**SERVICIO**: OFICINA CISO

# CONTRATO DE PRESTACIÓN DE SERVICIOS

En Madrid, a 28 de diciembre de 2023

## INTERVIENEN

**De una parte:**
La mercantil **PONOS IBERICA SL** (en adelante, **PONOS**) con C.I.F. **B95921417**, y domicilio social sito en ALAMEDA RECALDE, 9 3º 48009 BILBAO, inscrita en el Registro Mercantil de Vizcaya, en el Tomo 5788 general, de la Sección 0 del Libro de sociedades, Folio 42, Hoja núm. BI-71835

**De otra parte:**
La mercantil **SEC&TECH4ALL 2023 SL** (en adelante, **SEC&TECH4ALL**) con C.I.F. **B56873680**, y domicilio social sito en Calle Pontevedra 64 28939 Arroyomolinos, Madrid.

A efectos del presente contrato (en lo sucesivo, **EL CONTRATO**) los intervinientes en su conjunto serán denominados en lo sucesivo **LAS PARTES**.

## ACTUAN

D. **José María García Orois**, mayor de edad, con DNI número **16.061.152-E**; en nombre y representación de **PONOS**; en su condición de apoderado según los poderes conferidos a su favor en fecha 25 de mayo de 2021, ante el Notario D. Ignacio Alonso Salazar, de Bilbao, bajo el número 1668 de su protocolo.

Don **Israel Díaz Domínguez**, mayor de edad, con D.N.I. núm. **52126397W**; en nombre y representación dSEC&TECH4ALL, en su condición de Administrador Único.

Quienes, reconociéndose mutuamente capacidad legal suficiente para la suscripción de los pactos contenidos en el presente **CONTRATO**, y manifestando expresamente la vigencia de sus respectivos poderes de representación:

## EXPONEN

**I.** Que **PONOS** es una empresa dedicada a la prestación de servicios de asistencia y consultoría tecnológica a diferentes clientes privados y públicos.

**II.** Que **SEC&TECH4ALL** es una sociedad dedicada, entre otras actividades, a la prestación de servicios de **CIBERSEGURIDAD y CISO Virtual** de Asitur, que se encuentra en disposición de colaborar con **PONOS** mediante la puesta a disposición de los medios materiales y humanos para la prestación de los servicios mencionados en condiciones de máxima calidad y eficiencia disponiendo para ello de personal especializado y de la infraestructura necesaria para la prestación de los servicios

- **a.** **SEC&TECH4ALL** manifiesta expresamente que no tiene limitación - incompatibilidad alguna, legal y/o contractual para la prestación de sus servicios profesionales y CISO Virtual de Asitur a **PONOS**.

**III.** Que **PONOS** está interesada en recibir los servicios dSEC&TECH4ALL consistentes en la prestación en favor de **PONOS** de los servicios de oficina de seguridad de Asitur (CISO).

En su virtud:

**LAS PARTES** han alcanzado un acuerdo sobre los términos aplicables, a cuyo efecto suscriben el presente **Contrato de prestación de servicios** sobre la base de las siguientes:

## ESTIPULACIONES

## A) OBJETO Y PRESTACIÓN DEL SERVICIO

### PRIMERA.- CUESTIONES PREVIAS: DEFINICIONES - IDONEIDAD DEL PROVEEDOR

#### 1.1 Código Ético: Buenas Prácticas

**PONOS** aplica sus principios éticos en las relaciones con sus proveedores, determinando los siguientes criterios en sus interacciones:

- **Lealtad y Honestidad:** Defendiendo las relaciones de libre mercado y respetando los criterios legales y sectoriales.
- **Calidad:** Proporcionando y gestionando todas las prestaciones de servicios con criterios de excelencia.
- **Respeto Normativo:** A todas las normas generales y sectoriales establecidas y concretamente a las referidas a la confidencialidad y respeto de la intimidad, protegiendo de los datos conocidos en nuestras relaciones mercantiles.
- **Objetividad y Transparencia:** En la valoración de bienes y servicios ofrecidos y recibidos, garantizando programas de mejora de estos, así como la independencia e imparcialidad en sus criterios de elección.
- **Implicación e integridad:** No se admitirá por parte de ningún proveedor la entrega en provecho propio o de un tercero de dadivas, presentes u ofrecimientos realizados a empleados o cualquier otra persona que tenga relación con estos y que tengan por objeto realizar un acto injusto y perjudicial para **PONOS**.

  No se entenderán como tales los presentes propios de la cortesía empresarial y comercial, si bien estos han de ser debidamente informados y registrados, según el protocolo vigente en cada momento. Esta obligación es de aplicación a los proveedores que tengan cualquier tipo de relación mercantil con **PONOS**. El incumplimiento de este requisito facultará a **PONOS** para la tomar las medidas sancionadoras oportunas, así como replantearse la continuidad de la relación mercantil de forma parcial o definitiva.

**SEC&TECH4ALL** se compromete a cumplir y llevar a la práctica tanto en el desarrollo de los Servicios que son objeto del presente Contrato como en el ejercicio diario de toda su actividad profesional los principios éticos de **PONOS** en relación a su actuación con proveedores

#### 1.2. Idoneidad Del Proveedor: Medidas Anti Fraude, Inspecciones, Auditorias y Verificaciones

**PONOS** se reserva la faculta de exigir en cualquier momento durante la vigencia del presente contrato cualesquiera documentos sean pertinentes para verificar la idoneidad [legal y operativa] del proveedor para poder prestar y seguir prestando los servicios contratados.

#### 1.2.1. Inspecciones y Auditorias

**PONOS** se reserva el derecho a auditar el cumplimiento puntual y correcto por parte del proveedor de sus obligaciones contractuales, debiendo comunicar a **SEC&TECH4ALL** la realización de tales auditorías con el preaviso referido a continuación y asumiendo el coste de estas, pudiendo solicitar las informaciones precisas a los efectos de constatar el buen funcionamiento de los Servicios contratados.

Las mencionadas auditorías e inspecciones se efectuarán previa notificación y con un preaviso de diez (10) días naturales, salvo que existan circunstancias que justifiquen un menor plazo de preaviso.

### SEGUNDA.- ANTECEDENTES, OBJETO Y ALCANCE DEL SERVICIO

#### 2.1. Antecedentes del contrato

**Asitur, client de Ponos,** se encuentra en estos momentos inmersa en un Plan Estratégico para su transformación y adaptación al mundo digital. Por ello, dentro de este Plan Estratégico cobra una relevancia fundamental el aseguramiento de la seguridad de la información de los sistemas de **PONOS,** como proveedor de Asitur. Por tanto, para fortalecer el nivel de madurez en ciberseguridad y seguridad de la Información de

**Asitur**, **PONOS** considera un factor clave de éxito la contratación del servicio oficina de seguridad de Asitur (CISO).

El servicio oficina de seguridad de Asitur (CISO) garantizará la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), la asesoría en materia de ciberseguridad y seguridad de la información al Comité de Seguridad de **Asitur**, incluyendo a los diferentes Grupos de Trabajo de Seguridad de **Asitur**, así como el reporte del Estado de Seguridad de la Información al Comité de Dirección de **Asitur** y al Consejo de Administración de **Asitur**. Asimismo, siguiendo las buenas prácticas de *ITIL v4*, el servicio no solo se centrará en su parte específica de operación de los sistemas de ciberseguridad, sino en la mejora continua y aplicación de las mejores prácticas, aumentando, y por lo tanto demostrando, que el nivel de madurez en ciberseguridad de **Asitur** aumenta.

Finalmente, hay que tomar en consideración que, a la fecha de firma del presente contrato, **Asitur** dispone tanto de un CISO externo como de un SOC (*Security Operations Center*) externo, ambos en proceso de cambio a un nuevo proveedor que preste dichos servicios. Por lo tanto, es fundamental que los servicios de servicio oficina de seguridad (CISO) objeto del presente contrato se adapten a dicho proceso de cambio, a las tecnologías actualmente contratadas por **Asitur** en materia de seguridad, así como al estado actual del plan de certificación en la ISO 27001 de **Asitur**.

En este sentido, **SEC&TECH4ALL** declara que ha recibido toda la información en relación con la infraestructura y los sistemas de ciberseguridad de PONOS necesaria para el estudio previo de los servicios objeto del presente contrato y que, por tanto, es conocedor de los requisitos y necesidades para la prestación de estos.

## 2.2. Objeto del contrato

El objeto del presente contrato es la prestación por **SEC&TECH4ALL** en favor de **PONOS** de los servicios de oficina de seguridad de Asitur (CISO) con el alcance previsto en la Estipulación 2.3, así como el resto de las condiciones previstas en el presente contrato.

En atención a la información a la que se va a acceder para la ejecución del objeto del presente contrato, **SEC&TECH4ALL** deberá disponer y cumplir con los estándares de seguridad y protección de datos de carácter personal.

## 2.3. Alcance del servicio

**LAS PARTES** acuerdan que los servicios de oficina de seguridad (CISO) que **SEC&TECH4ALL** se obliga a prestar en favor de **PONOS** tendrán el siguiente alcance:

### 2.3.1. Servicios respecto de los cuales **SEC&TECH4ALL** será responsable de su ejecución:

**A.- Servicios de seguridad**

- Miembro del Comité de Seguridad de **Asitur**.
- Implantación de la ISO 27001 en **Asitur**.
- Interacción con los servicios de administración de las plataformas de que dispone **Asitur**.
- Interacción con los proveedores de servicios de seguridad de **Asitur**.
- Interacción con los clientes y/o accionistas de **Asitur** que soliciten evaluaciones de riesgos de terceros, así como evaluaciones del nivel de seguridad de **Asitur**.

**B.- Procesos de gestión de incidentes y problemas**

Los procesos de gestión de incidentes y problemas son fundamentales para el correcto funcionamiento de un Centro de Operaciones de Seguridad (SOC) y del servicio de oficina de seguridad CISO de Asitur. Entre otras, las actividades mínimas que se desarrollan son:

- Gestión de incidentes.
- Escalamiento y priorización
- Notificación y comunicación.
- Investigación y análisis.
- Resolución y recuperación.
- Gestión de problemas.

