DESCRIPCIÓN DEL TRATAMIENTO ENCOMENDADO, FINALIDAD Y CATEGORÍAS DE DATOS TRATADOS

Ficheros y categorías de datos personales e interesados	• Fichero de clientes: datos de contacto, económicos, facturación. • Fichero de trabajadores: datos de contacto, económicos, familiares, circunstancias sociales y aquellos datos necesarios para la elaboración de nóminas, pago de seguros sociales y trámites legales en la gestión de RR.HH.
Origen de los datos	• Del propio interesado o su representante legal.
Tratamientos a realizar	• Recogida, registro, estructuración, modificación e interconexión.
Duración del tratamiento	• El tratamiento de datos tendrá la duración prevista en el contrato o mientras dure la prestación de servicios.
Subcontrataciones previstas	Imedisa Artes Gráficas debe subcontratar servicios de: • Hosting. • Mantenimiento de software. • Mantenimiento de hardware. • Seguridad lógica.
Transferencias internacionales de datos	• No se prevén transferencias internacionales de datos.
Evaluación de impacto	• Imedisa Artes Gráficas realizará una EIPD o evaluación de impacto y mantendrá un registro de tratamientos realizados.
Medidas de seguridad	El ENCARGADO DE TRATAMIENTO aplicará las medidas técnicas y organizativas de seguridad en los términos establecidos en el artículo 23 del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 27 de abril de 2.016. El ENCARGADO DE TRATAMIENTO garantiza que ha realizado un correcto análisis de riesgos y aplicación de las medidas de seguridad, técnicas y organizativas necesarias, adecuadas y proporcionales al riesgo. El ENCARGADO DE TRATAMIENTO garantiza que las metodologías de gestión del riesgo, planificación, aplicación y seguimiento de las medidas de seguridad serán adecuadas a sistemas internacionales reconocidos.

A continuación se exponen las medidas de seguridad aplicadas por el encargado de tratamiento, que el cliente declara como suficientes para garantizar su solvencia en los términos del RGPD:

Medidas de seguridad	**1. POLÍTICA DE PRIVACIDAD:** 1.1 Cuenta con una política de privacidad aprobada por la dirección. 1.2 Ha asignado responsabilidades en privacidad y seguridad. 1.3 Realiza una gestión y seguimiento documentado de las medidas de seguridad y de las incidencias detectadas. 1.4 Cuenta con procesos de autorización para el acceso a la información confidencial.
	2. TERCEROS: 2.1 Tiene identificados los proveedores que pueden tener acceso a la información, y verifica su solvencia para cumplir con el RGPD. 2.2 Suscribe con estos proveedores contratos de confidencialidad y tratamiento de datos por cuenta de terceros en los términos fijados por el RGPD.
	3. ACTIVOS: 3.1 Realiza inventarios del hardware y software implicado y los mantiene actualizados. 3.2 La información confidencial es clasificada y recibe un tratamiento específico de seguridad.
	4. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS: 4.1 Asigna funciones específicas y responsabilidades en materia de seguridad. 4.2 El personal con acceso a información confidencial recibe formación en materia de seguridad. 4.3 El personal con acceso a la información recibe por escrito normativa o instrucciones internas de seguridad. 4.4 El personal es informado de sus obligaciones y consecuencias en caso de infracción de la normativa interna de seguridad. 4.5 Retira los permisos de acceso y aplica controles para la devolución de toda la información y equipos asignados al personal que sea baja definitiva.

