información y de la Dirección como máximo Responsable del Sistema de gestión de seguridad de la información.

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

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad TIC la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Dirección de GRUPO V3J y difundida para que la conozcan todas las partes afectadas.

DATOS DE CARÁCTER PERSONAL

GRUPO V3J trata datos de carácter personal. El documento de seguridad ANEXO I REGISTRO DE ACTIVIDADES COMO RESPONSABLE DEL TRATAMIENTO (FICHEROS), al que tendrán acceso sólo las personas autorizadas, recoge los ficheros afectados y los responsables correspondientes. Todos los sistemas de información de GRUPO V3J se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad de GRUPO V3J en diferentes materias:

- POL-01 Política de Control de Accesos
- POL-02 Política de Contraseñas
- POL-03 Política de Uso aceptable de Activo
- POL-04 Política de Controles Criptográficas
- POL-05 Política de Uso aceptable de servicio en la nube

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la GRUPO V3J que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La Política de Seguridad de la Información estará disponible en la página web de la organización.

OBLIGACIONES DEL PERSONAL

Todos los miembros de GRUPO V3J tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.
Todos los miembros de GRUPO V3J atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año.

Se establecerá un programa de concienciación continua para atender a todos los miembros de GRUPO V3J, en particular a los de nueva incorporación.
Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo

TERCERAS PARTES

Cuando GRUPO V3J preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.
Cuando GRUPO V3J utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en
materia de seguridad, al menos al mismo nivel que el establecido en esta Política.
Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

CEO
23 de marzo de 2026

Rev. 00

ANEXO I

REGISTRO DE ACTIVIDADES COMO RESPONSABLE DEL TRATAMIENTO (FICHEROS)

1. Identificación de la organización Responsable del tratamiento

De conformidad con lo dispuesto en el Reglamento (UE) 2016/679, de 27 de abril de 2016 (RGPD), la organización Responsable del tratamiento es quien determina los fines y los medios del tratamiento de datos personales (Ficheros).

Razón social	V3J INGENIERIA Y SERVICIOS SL
Marca comercial	V3J INGENIERIA Y SERVICIOS SL
Actividad	energia
Dirección	CALLE MARQUES DE DOS AGUAS, 7 - 1 d 46002 VALENCIA (València) ESPAÑA
Teléfono	96351934
E-mail	v3j@v3jjngenieria.com
DPO	FRANCISCO DE ASÍS MARCO BATALLER (QUANTUM CONSULTORES) fmarco@quantumconsultores.es

2. Identificación de los tratamientos de datos personales tratados por cuenta propia

Un fichero es un conjunto estructurado de datos personales accesibles con arreglo a criterios determinados y susceptibles de tratamiento para un fin específico.

Tratamiento	Descripción
1 LABORAL Y RR. HH.	Gestión administrativa y laboral del personal empleado en la organización
2 CLIENTES Y PROVEEDORES	Gestión comercial con clientes y proveedores. Incluye datos de contacto de personas físicas que presten servicios a una persona jurídica, inclusive los profesionales individuales
3 FISCAL Y CONTABLE	Registro de las obligaciones fiscales y contables sujetas a la actividad económica
4 CONTACTOS	Comunicación, información y gestión sobre productos y servicios. Incluye contactos web y redes sociales
5 CURRÍCULUMS	Gestión de candidatos a empleados
6 COMUNICACIONES WHATSAPP	Comunicaciones comerciales. Información sobre productos y servicios. Gestión de citas
7 GESTIÓN COMERCIAL	Comunicación, información y gestión sobre productos y servicios. Incluye contactos web y redes sociales
8 PREVENCIÓN DE RIESGOS LABORALES	Gestión de la prevención de riesgos laborales de los empleados
9 REGISTRO JORNADA LABORAL	Registro horario de la jornada laboral para dar cumplimiento al RDL 8/2019 de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo
10 GESTIÓN WEBSITE	Gestión de la website, comunicaciones comerciales de productos y servicios. Contactos web. Redes sociales

3. Registro de las actividades del tratamiento

De conformidad con el artículo 30 del Reglamento (UE) 2016/679, de 27 de abril de 2016 (RGPD), la Organización deberá llevar y conservar actualizado un Registro de las actividades de tratamiento efectuadas bajo su responsabilidad, en formato electrónico, que contenga:

- Nombre y datos de contacto del Responsable del tratamiento y, en su caso, del Corresponsable del tratamiento, del Representante del Responsable y del Delegado de protección de datos (DPO).
- Fines del tratamiento.
- Descripción de las categorías de interesados.
- Descripción de las categorías de datos.
- Categorías de Destinatarios.
- Transferencias de datos a terceros países, con la identificación de los mismos y documentación de garantías adecuadas.
- Cuando sea posible:
    - Plazos previstos para la supresión de las diferentes categorías de datos.
    - Descripción general de las medidas técnicas y organizativas de seguridad.