- Mejora continua.

**C.- <u>Comunicación y notificación de incidentes</u>**

La comunicación y notificación de incidentes es un aspecto fundamental en la gestión de seguridad de un Centro de Operaciones de Seguridad (SOC) y del servicio de oficina de seguridad CISO de Asitur.

Actualmente **Asitur** dispone de una herramienta para gestionar tickets, Service Desk, que será de obligado uso para la gestión de tickets del SOC con **Asitur**.

Entre otras, las actividades mínimas del SOC que se desarrollan son:

- Proceso de notificación.
- Canales de comunicación (24x7).
- Información de notificación.
- Escalamiento de incidentes.
- Actualizaciones de estado.
- Coordinación con otras partes involucradas.
- Notificación post-incidente.

**D.- <u>Gobierno, Liderazgo y Estrategia</u>**

- Gobierno de la seguridad de la información.
    - Relación de la oficina con el resto de la organización.
    - Gestión de compromisos.
    - Asegurar que el equipo de gobierno tiene siempre contenido y actividad.
- Alineamiento del negocio y la estrategia.
    - Realización de análisis de madurez y análisis de mercado.
    - Articulación y definición de la estrategia de seguridad.
    - Programa de seguridad.
        - Establecer un *roadmap* a largo plazo.
        - Identificación de logros rápidos (*quick wins*).
- Relación con las partes interesadas (*stakeholders*).
    - Alineamiento con la estrategia corporativa.
    - Gestión de conflictos.
    - Creación de valor e innovación.
    - Gestión de expectativas.
    - Coordinación con el CSO, CRO, DPO y Consejo de Dirección.
- Métricas y Reporte.
    - Métricas operacionales y de ejecución.
    - Indicadores de riesgo.
    - Validación de la efectividad de las métricas.
- Financiero.
    - Creación de casos de negocio y cálculos de ROI.
    - Gestión y monitorización del presupuesto.
- Diseño de la organización.
    - Definición de roles y perfiles.
    - Diseño de la organización.
    - Gestión del cambio organizativo.
    - Desarrollo del talento del equipo.

**E.- <u>Riesgos y Controles</u>**

- Marcos de gestión de Riesgos.
    - Conocimiento de los siguientes marcos y leyes:
        - ISO 27001.
        - RGPG/LOPDGDD.
        - COBIT.
    - Aseguramiento de los controles.

        - Gestión del riesgo.
        - Revisión y controles.
        - Informes.
        - Auditorías Internas y externas.
- Gestión del Riesgo.
    - Plan de valoración del riesgo.
    - Gobierno del riesgo.
    - Gestión del riesgo.
    - Procesos de aceptación del riesgo.
- Mejora Continua.
    - Chequeos de la salud de la seguridad.
        - Tests table top.
        - Situación del riesgo tecnológico.
        - Propuestas de remediación.
    - Valoración de la preparación ante incidentes.
    - Valoración de los controles de IT.
    - Capacidad de valoración y/o realización de detección de amenazas.
    - Planificación priorizada de las acciones de remediación.

**F.- <u>Cumplimiento y Legal</u>**

- Aseguramiento del cumplimiento.
    - Interno.
        - Revisión de la gestión Interna.
        - Gestión y/o realización de auditorías internas.
    - Externo.
        - Gestión y/o realización de auditorías externas.
- Gestión de requerimientos externamente impuestos.
    - Regulación de protección de datos.
    - Directivas, Leyes y Reglamentos.
- Requerimientos de cumplimientos internos.
    - Políticas y estándares de seguridad.
    - Requerimientos no funcionales de proyectos.
    - Realizar publicaciones y concienciación.
    - Cumplimiento de la cadena de producción.
- Retención y destrucción de datos.
    - Políticas de retención de datos.
    - Planificación de las retenciones.
    - Aseguramiento de cumplimiento de políticas por parte del negocio.

**G.- <u>Securizar el negocio</u>**

- Diseño seguro del on boarding / finalización.
    - Trabajadores de la organización.
    - Clientes y partners.
    - Suministradores.
- Diseño y gestión para securizar iniciativas nuevas del negocio.
    - Identificación de nuevas iniciativas.
    - Incorporación a las existentes.
- Diseño y gestión del plan de continuidad del negocio.
    - Planificar escenarios de *cyber*ataque.
    - Seguridad de los planes de continuidad del negocio.
- Diseño y gestión del comportamiento del empleado.
    - Concienciación del empleado / cultura del riesgo.
        - Formación y concienciación.
- Adquisiciones y fusiones.

- Gestión del riesgo: antes, durante y después de la adquisición.
- Diseñar la Integración de lo adquirido.

**H.- <u>Operaciones Seguridad</u>**

- Gestión de incidentes.
  - Aseguramiento de la participación de todos los afectados.
  - Proceso de Incidentes.
    - Plan de crisis: escenario de *cyber*ataque.
  - Integración con otros planes relacionados.
    - Plan de crisis.
    - Plan de brecha de datos personales.
    - Plan de continuidad de negocio.
- Gestión del proceso de las vulnerabilidades.
- Diseño del SOC.
  - Transferencia del Conocimiento.
  - Identificación de métricas e indicadores.
  - Gestión del proveedor.
  - Análisis de mercado de la industria del SOC.

**I.- <u>Asegurar nuevas iniciativas</u>**

- Diseño.
  - Definición de arquitecturas de seguridad.
  - Definición de requerimientos de seguridad y requerimientos no funcionales.
- Aseguramiento y gestión del test de la seguridad.
  - Certificación y acreditación de los requerimientos.

**J.- <u>Securizar la cadena de suministro</u>**

- Revisión de los precontratos.
- Contratos.

**K.- <u>Diseño de la securización de la tecnología</u>**

- Acceso & Identidad.
  - Políticas de claves.
  - Conocimiento de las tecnologías de identidad y acceso.
- Tecnologías emergentes e innovadoras.
  - *Blockchain*.
  - *Cryptomonedas*.
  - Inteligencia artificial y robotización.
- Seguridad en la Nube.
  - Estrategia *SaaS*.
  - Controles de seguridad en la nube.
    - Arquitectura segura en la nube.
- Seguridad en el puesto.
  - Políticas de claves.

2.3.2. <u>Servicios respecto de los cuales **SEC&TECH4ALL no será responsable de su ejecución**, pero sí de identificar los requisitos, asegurar su cumplimiento y monitorizar la actividad desde el inicio al fin:</u>

**A.- <u>Riesgos y Controles</u>**

- Mejora Continua.
  - Test de Penetración.

**B.- <u>Securizar el negocio</u>**

- Comportamiento del empleado.
  - Investigaciones forenses.

**C.- <u>Operaciones Seguridad</u>**

- Operaciones de plataformas de seguridad.
  - Operación y monitorización.
  - Actualización de las tecnologías.
- Gestión de incidentes.
  - Proceso de Incidentes.
    - Manuales de ejecución según tipo de incidente crítico.
    - Test de incidentes.
    - Orquestación de la Seguridad (SOAR).
    - Respuesta y detección gestionada.
  - Soporte a las acciones forenses 24x7.
- Gestión de amenazas.
  - Alertas de herramientas de seguridad.
  - Análisis de *logs*, correlación, SIEM y análisis de flujo de red (*netflow*).
  - Alimentación con amenazas de plataformas *opensource* o comerciales.
  - Caza de la amenaza (*Thread hunting*): automatizada y manual.
  - DNS, *Social Media* & *Dark Web*.
- Gestión de las vulnerabilidades
  - Identificación.
    - Alcance y descubrimiento de activos.
  - Remediación.
    - Propuesta para solucionar vulnerabilidades.
    - Verificación.
    - Métricas y líneas base.
- Diseño del *SOC*.
  - Entrenamiento continuo.
- Operaciones del *SOC*.
  o Manuales de ejecución y procedimientos del *SOC*.
  o Informes de métricas e indicadores.
  o Integración del *SOC* con el *sevice desk*.
  o Ejercicios de *cyber*ataque.

**D.- <u>Asegurar nuevas iniciativas</u>**

- Integrar la seguridad y el riesgo dentro de la PMO y el ciclo de vida del Software.
  - Metodologías Cascada, *Agile* y *DevOps*.
- Diseño.
  - Revisión de código y formación a los programadores.
  - Definición de estándares de desarrollo.
- Aseguramiento y test de la seguridad.
  - Revisión de código.
  - Test de vulnerabilidad de las aplicaciones.
  - Test de penetración.
  - Aseguramiento continuo.

**E.- <u>Securizar la cadena de suministro</u>**

- Revisión de los precontratos.
  - Valoración interna (*self assesment*).
  - Auditorías.
- Contratos.
  - Nuevos contratos.
  - Renovación de contratos.
- Revisión y aseguramiento.
  - Valoración interna (*self assesment*).
  - Auditorías.

**F.- <u>Securizar la tecnología</u>**

- Seguridad de la infraestructura y Sistemas Operativos de servidores.
  - Continuidad del servicio y recuperación ante desastres.
  - *Hardening*.
  - Parcheo.
  - Protección *antimalware* y APT.
  - Backups, replicación, sitios múltiples.
  - HIPS.
  - Monitorización de la seguridad.
- Aplicación de la seguridad.
  - Gobierno del acceso a los datos.
    - Propietario de la información y custodio.
    - Controles de acceso a las aplicaciones.
    - Controles de acceso basados en roles.
  - Monitorización de la seguridad.
  - Monitorizar la integridad de los ficheros.
- Acceso & Identidad.
  - Gestión de claves y credenciales.
- Seguridad Física.
  - Monitorización y control de acceso físico.
  - Detección y respuesta de intrusión.
  - Prevención de robo.
  - Redundancia.
- Seguridad de la red.
  - DDoS.
  - *Firewalls*, IDS, IPS.
  - Acceso remoto seguro.
  - Filtrado de contenido.
  - Seguridad las redes Wireless.
  - Redes virtuales, SD WAN.
  - Ampliación del perímetro.
- Seguridad en la Nube.
  - Controles de seguridad en la nube.
    - Arquitectura segura en la nube.
    - CASB.
    - Seguridad de la máquina virtual.
    - Integración *cloud to cloud*.
    - Virtualización de *appliances*.
    - Integración de la monitorización.
    - Acceso a datos corporativos de sitios no corporativos.
- Seguridad en el correo electrónico.
  - Controles *Antispam*.
  - Phishing.
  - Cifrado del correo.
- Seguridad en el puesto.
  - *Hardening*.
  - Parcheo.
  - *Antimalware*.
  - HIPS/EDR.
  - Monitorización de la seguridad / UBA.
  - Cifrado.
  - Inventario de aplicaciones y control del despliegue.
  - Segregación de los datos.