Medidas de seguridad	**5. SEGURIDAD FÍSICA Y DEL ENTORNO:** 5.1 La información confidencial no se ubica en áreas de atención o de acceso público. 5.2 Las áreas de trabajo son seguras evitan el acceso de terceros. 5.3 Dispone de un sistema de videovigilancia y de alarma.
	6. SEGURIDAD DE LOS EQUIPOS: 6.1 Los equipos que tratan la información están en áreas seguras. 6.2 Se aplican medidas de seguridad a los equipos con información que puedan salir fuera de las instalaciones. 6.3 Se aplican medidas de seguridad a los smartphones para evitar el acceso a información y su eliminación en caso de pérdida (MDM). 6.4 Aplica medidas de seguridad para la destrucción de los equipos desechados, de forma que la información que hubieran contenido no sea recuperable. 6.5 Aplica procedimientos de eliminación de información a equipos reutilizados. 6.6 Todos los equipos y servidores disponen de protección antivirus.
	7. GESTIÓN DE COMUNICACIONES Y OPERACIONES: 7.1 Aplica sistema de control contra código malicioso. 7.2 Dispone de firewall para el control de todas las redes. 7.3 Aplica controles de seguridad en la red. 7.4 Los accesos remotos a la información se realizan mediante un modo seguro VPN o equivalente.
	8. COPIAS DE SEGURIDAD Y RESILENCIA: 8.1 Dispone de un sistema adecuado de copias de seguridad de la información. 8.2 Verifica periódicamente que el sistema de copia está en correcto funcionamiento realizando pruebas de restauración. 8.3 Las copias de seguridad se almacenan en un lugar seguro fuera de las instalaciones. 8.4 Los soportes que almacenan la copia de seguridad están protegidos con contraseña o sistema equivalente. 8.5 Dispone de un plan de resilencia o recuperación ante desastres. 8.6 La aplicación del plan de contingencia o recuperación garantiza la restauración y activación de los servicios en un plazo adecuado al riesgo.
	9. MANIPULACIÓN DE SOPORTES: 9.1 Los soportes extraíbles están inventariados. 9.2 Se escanea malware previamente a la conexión de soportes externos a los sistemas de información. 9.3 Se protegen los soportes de información mediante técnicas de cifrado o equivalentes.
	10. CONTROL DE ACCESO LÓGICO: 10.1 La información confidencial se ubica en directorios de acceso restringido. 10.2 El acceso a la información se otorga atendiendo a los roles y responsabilidades del usuario, previa autorización. 10.3 Los usuarios con acceso a la información están registrados. 10.4 Los usuarios tienen únicamente los privilegios necesarios para el desempeño de sus funciones. 10.5 Los usuarios no tienen por defecto permisos de administración activados. 10.6 Los usuarios acceden mediante un sistema de identificación y autenticación. 10.7 A las contraseñas se les aplica directiva de complejidad. 10.8 Las contraseñas se modifican periódicamente. 10.9 La baja del usuario implica la retirada automática de los permisos de acceso. 10.10 Los controles de acceso se aplican a nivel de sistema operativo. 10.11 Los controles de acceso se aplican a nivel de aplicaciones. 10.12 Las contraseñas de Administración general de los sistemas y servidores están almacenadas en una caja de seguridad.
	11. CONTROL DE ACCESOS A LA RED: 11.1 Se procede a la autenticación de usuario para conexiones externas. 11.2 Los equipos pertenecientes a la red están identificados e inventariados. 11.3 Cuenta con procedimientos para la protección de los puertos. 11.4 El acceso de proveedores externos para tareas de mantenimiento se realiza previa notificación y comprobación de identificación y autenticación del proveedor. 11.5 El acceso remoto se realiza mediante conexiones seguras, tales como VPN o sistemas similares. 11.6 La red wifi cuenta con sistema de cifrado. 11.7 La red wifi de los sistemas de información está separada de la red wifi para invitados. 11.8 Las contraseñas de acceso a la red wifi se renuevan periódicamente. 11.9 Se aplican limitaciones de tiempo a las conexiones a la red. 11.10 Todas las comunicaciones, equipos y archivos se filtran con un sistema antivirus.

Medidas de seguridad	**12. MOVILIDAD:** 12.1 Los portátiles, smartphones y dispositivos equivalentes autorizados tienen control de accesos. 12.2 Los portátiles, smartphones y dispositivos equivalentes autorizados están cifrados. 12.3 Los portátiles, smartphones y dispositivos equivalentes autorizados tienen protección antivirus. 12.4 A los smartphones se les aplica software MDM.
	13. GESTIÓN DE INCIDENTES DE SEGURIDAD: 13.1 Dispone de un procedimiento para la gestión de incidencias de seguridad. 13.2 El personal de la organización ha sido informado de su obligación de notificar incidencias de seguridad. 13.3 El procedimiento incluye la notificación de brechas de seguridad de alto impacto a la AEPD en 72 horas.
	14. PROTECCIÓN DE LAS COMUNICACIONES: 14.1 Se utilizan métodos de cifrado o equivalentes para el envío de información confidencial. 14.2 Las comunicaciones entre servicios están cifradas.
	15. SUPERVISIÓN: 15.1 Los registros de los sistemas de información son conservados. 15.2 Se realizan auditorías internas o externas de forma periódica. 15.3 Se aplica un plan de mejora continua.