Los Responsables del tratamiento, o sus Representantes, deberán poner a disposición de la Autoridad de control este Registro de actividades, cuando esta lo solicite.

Este Registro se ha documentado para cada uno de los Tratamientos descritos en el apartado 2, lo cuales se detallan a continuación.

1. LABORAL Y RR. HH.

Descripción	Gestión administrativa y laboral del personal empleado en la organización
Finalidades	Prevención de riesgos laborales servicio externo. Gestión de nóminas. Recursos humanos
Categorías de interesados	Empleados
Criterios de conservación	Conservados mientras existan prescripciones legales que dictaminen la custodia
Sistema de tratamiento	Parcialmente Automatizado
Categorías de datos	
Tipos de datos	DNI/NIF/NIE/Pasaporte. Nombre y apellidos. Dirección postal o electrónica. Teléfono. Firma manual. Núm. de SS o mutualidad
Otro tipo de datos	Características personales. Académicos y profesionales. Detalles de empleo. Económicos. financieros y de seguro. Transacciones de bienes y servicios
Categorías de destinatarios	
Cesiones	Organismos de la Seguridad Social. Administración tributaria. Administración pública con competencia en la materia
Transferencias internacionales	No existen
Medidas de seguridad	
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)

2. CLIENTES Y PROVEEDORES

Descripción	Gestión comercial con clientes y proveedores. Incluye datos de contacto de personas físicas que presten servicios a una persona jurídica, inclusive los profesionales individuales
Finalidades	Gestión contable. fiscal y administrativa
Categorías de interesados	Proveedores. Clientes y usuarios

Criterios de conservación	Conservados durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia
Sistema de tratamiento	Parcialmente Automatizado
Categorías de datos	
Tipos de datos	DNI/NIF/NIE/Pasaporte. Nombre y apellidos. Dirección postal o electrónica. Teléfono. Firma manual
Otro tipo de datos	Características personales. Circunstancias sociales. Información comercial. Transacciones de bienes y servicios
Categorías de destinatarios	
Cesiones	No existen
Transferencias internacionales	No existen
Medidas de seguridad	
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)

3. FISCAL Y CONTABLE

Descripción	Registro de las obligaciones fiscales y contables sujetas a la actividad económica
Finalidades	Gestión contable. fiscal y administrativa
Categorías de interesados	Proveedores. Clientes y usuarios
Criterios de conservación	Conservados mientras existan prescripciones legales que dictaminen la custodia
Sistema de tratamiento	Parcialmente Automatizado
Categorías de datos	
Tipos de datos	DNI/NIF/NIE/Pasaporte. Nombre y apellidos. Dirección postal o electrónica. Teléfono
Otro tipo de datos	No existen
Categorías de destinatarios	
Cesiones	Bancos. cajas de ahorro y cajas rurales. Administración tributaria

Transferencias internacionales	No existen
Medidas de seguridad	
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)

4. CONTACTOS

Descripción	Comunicación, información y gestión sobre productos y servicios. Incluye contactos web y redes sociales
Finalidades	Publicidad y prospección comercial
Categorías de interesados	Personas de contacto. Clientes y usuarios. Solicitantes
Criterios de conservación	Conservados durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia
Sistema de tratamiento	Parcialmente Automatizado
Categorías de datos	
Tipos de datos	DNI/NIF/NIE/Pasaporte. Nombre y apellidos. Dirección postal o electrónica. Teléfono
Otro tipo de datos	Información comercial
Categorías de destinatarios	
Cesiones	No existen
Transferencias internacionales	No existen
Medidas de seguridad	
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados

Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)

5. CURRÍCULUMS

Descripción	Gestión de candidatos a empleados
Finalidades	Recursos humanos
Categorías de interesados	Empleados. Solicitantes
Criterios de conservación	No existen
Sistema de tratamiento	Parcialmente Automatizado
Categorías de datos	
Tipos de datos	DNI/NIF/NIE/Pasaporte. Nombre y apellidos. Dirección postal o electrónica. Teléfono. Imagen. Firma manual
Otro tipo de datos	Características personales. Circunstancias sociales. Académicos y profesionales. Detalles de empleo
Categorías de destinatarios	
Cesiones	No existen
Transferencias internacionales	No existen
Medidas de seguridad	
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)