  - Dispositivos robados/perdidos.
  - Almacenamiento de los datos en la nube.
  - Localización de dispositivos.
- Seguridad del Dato.
  - Mapeo de datos y procesos.
  - Seguridad en la analítica de datos.
  - Cifrado y enmascaramiento.
  - Prevención de robo/perdida de datos.

## TERCERA.- EJECUCIÓN DE LOS SERVICIOS, CERTIFICACIONES Y PERSONAL DEL PROVEEDOR

### 3.1. Ejecución de los servicios

**LAS PARTES** acuerdan que los servicios objeto del presente contrato se ejecutarán mediante un modelo de **90 horas mensuales** de trabajo cada una de ellas.

No obstante, el número de horas de trabajo mensuales podrá ser ampliado por acuerdo entre **LAS PARTES** de acuerdo con las tarifas previstas en la **Estipulación QUINTA**.

### 3.2. Certificaciones de SEC&TECH4ALL necesarias para la prestación de los servicios

En atención a la importancia de las funciones de la oficina de seguridad (CISO), **EL PROVEEDOR** garantiza que el personal que implique en la prestación de los servicios objeto del presente contrato dispondrá de las siguientes certificaciones:

1. Máster Universitario en el campo de la ciberseguridad (sólo los reglados y oficiales).
2. CISM: Certified Security Systems Security Professional ó CISSP: Certified Security Systems Security Professional.
3. Formación en Protección de Datos siguiendo el esquema AEPD-DPD.
4. PMP: Project Management Professional.
5. ISO 27001 Lead Implementer.
6. COBIT v5: Control Objectives for Information and related Technology.
7. CISA: Certified Security Systems Security Auditor
8. ITIL expert v4: Information Technology Infrastructure Library
9. TOGAF: The Open Group Architecture Framework v9
10. ITIL Information Technology Infrastructure Library (ITIL expert v4 ó ITIL expert v3).
11. ISO9001 Auditor (Internal o External)

**PONOS** se reserva el derecho de exigir en cualquier momento de la vigencia del presente contrato las evidencias que **PONOS** estime suficientes para comprobar la veracidad del compromiso previsto en la presente Estipulación.

### 3.3. Personal de SEC&TECH4ALL implicado en la ejecución de los servicios y órganos de decisión de PONOS

**SEC&TECH4ALL** dispondrá todos los medios y capacidad productiva necesaria para la prestación de los servicios objeto del presente contrato. **SEC&TECH4ALL** prestará los servicios objeto del contrato siendo su responsabilidad disponer de los medios técnicos y de organización precisos para su ejecución debiendo contar con los equipos necesarios y el personal suficientemente cualificado para la ejecución de estos en los términos previstos en el presente contrato.

**SEC&TECH4ALL** deberá contar en todo momento con una dimensión de empleados adecuada para la prestación de los servicios a los que se compromete, así como garantizar que, durante todo el periodo de duración del contrato, aquellos cuentan con el perfil profesional necesario para la prestación de los servicios a los que se obliga **SEC&TECH4ALL** en virtud del presente contrato. El servicio será liderado por un concreto empleado dSEC&TECH4ALL independientemente seleccionado por éste, el cual prestará sus servicios bajo las instrucciones y condiciones que aquel prevea.

**SEC&TECH4ALL** ostentará con total independencia las facultades de dirección y control de sus empleados que intervengan en la prestación de los servicios objeto del presente contrato y desarrollará las actuaciones que considere pertinentes en base a su régimen disciplinario con total independencia con base en los criterios y

procedimientos que haya previsto. Asimismo, **SEC&TECH4ALL** otorgará y coordinará los periodos de vacaciones anuales, permisos, licencias o ausencias de cualquier tipo del personal que intervengan en la prestación de los servicios con total independencia.

No obstante, **SEC&TECH4ALL** garantiza que el empleado de **SEC&TECH4ALL** que lidere los servicios de oficina de seguridad (CISO) contará con la siguiente formación:

1. Máster Universitario en Seguridad de las tecnologías de la Información y las Comunicaciones.
2. Ingeniería Técnica de Telecomunicación.
3. Master MBA.

## CUARTA. NIVELES DE SERVICIO Y PENALIZACIONES POR SU INCUMPLIMIENTO

### 4.1 Niveles de servicio

**SEC&TECH4ALL** se obliga a cumplir los siguientes niveles de servicio durante la ejecución de los servicios objeto del presente contrato:

**1.- Tiempo de respuesta ante incidentes de seguridad críticos:**

**SEC&TECH4ALL** se obliga a responder conforme al alcance previsto en la Estipulación 2.3 a los incidentes de seguridad críticos dentro de un plazo máximo de dos (2) horas desde que le sea comunicado el incidente por **PONOS**. Se definen los incidentes de seguridad críticos como aquellos en los que el sistema de producción está gravemente afectado o fuera de funcionamiento y/o las operaciones de sistema o las aplicaciones comerciales críticas no funcionan.

**LAS PARTES** acuerdan que, en caso de que se comunique a **SEC&TECH4ALL** un incidente de seguridad crítico que requiera la respuesta de **SEC&TECH4ALL** dentro del horario de lunes a viernes de 9:00 a 13:00 (excluyendo los correspondientes a la Comunidad de Madrid), estos servicios se incluirán dentro del precio pactado en la Estipulación 5.1 para la prestación de los servicios de oficina de seguridad (CISO). No obstante, **LAS PARTES** acuerdan que, en caso de que se comunique a **SEC&TECH4ALL** un incidente de seguridad crítico que requiera la respuesta de **SEC&TECH4ALL (I)** de lunes a viernes de 13:01 a 8:59 (excluyendo los festivos correspondientes a la Comunidad de Madrid) y/o **(II)** en sábados, domingos o festivos correspondientes a la Comunidad de Madrid, se aplicará por **SEC&TECH4ALL** a **PONOS** el precio previsto en la Estipulación 5.1

**2.- Disponibilidad del servicio**

**SEC&TECH4ALL** se compromete a garantizar una disponibilidad del servicio del 99,98%.

**3.- Nivel de satisfacción de PONOS**

Mide el grado de satisfacción de **PONOS** con los servicios proporcionados por **SEC&TECH4ALL**. Este nivel de servicio se medirá a través de encuestas, retroalimentación y revisiones periódicas con los clientes.

**SEC&TECH4ALL** se compromete a conseguir, como mínimo, un nivel de satisfacción del 85%. La valoración del nivel de satisfacción se realizará mensualmente por **Asitur** utilizando la ficha de evaluación de proveedores de **Asitur** que **SEC&TECH4ALL** declara conocer y aceptar. Asimismo, en el acta de aceptación de las facturas de **PONOS** que se elaborará con una frecuencia mensual se realizará por **PONOS** un segundo seguimiento del servicio prestado.

**4.- Informes y métricas**

**SEC&TECH4ALL** se compromete a proporcionar informes regulares sobre eventos de seguridad, incidentes, métricas clave y recomendaciones para mejoras de seguridad. La valoración del cumplimiento de este nivel de servicio se realizará mensualmente por **Asitur** utilizando la ficha de evaluación de proveedores de **Asitur** que **SEC&TECH4ALL** declara conocer y aceptar. Asimismo, en el acta de aceptación de las facturas de **PONOS** que se elaborará con una frecuencia mensual se realizará por **PONOS** un segundo seguimiento del servicio prestado.

**5.- Auditorías y cumplimiento**

**SEC&TECH4ALL** se compromete a prepararse para auditorías de seguridad y a proporcionar asistencia durante las mismas. La valoración del cumplimiento de este nivel de servicio se realizará mensualmente por **Asitur** utilizando la ficha de evaluación de proveedores de **Asitur** que **SEC&TECH4ALL** declara conocer y aceptar. Asimismo, en el acta de aceptación de las facturas de **PONOS** que se elaborará con una frecuencia mensual se realizará por **PONOS** un segundo seguimiento del servicio prestado.

**6.- Acceso a informes**

El acceso a informes son componentes importantes en el servicio de oficina de seguridad de Asitur(CISO) para permitir a **PONOS** acceder a la información y los informes relevantes sobre la seguridad de su entorno. Entre otras, las actividades mínimas que **SEC&TECH4ALL** deberá ejecutar son:

- Acceso a informes.
- Personalización de informes.
- Notificaciones y alertas.
- Historial de informes.

La valoración del cumplimiento de este nivel de servicio se realizará mensualmente por **Asitur** utilizando la ficha de evaluación de proveedores de **Asitur** que **SEC&TECH4ALL** declara conocer y aceptar. Asimismo, en el acta de aceptación de las facturas de **PONOS** que se elaborará con una frecuencia mensual se realizará por **PONOS** un segundo seguimiento del servicio prestado.

### 4.2. Penalizaciones por incumplimiento de los niveles de servicio

**LAS PARTES** acuerdan las siguientes penalizaciones en caso de no cumplirse los niveles de servicio previstos en la Estipulación 4.1:

**1.- Tiempo de respuesta ante incidentes de seguridad críticos:**

Se aplicará una penalización de **6.350€** en caso de incumplimiento de **SEC&TECH4ALL** del plazo de respuesta de, como máximo, dos (2) horas ante incidentes de seguridad críticos.

