ANEXO VIII:
ENCARGADOS DE TRATAMIENTO

ANTES DE CONTRATAR CON UN PROVEEDOR

1 Política de seguridad y de protección de datos personales

1.1 Su compañía, incluyendo todas sus filiales ¿Tiene una Política de Seguridad y Privacidad de datos adaptada a la legislación aplicable y estándares en todas las jurisdicciones donde opera?

SI		NO	

En caso negativo, le rogamos facilite detalles sobre otros procedimientos internos de la empresa para la protección de datos y las jurisdicciones donde no se encuentran adaptados:

1.2 ¿Dispone de un plan de emergencia en el caso de que descubran una brecha de seguridad de sistemas o brecha de privacidad/seguridad de datos?

SI		NO	

En caso afirmativo, por favor facilite detalles a continuación:.

1.3 ¿Su compañía informa y facilita a todos sus empleados los procedimientos y políticas internas de protección de datos así como sus actualizaciones y les requiere la confirmación de su cumplimiento?

SI		NO	

En caso negativo, le rogamos facilite explicación del motivo:

1.4 ¿Cuándo y por parte de quién fueron revisados por última vez los procedimiento internos de protección de datos?

1.5 ¿Dispone su compañía de certificados relacionadas con la gestión de los sistemas de información (por ejemplo, ISO9001, ISO27001; ISO20000-1, CMMI, PCI DSS, etc.)?

SI		NO	

En caso afirmativo, le rogamos indique cuáles:

1.6 ¿Su compañía tiene alguna filial en los Estados Unidos de América?

SI		NO	

En caso afirmativo, ¿se ha registrado su compañía y da cumplimiento al Programa "*Privacy Shield*" firmado entre la Unión Europea y los Estados Unidos de América?

SI		NO	

En caso negativo, rogamos facilite detalles en relación a la falta de cumplimiento con dicho programa:

1.7 ¿Tiene su compañía un Responsable de seguridad, un Responsable de protección de los datos, un asesor legal interno o cualquier otra persona formalmente responsable de la protección y seguridad de los datos?

SI		NO	

En caso negativo, ¿quién es responsable de la gestión y cumplimiento de lo relativo a la seguridad y protección de los datos?:

2 Protección de los sistemas y antivirus

2.1 Su compañía, utiliza procesos y sistemas de protección anti-virus actualizado en sus equipos, sistemas de comunicación y servidores para servicios básicos y de misión crítica para protegerlos contra código malicioso (incluyendo pero no limitando, virus, troyanos/gusanos, spyware, malware y root-kits?

SI		NO	

En caso afirmativo, ¿cada cuanto tiempo actualizan estos procedimientos y sistemas de protección? ¿Se actualiza automáticamente?:

2.2 ¿Dispone de un programa de evaluación de vulnerabilidades proactivo que monitoriza las brechas y asegura un tiempo de actualización en los parches de seguridad críticos, vulnerabilidades conocidas?

SI		NO	

3 Seguridad y funcionamiento de red

3.1 Su compañía ¿utiliza sistemas de protección con el fin de evitar accesos no autorizados o daños a sus sistemas informáticos, redes, o sistemas de almacenamiento de datos e información (tales como IPS, "firewalls", autentificación de usuarios en remoto, etc.)?

SI		NO	

En caso afirmativo, ¿están todos los ordenadores, dispositivos móviles y sitios web protegidos con "firewalls" o tienen sistemas de prevención de intrusión/acceso en los mismos?

SI		NO	

3.2 ¿Tiene su compañía procesos instaurados de identificación y detección de debilidades en sus sistemas/redes?

SI		NO	

En caso negativo, motive la decisión:

3.3 Su compañía, ¿monitoriza sus redes y sistemas informáticos buscando violaciones de seguridad?

SI		NO	

En caso negativo, motive la decisión:

3.4 Su compañía, ¿Realiza con regularidad auditorias y revisiones de la arquitectura de seguridad de la red?

SI		NO	

En caso afirmativo, ¿se ha implantado un plan correctivo?

SI		NO	

3.5 ¿Tiene su compañía requerimientos de cifrado para datos en tránsito y datos en depósito que protejan la integridad de la información confidencial, incluidos los datos contenidos en dispositivos o tecnología móvil (por ejemplo, portátiles, grabaciones de backup en DVD, drivers, dispositivos USB…etc.?

SI		NO	

4 Copias de seguridad y Plan de continuidad

4.1 Su compañía mantiene mecanismos de copias de seguridad y procesos de recuperación para todos:

SI		NO	

i) los sistemas de misión crítica

SI		NO	

ii) los datos y activos informáticos

4.2 ¿Dispone de un plan de continuidad del negocio (BCP) y plan de recuperación ante desastres (DRP) de trabajo para evitar la Interrupción del negocio a causa de problemas informáticos o acelerar su recuperación?

SI		NO	

En caso afirmativo, ¿Cuánto tiempo le llevaría restablecer las operaciones después de un ataque cibernético u otra pérdida/corrupción de datos?

En caso negativo, ¿tiene previsto establecer un plan de continuidad? ¿Cuándo? Rogamos facilite detalle:

5 Seguridad física de la sala de ordenadores

5.1 Su compañía ¿Ha realizado un inventario de los sistemas críticos?

SI		NO	

5.2 Su compañía, ¿Tiene establecidos controles físicos de seguridad para la detección y detención de accesos no autorizados a los sistemas informáticos y centros de datos?

SI		NO	

6 Actividades de Outsourcing (Servicios de Externalización)

6.1 Su compañía, ¿externaliza alguna parte de sus redes, sistemas informáticos o funciones de seguridad de la información?

SI		NO	

En caso afirmativo, ¿Audita su compañía periódicamente las funciones del al subcontratista (también denominado "prestador de servicios") para asegurarse de que cumplen con las políticas de seguridad del solicitante?:

¿Quién se encarga de la externalización de la seguridad?:

6.2 ¿Su compañía, requiere al subcontratista que dé cumplimiento con los términos de la política de protección de datos de su compañía?

SI		NO	

6.3 ¿Se han suscrito Acuerdos de Nivel de Servicio (SLAs) con el subcontratista y/o acuerdos de encargado de tratamiento?

SI		NO	

6.4 ¿Se exige al subcontratista la contratación de póliza de RC Profesional y/o protección de datos?

SI		NO	

En caso afirmativo, especificar cual de ellas:

6.5 Su compañía, ¿dispone de servicios en nube o *cloud computing*?

SI		NO	

En caso afirmativo:

¿Dispone de una política de seguridad cloud? Si No

SI		NO	

En caso negativo, le rogamos facilite detalles sobre otros procedimientos internos para asegurar los datos personales y corporativos:

Proveedor:	
CIF:	

Nombre y Apellidos	
Número de Identificación Fiscal	
Cargo en la empresa	
Lugar y fecha	

_____

Firma

Los datos personales que puedan constar en este documento se incorporarán en los ficheros propiedad de INDUSTRIA RESTAURACIÓN COLECTIVA, SL con la finalidad de llevar a cabo la gestión contractual con ustedes. Puede ejercitar sus derechos de acceso, cancelación, rectificación y oposición, dirigiendo un escrito a nuestro domicilio social adjuntando fotocopia del DNI.