6. COMUNICACIONES WHATSAPP

Descripción	Comunicaciones comerciales. Información sobre productos y servicios. Gestión de citas
Finalidades	Publicidad y prospección comercial. Gestión contable. fiscal y administrativa
Categorías de interesados	Personas de contacto. Clientes y usuarios. Solicitantes
Criterios de conservación	Conservados durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia
Sistema de tratamiento	Automatizado
Categorías de datos	
Tipos de datos	Nombre y apellidos. Teléfono
Otro tipo de datos	Información comercial
Categorías de destinatarios	
Cesiones	No existen
Transferencias internacionales	No existen
Medidas de seguridad	
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)

7. GESTIÓN COMERCIAL

Descripción	Comunicación, información y gestión sobre productos y servicios. Incluye contactos web y redes sociales
Finalidades	Publicidad y prospección comercial
Categorías de interesados	Personas de contacto. Clientes y usuarios. Solicitantes
Criterios de conservación	Conservados durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia
Sistema de tratamiento	Parcialmente Automatizado
Categorías de datos	
Tipos de datos	DNI/NIF/NIE/Pasaporte. Nombre y apellidos. Dirección postal o electrónica. Teléfono

Otro tipo de datos	Información comercial
Categorías de destinatarios	
Cesiones	No existen
Transferencias internacionales	No existen
Medidas de seguridad	
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)

8. PREVENCIÓN DE RIESGOS LABORALES

Descripción	Gestión de la prevención de riesgos laborales de los empleados
Finalidades	Prevención de riesgos laborales servicio externo
Categorías de interesados	Empleados
Criterios de conservación	Conservados mientras existan prescripciones legales que dictaminen la custodia
Sistema de tratamiento	Parcialmente Automatizado
Categorías de datos	
Tipos de datos	DNI/NIF/NIE/Pasaporte. Nombre y apellidos. Dirección postal o electrónica. Teléfono. Firma manual. Núm. de SS o mutualidad
Otro tipo de datos	No existen
Categorías de destinatarios	
Cesiones	No existen
Transferencias internacionales	No existen
Medidas de seguridad	
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados

Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)

9. REGISTRO JORNADA LABORAL

Descripción	Registro horario de la jornada laboral para dar cumplimiento al RDL 8/2019 de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo
Finalidades	Recursos humanos. Gestión de nóminas
Categorías de interesados	Empleados
Criterios de conservación	Conservados durante 4 años para el registro horario de jornada laboral
Sistema de tratamiento	Parcialmente Automatizado
Categorías de datos	
Tipos de datos	DNI/NIF/NIE/Pasaporte. Nombre y apellidos. Identificador de usuario
Otro tipo de datos	No existen
Categorías de destinatarios	
Cesiones	Interesados legítimos. Organismos de la Seguridad Social
Transferencias internacionales	No existen
Medidas de seguridad	
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)

10. GESTIÓN WEBSITE

Descripción	Gestión de la website, comunicaciones comerciales de productos y servicios. Contactos web. Redes sociales
Finalidades	Publicidad y prospección comercial
Categorías de interesados	Personas de contacto. Clientes y usuarios. Solicitantes
Criterios de conservación	Conservados durante no más tiempo del necesario para mantener el fin del tratamiento o mientras existan prescripciones legales que dictaminen su custodia
Sistema de tratamiento	Automatizado
Categorías de datos	
Tipos de datos	DNI/NIF/NIE/Pasaporte. Nombre y apellidos. Dirección postal o electrónica. Teléfono
Otro tipo de datos	Información comercial
Categorías de destinatarios	
Cesiones	No existen
Transferencias internacionales	No existen
Medidas de seguridad	
Acceso a documentos	SE APLICAN medidas adecuadas para impedir el acceso a personas no autorizadas
Acceso a equipos y redes informáticas	SE ACCEDE mediante usuario y contraseña personalizados
Seguridad de la contraseña	Se aplican medidas de seguridad (cifrado, combinación de caracteres, cambio periódico, etc.)
Protección de equipos y redes informáticas	SE HAN INSTALADO dispositivos y/o aplicaciones para proteger los equipos informáticos y se mantienen actualizados
Copias de respaldo	SE REALIZAN copias de seguridad externas, como mínimo semanalmente, y se guardan con medidas de seguridad
Transporte y transmisión de datos	LO REALIZA personal autorizado con medidas de seguridad
Conservación de datos	Se guardan en mobiliario o departamentos SIN ACCESO DIRECTO a los datos
Destrucción de datos	SE DESTRUYEN o suprimen con medidas de seguridad (destructora, formateo, empresa homologada de residuos, etc.)