**2.- Disponibilidad del servicio**

Se aplicará una penalización de 100€ mensuales si la disponibilidad del servicio mensual es inferior al 99,98%

**3.- Nivel de satisfacción de PONOS**

Se aplicará una penalización de 100€ mensuales si el nivel de satisfacción mensual es inferior al 85**%.**

**4.- Informes y métricas**

Se aplicará una penalización de 100€ mensuales si **SEC&TECH4ALL** no proporciona los informes regulares sobre eventos de seguridad, incidentes, métricas clave y recomendaciones para mejoras de seguridad.

**5.- Auditorías y cumplimiento**

Se aplicará una penalización de 100€ mensuales si **SEC&TECH4ALL** no prepara de modo suficiente y adecuado las auditorías de seguridad y ni proporciona asistencia suficiente y adecuada durante las mismas.

**6.- Acceso a informes**

Se aplicará una penalización de 100€ mensuales si **Asitur** no puede acceder a la información y los informes relevantes sobre la seguridad de su entorno.

Para el pago de las penalizaciones por parte de **SEC&TECH4ALL** a **PONOS, LAS PARTES** acuerdan aplicar el instituto del pago por compensación previsto en los artículos 1195, 1196 y 1197 del Código Civil, por lo que **PONOS** podrá deducir del importe de las facturas emitidas por **SEC&TECH4ALL** en virtud del presente contrato, la cantidad que corresponda de conformidad con la aplicación de las penalizaciones previstas en la presente clausula.

## B) CONDICIONES ECONÓMICAS

### QUINTA.- PRECIO Y FACTURACIÓN

#### 5.1. Precio (IVA no incluido)

- El precio pactado por **LAS PARTES** para la ejecución de la totalidad de los servicios incluidos en el presente contrato y sus anexos es el previsto a continuación:

  **A.** **Prestación de servicios de oficina de seguridad de Asitur(CISO): 6.350 €/mes** (Impuestos no incluidos). No obstante, **LAS PARTES** acuerdan que, si en aplicación de lo previsto en la **Estipulación TERCERA**, acuerdan aumentar el número de 90 horas de trabajo mensuales, estas tendrán un precio de **70.54 €** por cada hora adicional.

  **B.** **Respuesta ante incidentes de seguridad críticos fuera de horario de oficina:**

  **a.** **Las respuestas ante incidentes de seguridad críticos ejecutadas por SEC&TECH4ALL de lunes a viernes de 13:01 a 8:59 (excluyendo los festivos correspondientes a la Comunidad de Madrid)** tendrán un precio de **70,54€** (Impuestos no incluidos) por cada hora o fracción de hora de trabajo necesaria para la respuesta dSEC&TECH4ALL ante el incidente de seguridad crítico. **SEC&TECH4ALL** deberá de acreditar a **PONOS** las horas de trabajo ejecutadas para la respuesta ante los incidentes de seguridad críticos para que se produzca el devengo del precio pactado para estas.

  **b.** **Las respuestas ante incidentes de seguridad ejecutadas por SEC&TECH4ALL en sábado, domingo y/o festivo correspondiente a la Comunidad de Madrid** tendrán un precio de **141,08€** (Impuestos no incluidos) por cada hora o fracción de hora de trabajo necesaria para la respuesta de **SEC&TECH4ALL** ante el incidente de seguridad crítico. **SEC&TECH4ALL** deberá de acreditar a **PONOS** las horas de trabajo ejecutadas para la respuesta ante los incidentes de seguridad críticos para que se produzca el devengo del precio pactado para estas.

- Los precios indicados en atención al alcance del presente contrato son **absolutamente cerrados**, encontrándose comprendido en el precio todos los jornales, medios y materiales que sean precisos, antecedentes, coetáneos o posteriores, para su correcta y adecuada ejecución, así como cualquier desplazamiento que fuera necesario realizar a las oficinas de **Asitur** por parte de **SEC&TECH4ALL**.

#### 5.2. Devengo, Facturación y Pago

- El **devengo** se producirá mensualmente desde el inicio de los servicios de acuerdo con lo previsto en la **Estipulación SEXTA**.
- **SEC&TECH4ALL** emitirá una factura por el precio de los servicios establecido en el contrato en el plazo de treinta (30) días desde su devengo.
- **Pago y forma de pago**: mediante transferencia bancaria a treinta (30) días desde la recepción de la factura, en el número de cuenta titularidad de **SEC&TECH4ALL**.

#### 5.3. Requisitos de Exigibilidad

- Expresamente se excluyen de la obligación de pago por **PONOS** todas aquellas facturas emitidas con ocasión de la prestación realizada por **SEC&TECH4ALL** sin existir orden, autorización o validación expresa para ello.
- En cualquier caso, para que SEC&TECH4ALL pueda exigir el pago de toda clase de prestaciones terminadas serán requisitos inexcusables la presentación por **SEC&TECH4ALL** a **PONOS** todos y cada uno de los siguientes documentos, a saber:
  1) **Acreditación de la vigencia del seguro de responsabilidad civil** a que se refiere la **ESTIPULACIÓN NOVENA** del presente contrato.
  2) Certificados acreditativos de encontrase al corriente de pagos de sus obligaciones fiscales de la Seguridad Social de acuerdo con lo previsto en la **ESTIPULACION OCTAVA.**
- La falta de entrega de todos o algunos de los anteriores documentos faculta a **PONOS** a suspender el pago de las correspondientes facturas hasta que se subsane dicha falta de entrega de documentación.

## C) VIGENCIA Y DURACIÓN

### SEXTA.- ENTRADA EN VIGOR / DURACIÓN

El presente contrato entrará en vigor en la fecha de firma del contrato, que coincide con la del encabezado, y tendrá una duración de un (1) año natural desde entonces. Una vez transcurrido el plazo de duración inicialmente pactado, este se renovará automáticamente por periodos anuales sucesivos, salvo que **PONOS** comunique a **SEC&TECH4ALL** expresamente y por escrito con una antelación mínima de quince (15) días a la fecha de finalización de la duración inicial del contrato y de sus sucesivas prórrogas su voluntad de no proceder a la renovación del contrato. Asimismo, **SEC&TECH4ALL** podrá comunicar a **PONOS** expresamente y por escrito con una antelación mínima de tres (3) mes a la fecha de finalización de la duración inicial del contrato y de sus sucesivas prórrogas su voluntad de no proceder a la renovación del contrato.

### SÉPTIMA.- RESOLUCIÓN

#### 7.1. Regla General: Supuestos de Resolución Anticipada mediando Plazo de Preaviso

**PONOS** podrá resolver el presente contrato en cualquier momento con un simple preaviso de quince (15) días de antelación a la fecha de resolución, sin que por ello se devengue derecho indemnizatorio a favor de cualquiera de **LAS PARTES.**

A su vez, **SEC&TECH4ALL** podrá resolver el presente contrato en cualquier momento con un simple preaviso de tres (3) meses de antelación a la fecha de resolución, sin que por ello se devengue derecho indemnizatorio a favor de cualquiera de **LAS PARTES.**

#### 7.2. Regla Especial: Supuestos de resolución en caso de incumplimiento y supuestos de resolución sin necesidad de que medie plazo de preaviso

**Las PARTES** estarán facultadas a resolver el presente CONTRATO en caso de incumplimiento de la otra **PARTE**, siempre que haya notificado el incumplimiento y su intención de resolver el CONTRATO y, en el plazo de diez (10) días desde tal notificación, la **PARTE** incumplidora no haya subsanado su incumplimiento.

No obstante, cada **PARTE** podrá resolver el CONTRATO mediante simple notificación y sin necesidad de preaviso cuando la otra PARTE haya incumplido alguna de sus obligaciones esenciales, entendiéndose por tales las siguientes:

- Incumplimiento del Código Ético definido en la Estipulación 1.1.
- Incumplimiento de los compromisos previstos en la Estipulación 3.2.
- Incumplimiento del calendario de ejecución fijado en la Estipulación 4.1.
- Incumplimiento de las obligaciones de pago en tiempo y forma establecidas en las Estipulaciones 5.1, 5.2 y 5.3.
- Incumplimiento de las obligaciones fiscales, laborales y de seguridad social detalladas en la Estipulación 8.
- Incumplimiento de cualquiera de **LAS PARTES** de las limitaciones consignadas en la Estipulación 12 relativa a – PERSONAL -.
- Incumplimiento de las obligaciones en materia de tratamiento de datos de carácter personal y de confidencialidad recogidas en la Estipulación 14.

En los supuestos previstos en el presente contrato en virtud de los cuales se faculte a cualquiera de **LAS PARTES** a proceder con la resolución anticipada sin necesidad de que medie plazo de preaviso, a salvo de la notificación en dicho sentido, no se devengará indemnización alguna a cargo de quien hubiera ejercitado dicha resolución anticipada.

En el caso en el que la resolución del presente contrato hubiera venido motivada por un incumplimiento previo de las obligaciones asumidas por la otra parte, en virtud del mismo, la parte incumplidora vendrá obligada a abonar a la otra parte la indemnización por los daños y perjuicios que le hubiera causado su incumplimiento.

### 7.3. Protocolo de Actuación en supuestos de Resolución / Finalización del Contrato

En todos los casos tras la **RESOLUCION Y/O TERMINACION DEL CONTRATO, EL PROVEDOR** quedará obligado a suministrar toda la documentación e información de los sistemas administrados en ejecución del presente contrato y que permitan a **PONOS** tomar el control de estos con plena operatividad, prestando **SEC&TECH4ALL** su máxima colaboración en el traspaso de la tecnología.

## D) RESPONSABILIDAD

### OCTAVA.- CUMPLIMIENTO DE OBLIGACIONES FISCALES / LABORALES Y DE LA SEGURIDAD SOCIAL

- **SEC&TECH4ALL** manifiesta estar al día de la fecha al corriente de sus obligaciones fiscales, con la Seguridad Social y con sus propios trabajadores, así como de la aplicación de la normativa de Prevención de Riesgos Laborales asumiendo la responsabilidad plena para el pago de cuantas obligaciones se deriven de las relaciones de trabajo que tenga establecidas con el personal que desempeñe los servicios contratados.

  A tal efecto, son obligaciones esenciales las siguientes:
  - **Entregar a PONOS**, **dentro de los quince días siguientes a la firma del presente contrato**, el **certificado específico de encontrarse, al corriente de sus obligaciones tributarias** y al que hace referencia el art. 43 f) de la Ley General Tributaria *(Ley 58/2003).* Esta certificación deberá ser renovada y entregada a **PONOS** con carácter semestral durante la vigencia del Contrato.
  - **Entregar a PONOS en el plazo máximo de quince días desde la entrada en vigor de este Contrato, certificación negativa de descubiertos emitida por la Tesorería General de la Seguridad Social**, y a la que se refiere el art. 42 del Estatuto de los Trabajadores. Esta certificación deberá ser renovada y entregada a **PONOS** con carácter semestral durante la vigencia de este Contrato.
- La entrega a **PONOS** de los Certificados referidos en la presente estipulación se configura como condición esencial del presente contrato.

  El incumplimiento de estas dos obligaciones precedentes por parte del **PROVEEDOR** dará derecho a **PONOS** a optar entre:
  - Suspender de forma cautelar el abono de los pagos a favor del **PROVEEDOR** por los servicios prestados hasta el momento de regularizar la presentación de los certificados o sus prórrogas y, en su caso, a retener y compensar el importe económico de los descubiertos que en materia de cuotas de Seguridad Social o deudas fiscales tenga **EL PROVEEDOR** en garantía y aseguramiento de la responsabilidad solidaria y/o subsidiaria que pudiera derivarse a **PONOS** en esta materia.
  - Resolver inmediatamente sin respetar el plazo de preaviso del presente contrato comunicándoselo por escrito y sin derecho a indemnización alguna para el **PROVEEDOR**.

### NOVENA.- RESPONSABILIDAD CIVIL

**El PROVEEDOR llevará a cabo las prestaciones objeto del presente contrato a su propio riesgo y ventura**, sin excepción de clase alguna. Asimismo, asume la responsabilidad por el trabajo ejecutado por las personas que ocupare en la Prestación.

**SEC&TECH4ALL** declara y garantiza que para la ejecución de la prestación dispone de los derechos de propiedad intelectual sobre los programas y aplicaciones informáticas que utilice para el desarrollo de esta siendo éstos de su propiedad y/o en su caso dispone de las oportunas licencias de uso válido a dichos efectos.

Para garantizar dicha responsabilidad, **SEC&TECH4ALL** se obliga, durante la vigencia del presente contrato y sus prórrogas, a tener vigente una póliza de seguro de responsabilidad civil incluyendo la cobertura por responsabilidad patronal.

**SEC&TECH4ALL** remitirá a **PONOS** copia íntegra de la póliza vigente suscrita en cumplimiento de la anterior obligación, así como justificante del pago anual de la prima correspondiente a dicha póliza.

Cada una de las partes responderá ante la otra de los daños y perjuicios de toda índole que se deriven del incumplimiento de cualquiera de las obligaciones asumidas por cada una de ellas en el presente contrato.

## DÉCIMA.- MULTAS Y SANCIONES

**SEC&TECH4ALL** no podrá repercutir contra **PONOS** multa, sanción o cualquier tipo de responsabilidad que por incumplimiento de alguna de las obligaciones referidas en presente contrato le impongan las autoridades competentes y, si fuera el caso, se acuerda expresamente que **SEC&TECH4ALL** indemnizará a **PONOS** de toda cantidad que se viese obligado a pagar por incumplimiento de las obligaciones aquí señaladas, aunque ello le venga impuesto por resolución judicial y/o administrativa.

# E) AUTORIZACIONES / LIMITACIONES

## DECIMOPRIMERA.- CESIÓN DEL CONTRATO Y SUBCONTRATACIÓN

**SEC&TECH4ALL** se compromete a no ceder los derechos dimanantes del presente contrato sin previa autorización escrita de **PONOS** que no podrá ser denegada sin justa causa.

Asimismo, solo podrá subcontratar los servicios descritos en el presente contrato a las entidades que previamente designe bastando la mera comunicación para llevar a cabo tal subcontratación, si bien, esta se referirá a servicios parciales y de soporte del servicio contratado, exigiendo las mismas obligaciones que las asumidas en el presente contrato y sus anexos y respondiendo íntegramente frente a **PONOS**.

## DECIMOSEGUNDA.- PERSONAL

**LAS PARTES** durante la vigencia del presente contrato y en los 6 meses posteriores a la finalización y/o terminación del mismo, cualquiera que fuera su causa, se comprometen a no reclamar activamente ni a realizar ofertas de empleo al personal laboral implicado de la otra parte en el objeto del referido contrato y en la ejecución del mismo, a salvo de que se disponga de expresa autorización de **PONOS** o **SEC&TECH4ALL**, según corresponda. Se excluye de la presente limitación aquel personal de cada una de las partes que hubiera cesado en su relación laboral con su respectiva empresa con motivo de una situación de despido.

En caso de incumplimiento las limitaciones consignadas en el párrafo anterior y/o la aceptación de una oferta de trabajo por parte del personal laboral de cada parte e implicado en el objeto del presente contrato, durante la vigencia del mismo y en los 6 meses posteriores a su finalización, exceptuando situaciones de despido conforme lo descrito en el apartado previo, la parte incumplidora estará obligada a indemnizar a la otra parte en una cuantía por cada incumplimiento, a modo de clausula penal, equivalente a tres mensualidades de salario bruto del trabajador afectado y tomando como referencia el salario bruto mensual del empleado al tiempo de la firma del presente contrato.

No obstante, **LAS PARTES** acuerdan expresamente que, a partir del sexto mes de vigencia del presente contrato, no será de aplicación lo previsto en la presente cláusula exclusivamente para el caso de que **PONOS** decida internalizar al empleado de **SEC&TECH4ALL** que lidere la oficina de seguridad (CISO) requiriéndose en tal caso la conformidad de dicho empleado y una simple comunicación escrita por parte de **PONOS** a **SEC&TECH4ALL**.

## DECIMOTERCERA.- PROPIEDAD INTELECTUAL E INDUSTRIAL

### 13.1. Respecto del servicio ejecutado

**SEC&TECH4ALL** declara y garantiza que para la prestación de los servicios dispone de los derechos de propiedad intelectual sobre los programas y aplicaciones informáticas que utilice para esta, siendo estos de su propiedad y/o en su caso dispone de las oportunas licencias de uso validas a dichos efectos. De acuerdo con la anterior manifestación, que resulta de imposible verificación por parte de **PONOS**, **SEC&TECH4ALL** exonera expresamente a **PONOS** de cualquier género de responsabilidad ante cualquier reclamación a instancias de un tercero.

El presente Contrato no implica otorgamiento de **PONOS** a **SEC&TECH4ALL** de licencia, permiso o derecho expreso o implícito para el uso de derecho de propiedad industrial o intelectual de las herramientas informáticas que fuera titular o tuviera legítima autorización de uso.

### 13.2. Respecto del producto de los servicios ejecutados

La titularidad de la obra resultante de la ejecución de los servicios previstos en el presente contrato recaerá única y exclusivamente sobre **PONOS** de conformidad con lo dispuesto en el art. 97 y ss. del Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

En dicho sentido, corresponden única y exclusivamente a **PONOS** los derechos de explotación de conformidad con lo dispuesto en el art. 99 del referido cuerpo legal, toda vez que, **PONOS** será el titular único y que ostente la propiedad intelectual e industrial de cualquier obra resultante de la ejecución de los servicios objeto del presente contrato, considerándose como tal, sin que impliquen limitación, toda la documentación, registros y datos, entre otros, tanto si se trata de obra nueva como de obra derivada de otra existente o adaptaciones de metodologías realizadas conjuntamente.

En relación a la cesión de los derechos de explotación se acuerda por **LAS PARTES** lo siguiente:

**1)** Que la cesión se realiza sin límite de tiempo ni límite territorial.
**2)** Que se refiere a cualesquiera modalidades de explotación y medios de difusión conocidos en la actualidad o por conocer en el futuro.
**3)** Que la cesión se confiere en régimen de exclusividad, con facultad de cesión total o parcial a terceros.
**4)** Que **SEC&TECH4ALL** se obliga a suscribir todos aquellos documentos contractuales que fuesen necesarios para garantizar la cesión de derechos en el supuesto de que así fuera necesario.
**5)** Que **SEC&TECH4ALL** accede, irrevocablemente a que se practiquen cualesquiera modificaciones en el producto que sean necesarias y a que la explotación de este se realice de la forma más conveniente para **PONOS** en cada momento.
**6)** Que **SEC&TECH4ALL** declara, bajo su exclusiva responsabilidad, que ostenta todos los derechos, facultades y títulos necesarios para operar la presente cesión de derechos de explotación en materia de propiedad intelectual y/o industrial a favor de **PONOS**.

En consecuencia, **SEC&TECH4ALL** deberá entregar a **PONOS** la documentación producida durante la ejecución de los servicios previstos en el presente contrato a la terminación de este, cualquiera que fuera el motivo, e inmediatamente y tan pronto como le sean solicitados por **PONOS**) en un soporte de almacenamiento digital a los efectos de que la información contenida en esta pueda ser empleada por **PONOS**.

## F) PROTECCION DE DATOS / CONFIDENCIALIDAD

## DECIMOCUARTA.- CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

### 14.1. Informativa de Datos Personales Contenidos en el Contrato

A los efectos de lo dispuesto en la normativa vigente sobre la protección de datos de carácter personal, serán objeto de tratamiento los datos personales de los firmantes, así como los relativos a las personas de contacto de cada entidad, tratados por cada una de las partes intervinientes, respectivamente, con el fin de mantener las relaciones entre ellas necesarias para la prestación de los servicios objeto de contratación y cumplir con todos los aspectos que de ello se deriven (formalización y archivo de los contratos, gestión de la contabilidad, cumplimiento de obligaciones impositivas y de facturación).

La base legal para el tratamiento de los datos es el interés legítimo de cada entidad como Responsable del tratamiento. Estos datos no se cederán a terceros ni serán objeto de transferencias internacionales salvo que contemos con su consentimiento o se precise el cumplimiento de obligaciones legales. Los datos se conservarán mientras se mantenga la relación contractual entre las partes y en todo caso, durante el plazo necesario para atender las obligaciones y responsabilidades legales que pudieran derivarse de la prestación del servicio y del tratamiento de los datos realizados.

Los datos de los firmantes y las personas de contacto de cada entidad serán tratados exclusivamente para los fines expuestos y no serán tratados ulteriormente de manera incompatible con dichos fines.

Mientras no nos comunique lo contrario, se entenderá que los datos de los firmantes y las personas de contacto de cada entidad no han sido modificados y que usted se compromete a notificarnos cualquier variación sobre los mismos.

Se informa que PONOS IBERICA, S.L. ha designado a un Delegado de Protección de Datos, con quien podrá contactar a través de la siguiente dirección de correo electrónico: protecciondedatos@pidf.eu

En el caso de que el proveedor tenga designado un Delegado De Protección De Datos (DPO) o un Coordinador de Protección de Datos es necesario que se cumplimenten los siguientes campos. En caso negativo cumplimentar indicando NO en cada recuadro.

| | NOMBRE Y APELLIDOS | E MAIL |
|---|---|---|
| Delegado de protección de datos (DPO) | Ìsrael Díaz Domínguez | idiaz@coitt.es |
| Coordinador de protección de datos | | |

Asimismo, se informa sobre la posibilidad de ejercitar en cualquier momento el derecho a obtener confirmación sobre si se están tratando o no sus datos personales, así como a ejercer los derechos de acceso, rectificación, limitación de tratamiento, supresión, portabilidad y oposición, dirigiendo su solicitud por escrito a la atención del Delegado de Protección de datos de PONOS Asistencia, junto con una fotocopia de su DNI, al domicilio establecido en el presente contrato, o bien enviando un correo electrónico, adjuntando fotocopia de su DNI a dgonzalo@pidf.es

Las partes intervinientes tienen derecho a presentar una reclamación ante la Agencia Española de Protección de Datos (AEPD).

### 14.2. Respecto del Tratamiento de Datos de los interesados

En cumplimiento de la normativa a de Protección de Datos de Carácter Personal se adjunta el **ANEXO I** como parte inseparable del presente contrato. En virtud del cual:

- **PONOS** actúa como ENCARGADO DEL TRATAMIENTO de los datos de carácter personal de los asegurados de sus compañías clientes y como RESPONSABLE DEL TRATAMIENTO de los datos de carácter personal de sus empleados, clientes y proveedores.
- Las compañías clientes de **PONOS** actúan como RESPONSABLE DEL TRATAMIENTO de los datos de carácter personal de sus asegurados.
- **El PROVEEDOR** actúa como SUBENCARGADO DEL TRATAMIENTO de los datos de los asegurados de las compañías clientes de **PONOS** y como ENCARGADO DEL TRATAMIENTO de los datos de carácter personal de los empleados, clientes y proveedores de **PONOS**.

### 14.3. Confidencialidad

**SEC&TECH4ALL** remitirá una relación del personal a su cargo que tendrá acceso a la información para la prestación contratada, manteniendo actualizado dicho listado, el cual, se remitirá a **PONOS** cada vez que se produzca un cambio y/o modificación.

Para el cumplimiento de lo dispuesto en el párrafo anterior, **SEC&TECH4ALL** se ocupará y responsabilizará de recabar el oportuno consentimiento de los titulares de los datos respecto de los cuales dará acceso de los mismos a **PONOS** con el objeto y finalidades antedichas.

**LAS PARTES** no podrán revelar a ningún tercero sin la autorización previa y por escrito de la/s otra/s parte/s ninguna información confidencial. A los efectos del presente acuerdo, tendrá la consideración de información confidencial toda aquella susceptible de ser revelada de palabra, por escrito o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que se invente en el futuro, intercambiada como consecuencia de este contrato.

El término “Información Confidencial” incluye, sin limitación, los secretos empresariales, programas de ordenador, software, documentación, fórmulas, datos, inventos, técnicas, planes de marketing, estrategias, planificaciones, información sobre empleados, información financiera, precio – tarifas –baremos, información técnica, información comercial, información legal así como información confidencial relativa a la actividad empresarial de las partes en lo relativo al modo en que ha sido, o será, gestionada en el futuro; información confidencial del Propietario relativa al pasado, presente o posible futuro de los productos, métodos de fabricación u operativos, incluida la información sobre investigación, desarrollo, ingeniería, compras, fabricación, contabilidad, marketing, ventas o leasing, e incluyendo cualquier software, incluido el de terceros.

El personal al servicio de **SEC&TECH4ALL** y cualquier otra persona o colaborador [consultores o asesores] que intervenga en la prestación de servicios objeto de este contrato y que dependa de este, está obligada a guardar la más estricta confidencialidad sobre toda Información Confidencial.

En consideración especial al carácter reservado de la Información Confidencial que se pueda comunicar con ocasión del presente contrato, **LAS PARTES** restringirá el acceso a tal información al número mínimo e indispensable de sus empleados o dependientes, para acometer los servicios objeto del presente contrato.

Asimismo, **LAS PARTES** deberá limitar el uso de la información confidencial recibida al personal estrictamente necesario para el cumplimiento del objeto de este contrato, asumiendo la responsabilidad por todo uso distinto al mismo, realizado por ella o por las personas físicas o jurídicas a las que haya permitido el acceso a la Información Confidencial.

## G) NOTIFICACIONES Y SOLUCION DE CONFLICTOS

### DECIMOQUINTA.- COMUNICACIONES ENTRE LAS PARTES

Todas las notificaciones que hayan de realizarse en virtud de lo establecido en el presente contrato deberán ejecutarse de forma fehaciente, mediante cualquier medio de comunicación que deje constancia del contenido y la recepción, en los domicilios fijados en el encabezamiento del contrato.

En el supuesto de que, durante la vigencia del presente contrato, alguna de las partes cambiara el domicilio de notificaciones, se lo deberá comunicar a la otra de modo fehaciente con carácter previo.

Para cuestiones operativas y relacionadas con la prestación de los servicios contratados se señalan las siguientes personas de contacto:

**PONOS:** Ángel Luis Mendez (almendez@pidf.es)

**EL PROVEEDOR:** Israel Díaz Domínguez (idiaz@coitt.es)

### DECIMOSEXTA.- INTEGRACIÓN Y NATURALEZA CONTRACTUAL

- La relación entre **LAS PARTES** en virtud del presente contrato tiene carácter exclusivamente mercantil, siendo **SEC&TECH4ALL** una empresa independiente de **PONOS**, que selecciona al personal y profesionales a su cargo con libertad de criterio, fijando y satisfaciendo sus retribuciones y honorarios, a la vez que establece su organización y ejercita las facultades disciplinarias, sin que exista ningún tipo de relación laboral entre el personal de **SEC&TECH4ALL** y **PONOS**, actuando dicho personal, siempre y en todo caso bajo las instrucciones y dependencia de **SEC&TECH4ALL**.
- Asimismo, **LAS PARTES** mantienen su plena independencia mercantil, sin que suponga la celebración del presente contrato vínculo societario alguno entre las mismas.
- Para todo lo no previsto en el presente Contrato, las partes se regirán por el Derecho español y, en concreto, serán de aplicación las disposiciones del Código de Comercio, leyes especiales, usos mercantiles y demás disposiciones de derecho común.

**En su virtud,**

El presente contrato y sus anexos sustituyen a cualquier otro contrato escrito o acuerdo verbal que sobre el mismo objeto pudiera existir entre **LAS PARTES**, quedando los mismos sin efecto a partir de la fecha de entrada en vigor del presente contrato. Asimismo, cualesquiera nuevos documentos que integren la relación contractual descrita en el presente documento tales como sus anexos serán de aplicación complementaria prevaleciendo lo dispuesto en este, a salvo de que se expresamente se disponga lo contrario pese a que resulte de fecha posterior.

### DECIMOSÉPTIMA.- FUERO Y JURISDICCIÓN

En relación con cualquier duda o conflicto que surja con motivo de la interpretación y/ o cumplimiento del presente contrato, **LAS PARTES** acuerdan someterse a la jurisdicción de los Juzgados y Tribunales de la ciudad de Madrid, con renuncia al fuero que pudiera corresponderle para el caso de que no resultara imperativo.

## DECIMOCTAVA.- RELACIÓN DOCUMENTAL: DETALLE DE DOCUMENTACIÓN REQUERIDA

### 18.1. Relación de Documentos Anexos

| | |
|---|---|
| **ANEXO I** | Anexo de protección de datos de carácter personal |
| **ANEXO II** | Medidas de seguridad de la información |

### 18.2. Detalle de Documentación Requerida a PROVEEDOR

| DOCUMENTACIÓN SOLICITADA | PLAZO DE ENTREGA |
|---|---|
| **Certificado** emitido por la **A. Tributaria** de estar al corriente de pagos de obligaciones Tributarias | 15 días desde firma contrato |
| **Certificado** emitido por la **T. G. S. Social** de estar al corriente de pagos de obligaciones Tributarias | 15 días desde firma contrato |
| **Póliza** Vigente de **Seguro de Responsabilidad Civil incluida la cobertura de responsabilidad patronal** | Al tiempo de la firma |

Y en prueba de conformidad, firman **LAS PARTES**, a un único efecto, el presente contrato, el cual consta de (19) caras de folio además de sus **Anexos**, dejando sin efecto cualesquiera contratos verbales y/o escritos anteriores que versaran sobre el mismo objeto.

**PONOS IBÉRICA, SL.**

Firmado por GARCIA OROIS JOSE MARIA - ***6115** el día 02/01/2024 con un certificado emitido por AC FNMT Usuarios

**Fdo.: José María García Orois**

**SEC&TECH4ALL 2023, SL**

Firmado por DIAZ DOMINGUEZ ISRAEL - ***2639**, el día 03/01/2024 con un certificado emitido por AC FNMT Usuarios Correo electrónico: idiaz@coitt.es

**Fdo.: Israel Díaz Domínguez**

## ANEXO I – CONTRATO DE ACCESO A DATOS POR CUENTA DE TERCEROS

### MANIFIESTAN

1. Que **PONOS** se encuentra vinculada por una relación contractual de carácter mercantil con diversos clientes.
2. Que para la prestación del servicio descrito en el contrato al que se adiciona el presente Anexo es necesario que **SEC&TECH4ALL** tenga acceso y trate datos de carácter personal de los que los clientes de **PONOS** son Responsables del Tratamiento, así como datos de carácter personal de los que **PONOS** es el Responsable del Tratamiento.
   a. Será de aplicación el presente anexo a la totalidad de servicios contratados y mientras estos se encuentren vigentes.
3. Que **LAS PARTES** reconocen cumplir con todas las obligaciones derivadas del RGPD, de la normativa nacional vigente sobre protección de datos de carácter personal y de cualquier otra norma que resulte de aplicación, en especial, las relativas al derecho de información, consentimiento y al deber de secreto.
4. Todo ello y a fin de cumplir con lo dispuesto en el RGPD y la LOPDGDD, el **Responsable del Tratamiento** autoriza a **PONOS** para que **SEC&TECH4ALL**, como **Subencargado del tratamiento**, acceda y trate datos personales de su responsabilidad y que son necesarios para el cumplimiento del servicio contratado. Asimismo, **PONOS** autoriza a **SEC&TECH4ALL** para que, como **Encargado del tratamiento**, acceda y trate datos personales de su responsabilidad y que son necesarios para el cumplimiento del servicio contratado

En su virtud, **LAS PARTES** de forma libre y voluntaria acuerdan regular este acceso y tratamiento de datos de carácter personal en el presente Anexo y sobre la base de las siguientes:

### CLÁUSULAS

### PRIMERA. – DEFINICIONES

**RGPD:** Reglamento (UE) 2016/679 del Parlamento Europeo y Del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)

**LOPDGDD**: Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y por la que se deroga la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

**Responsable de Tratamiento:** persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros: A efectos del presente anexo tienen tal consideración **LOS CLIENTES DE PONOS** así como **PONOS**.

**Encargado de tratamiento:** persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento: a efectos del presente contrato lo es **PONOS** o **SEC&TECH4ALL**, en función de los datos objeto del tratamiento y de quien sea considerado Responsable del Tratamiento respecto de cada uno de ellos.

**Subencargado del Tratamiento**: persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento, pero por encargo del encargado del tratamiento. A efectos del presente contrato lo es **SEC&TECH4ALL**.

**Datos personales**: toda información sobre una persona física identificada o identificable ("el interesado"); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

**Fichero:** todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica

**Violación de la seguridad de los datos personales:** toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

## SEGUNDA.- OBJETO DEL ENCARGO DEL TRATAMIENTO

Mediante las presentes cláusulas se habilita al **Encargado del Tratamiento / Subencargado de Tratamiento** para tratar por cuenta del **Responsable del Tratamiento**, los datos de carácter personal necesarios para prestar el servicio que forma parte del objeto del contrato al que se adiciona el presente anexo.

A estos efectos, el tratamiento que realizará el **Encargado del Tratamiento / Subencargado de Tratamiento** consistirá en: estructuración, supresión, registro, extracción, comunicación por transmisión, interconexión, limitación y destrucción.

## TERCERA.- IDENTIFICACIÓN DE LA INFORMACIÓN AFECTADA

**3.1.** Para la ejecución de las prestaciones derivadas del cumplimiento del Contrato, **PONOS** pone a disposición de **SEC&TECH4ALL** la información que se describe a continuación:

- Datos personales de los asegurados de las compañías clientes de **PONOS** disponibles en los sistemas de **PONOS**.
- Datos personales de los empleados de **PONOS** disponibles en los sistemas de **PONOS**.
- Datos personales de los proveedores de **PONOS** disponibles en los sistemas de **PONOS**.
- Datos personales de los clientes de **PONOS** disponibles en los sistemas de **PONOS**.

## CUARTA.- OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO

a. **PONOS** deberá dará acceso al **Encargado del Tratamiento / Subencargado de Tratamiento** a los datos a los que se refiere la CLÁUSULA TERCERA de este Anexo.
b. El **Responsable de Tratamiento** debe realizar un análisis de riesgos para determinar las medidas técnicas y organizativas apropiadas que garanticen la seguridad de la información tratada por el **Encargado del Tratamiento / Subencargado del Tratamiento** y los derechos de las personas afectadas.
c. El **Responsable de Tratamiento** debe realizar, cuando proceda, una evaluación del impacto de las operaciones de tratamiento a realizar por el **Encargado del Tratamiento / Subencargado del Tratamiento** y realizar las consultas previas que correspondan.
d. A la vista del análisis de riesgos y en su caso, de la evaluación de impacto que corresponda, el **Responsable del Tratamiento** debe, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, aplicar medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento objeto del presente Anexo es conforme con el RGPD y con la LOPDGDD.
e. El **Responsable del Tratamiento**, garantizará que dichas medidas se revisarán y actualizarán cuando sea necesario.
f. El **Responsable del Tratamiento** deberá informar al **Encargado del Tratamiento**, de las medidas técnicas y organizativas que se deberán adoptar con respecto a los datos objeto de tratamiento y comunicar que estas son apropiadas y suficientes para para garantizar el nivel de seguridad adecuado al riesgo existente y para proteger los derechos de los interesados.

El **Encargado de tratamiento** deberá informar al **Subencargado del Tratamiento**, antes de que éste acceda y realice el tratamiento, de las medidas técnicas y organizativas comunicadas por el Responsable del Tratamiento, que deberá adoptar con respecto a los datos objeto de tratamiento.

g. El **Responsable de Tratamiento** es responsable de que el tratamiento sea lícito, leal y transparente respecto del interesado.
h. El **Responsable de Tratamiento** debe velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD y de la LOPDGDD por parte del **Encargado del Tratamiento**.
i. El **Encargado de Tratamiento** debe velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD y de la LOPDGDD por parte del **Subencargado del Tratamiento**.
j. El **Responsable de Tratamiento** debe supervisar el tratamiento realizado por el **Encargado de Tratamiento**, incluida la realización de inspecciones y auditorías.
k. El **Encargado de Tratamiento** debe supervisar el tratamiento realizado por el **Subencargado del Tratamiento**, incluida la realización de inspecciones y auditorías
l. El **Responsable del Tratamiento** adoptará las políticas necesarias en materia de protección de datos
m. El **Responsable del Tratamiento** designará a un Delegado de Protección de Datos siempre que:
    a) El tratamiento lo lleve a cabo una autoridad o un organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;
    b) Las actividades principales del **Responsable del Tratamiento** consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala;
    c) Las actividades principales del **Responsable del Tratamiento** consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.
n. En su caso, el **Responsable del Tratamiento** comunicará al **Encargado del Tratamiento** los datos de contacto del Delegado de Protección de Datos y garantizará que éste participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.
o. El **Responsable del Tratamiento** debe adherirse al Código de Conducta que pueda aprobarse por parte de la Comisión u organismo correspondiente.
p. El **Responsable del Tratamiento** debe llevar un registro de actividades de tratamiento en caso de tratar datos personales que supongan un riesgo para los derechos y libertades del interesado y/o de manera no ocasional, o que implique el tratamiento de categorías especiales de datos y/o datos relativos a condenas e infracciones.
q. El **Responsable del Tratamiento** debe poner a disposición de los interesados los aspectos esenciales del presente acuerdo
r. El **Responsable del Tratamiento** debe cumplir con el deber de información a los interesados y atender los ejercicios de derechos establecidos en la normativa vigente en Protección de Datos de Carácter Personal].
s. Conforme a los requerimientos del artículo 33.- "Notificación de una violación de la seguridad de los datos personales a la autoridad de control" del RGPD y del artículo 34.- "Comunicación de una violación de la seguridad de los datos personales al interesado" del RGPD, el **Responsable del Tratamiento** debe notificar en tiempo y forma a la Autoridad de Control, y en su caso, a los interesados, las violaciones de seguridad que se produzcan sobre los datos objeto de tratamiento por parte del **Encargado del Tratamiento / Subencargado del Tratamiento**.
t. En caso de que los Inspectores de la Agencia Española de Protección de Datos se personaran en las instalaciones de **SEC&TECH4ALL** al objeto de ejercer la potestad inspectora que la LOPDGDD atribuye a la Agencia Española de Protección de Datos, este se compromete a comunicar inmediatamente y en el menor tiempo posible tal circunstancia a **PONOS** para que a su vez informe al **Responsable del Tratamiento**, en caso de que no lo fuese **PONOS**, al objeto de que, durante el ejercicio de las funciones inspectoras por los Inspectores de la Agencia Española de Protección de Datos, pueda personarse en las instalaciones de **SEC&TECH4ALL** si así lo considerase necesario.

## QUINTA. – INSTRUCCIONES

a. Mediante la presente cláusula, el **Responsable del Tratamiento / Encargado del Tratamiento** proporciona al **Encargado del Tratamiento / Subencargado del Tratamiento** las instrucciones necesarias para acceder y tratar los datos de carácter personal objeto de tratamiento.
b. El **Encargado del Tratamiento / Subencargado del Tratamiento** y sus empleados trataran los datos de acuerdo con las instrucciones contenidas en el presente Anexo.
c. Si el **Encargado del Tratamiento / Subencargado del Tratamiento** considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, informará inmediatamente al **Responsable del Tratamiento / Encargado del Tratamiento**.
d. El **Encargado del Tratamiento / Subencargado del Tratamiento** utilizará los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto de este encargo y en ningún caso podrá utilizarlos para fines propios.

## SEXTA.- CONFIDENCIALIDAD

a. El **Encargado del Tratamiento / Subencargado del Tratamiento** está obligado a guardar bajo su control y custodia los datos personales a los que acceda con motivo de la prestación del servicio y a no divulgarlos, transferirlos o de cualquier otra forma comunicarlos, ya sea verbalmente o por escrito, por medios electrónicos, papel o mediante acceso informático, ni siquiera para su conservación, a otras personas salvo que se trate de un proveedor del servicio cuya contratación haya sido comunicada previamente al **Responsable del Tratamiento / Encargado del Tratamiento** y autorizada por el **Responsable del Tratamiento / Encargado del Tratamiento**. En tal caso, deberá formalizar el correspondiente contrato de Tratamiento de datos, en los mismos términos que se recogen en el presente contrato, respondiendo solidariamente junto con dicho proveedor de servicios contratado de los daños y perjuicios que se puedan ocasionar al Responsable del Tratamiento por incumplimiento de esta obligación
b. El **Encargado del Tratamiento / Subencargado del Tratamiento** y sus empleados deben guardar la confidencialidad y secreto sobre los datos de carácter personal a los que acceda y trate con motivo de su prestación profesional, estando sujetos, en consecuencia, al más estricto secreto profesional. Este compromiso es de carácter indefinido y se mantendrá, incluso una vez finalizada la relación existente.
c. El **Encargado del Tratamiento / Subencargado del Tratamiento** debe asegurar que los datos personales objeto de tratamiento son accedidos y manejados únicamente por aquellos empleados cuya intervención sea precisa para la finalidad prevista en el presente Anexo, o por aquellos terceros autorizados expresamente por el **Responsable del Tratamiento**, cuya intervención sea igualmente precisa. En ambos casos, se comprometerán de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que el **Encargado del Tratamiento / Subencargado del Tratamiento** debe informarles convenientemente. Este compromiso será firmado por el **Encargado del Tratamiento / Subencargado del Tratamiento** siendo el responsable de, custodiar, controlar y poner a disposición del **Responsable del Tratamiento / Encargado del Tratamiento** cuando así lo requiera, dichos compromisos de confidencialidad.

## SÉPTIMA.- OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO / SUBENCARGADO DEL TRATAMIENTO

a. El **Encargado del Tratamiento / Subencargado del Tratamiento** está obligado a implantar como mínimo las medidas de seguridad que se describen a continuación:

**DEBER DE CONFIDENCIALIDAD Y SECRETO**

- Se deberá evitar el acceso de personas no autorizadas a los datos personales, a tal fin se evitará dejar los datos personales expuestos a terceros. Cuando cualquier persona se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.
- Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las veinticuatro horas del día.
- No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.
- No se comunicarán datos personales o cualquier información personal a terceros.
- El deber de secreto y confidencialidad persistirá incluso cuando finalice la relación laboral del trabajador con la empresa.

**MEDIDAS TÉCNICAS**

- **IDENTIFICACIÓN**
    - Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal, se debe disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.
    - Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
    - Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres y mezcla de números y letras.
    - Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).
    - Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.
- **DEBER DE SALVAGUARDA**

  A continuación, se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:
    - ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.
    - MALWARE: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
    - CORTAFUEGOS O FIREWALL: Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.
    - CIFRADO DE DATOS: Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
    - COPIA DE SEGURIDAD: Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información

  El **Encargado del Tratamiento / Subencargado del Tratamiento** está obligado a poner a disposición del **Responsable del Tratamiento / Encargado del Tratamiento** toda la información necesaria para demostrar el cumplimiento de sus obligaciones, tal y como exige por la normativa aplicable sobre Protección de Datos de carácter personal.

  El **Encargado del Tratamiento / Subencargado del Tratamiento** proporcionará al **Responsable del Tratamiento / Encargado del Tratamiento** el informe de auditoría anual basado en [ISO 27001 o ISAE3402 o SSAE16-SOC 1 Tipo 2 o ISAE3000 o SSAE16-SOC 2 Tipo 2 o similar] o informes de auditoría similares creados por un tercero ("Informe de Auditoría") tan pronto disponga de ellos.

  Si el **Responsable del Tratamiento / Encargado del Tratamiento** considera que dicho Informe de Auditoría es insuficiente para demostrar el cumplimiento del **Encargado del Tratamiento / Subencargado del Tratamiento** o si el Informe de Auditoría identifica alguna insuficiencia, se podrá solicitar la realización de inspecciones por el **Responsable del Tratamiento / Encargado del**

**Tratamiento** o por otro auditor designado por el **Responsable del Tratamiento / Encargado del Tratamiento** ("Auditoría in situ").

Dicha Auditoría in situ está sujeta a la las siguientes condiciones: (i) La Auditoría in situ se limitará a las instalaciones donde se realice el tratamiento y al personal del **Encargado del Tratamiento / Subencargado del Tratamiento** involucrado en las actividades de tratamiento cubiertas por este Anexo; (ii) la Auditoría in situ sólo se realizarán una vez al año o cuando así lo requiera la normativa sobre Protección de Datos de Carácter Personal aplicable o una Autoridad de Control competente o inmediatamente después de haberse detectado una violación de seguridad que afecte a los datos personales tratados por el **Encargado del Tratamiento / Subencargado del Tratamiento** conforme al presente Anexo; (iii) puede realizarse durante horario laboral, sin interrumpir considerablemente las operaciones comerciales del **Encargado del Tratamiento / Subencargado del Tratamiento**, de acuerdo con la Política de Seguridad del **Encargado del Tratamiento / Subencargado del Tratamiento** y después de un aviso previo razonable por parte del **Responsable del Tratamiento / Encargado del Tratamiento**; (iv) el **Responsable del Tratamiento / Encargado del Tratamiento** sufragará los gastos que surjan de la Auditoría in situ o que tengan conexión con la misma, salvo que tras realizar dicha Auditoría in situ se identifique que el **Encargado del Tratamiento / Subencargado del Tratamiento** no cumple con sus obligaciones sobre seguridad de la información, conforme a lo establecido en la normativa aplicable sobre Protección de Datos de Carácter Personal y en el presente Anexo, en cuyo caso, el **Encargado del Tratamiento / Subencargado del Tratamiento** sufragará los gastos ocasionados por la realización de la Auditoría in situ; (v) el **Responsable del Tratamiento / Encargado del Tratamiento** creará un informe de auditoría donde se reflejen los hallazgos y observaciones de la Auditoría in situ que se realice ("Informe de Auditoría in situ"). Los informes de Auditoría in Situ y los que inicialmente proporcione el **Encargado del Tratamiento / Subencargado del Tratamiento** para demostrar el cumplimiento de sus obligaciones son información confidencial y no se divulgarán a terceros, a excepción de los asesores legales y consultores del **Responsable del Tratamiento / Encargado del Tratamiento** y **Encargado del Tratamiento / Subencargado del Tratamiento**, del Delegado de Protección de Datos que, en su caso, se designe por el **Encargado del Tratamiento / Subencargado del Tratamiento**, y/o el **Encargado del Tratamiento / Subencargado del Tratamiento** o a petición de una Autoridad de Control competente o cuando el **Responsable del Tratamiento / Encargado del Tratamiento** y el **Encargado del Tratamiento / Subencargado del Tratamiento** presten su consentimiento para revelarlos.

b. Cuando el **Encargado del Tratamiento / Subencargado del Tratamiento** emplee a más de 250 personas y/o el tratamiento objeto del presente Anexo suponga un riesgo para los derechos y las libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9.1 del RGPD, o datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10 del RGPD, estará obligado a llevar, por escrito, inclusive en formato electrónico, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del **Encargado del Tratamiento / Responsable del Tratamiento**, que contenga toda la información requerida por el artículo 30.2.- Registro de las actividades de tratamiento del RGPD.
c. El **Encargado del Tratamiento / Subencargado del Tratamiento** está obligado a garantizar que los empleados que van a acceder y tratar los datos de carácter personal objeto del tratamiento disponen de la formación necesaria en materia de protección de datos personales.
d. El **Encargado del Tratamiento / Subencargado del Tratamiento**, mediante la aportación de la documentación necesaria y disponible al **Responsable del Tratamiento / Encargado del Tratamiento**, dará apoyo al **Responsable del Tratamiento / Encargado del Tratamiento** en la realización de las Evaluaciones de Impacto relativas a la protección de datos y en la realización de las consultas previas a la Autoridad de control, cuando procedan.
e. El **Encargado del Tratamiento / Subencargado del Tratamiento** designará a un Delegado de Protección de Datos y comunicará su identidad y datos de contacto al **Responsable del Tratamiento / Encargado del Tratamiento** cuando:
    a. El tratamiento lo lleve a cabo una autoridad o un organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b. Las actividades principales del **Encargado del Tratamiento / Subencargado del Tratamiento** consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala;
c. Las actividades principales del **Encargado del Tratamiento / Subencargado del Tratamiento** consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.

f. El **Encargado del Tratamiento / Subencargado del Tratamiento** puede comunicar los datos objeto de tratamiento a otros **Encargados del Tratamiento / Subencargados del Tratamiento** del mismo **Responsable del Tratamiento / Encargado del Tratamiento**, de acuerdo con las instrucciones del **Responsable del Tratamiento / Encargado del Tratamiento**. En este caso, el **Responsable del Tratamiento / Encargado del Tratamiento** informará al **Encargado del Tratamiento / Subencargado de Tratamiento** inicial de forma previa y por escrito, de la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.
g. Si el **Encargado del Tratamiento / Subencargado del Tratamiento** tiene que transferir datos personales objeto de tratamiento a un tercer país o a una organización internacional, en virtud del Derecho de la Unión o de los Estados miembros que le sean aplicables, informará al **Responsable del Tratamiento / Encargado del Tratamiento** de esa exigencia legal de manera previa, salvo que tal Derecho lo prohíba por razones importantes de interés público.

## OCTAVA.- DERECHOS DE LOS INTERESADOS

El **Encargado del Tratamiento / Subencargado del Tratamiento** asistirá al **Responsable del Tratamiento / Encargado del Tratamiento**, en la medida de lo posible y especialmente a través de medidas técnicas y organizativas apropiadas, en la respuesta al ejercicio de los derechos de:

1. Acceso, rectificación, supresión y oposición
2. Limitación del tratamiento
3. Portabilidad de datos
4. A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

Corresponde al **Responsable del Tratamiento** facilitar el derecho de información en el momento de la recogida de los datos. No obstante, cuando las personas afectadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el **Encargado del Tratamiento / Subencargado del Tratamiento**, éste debe comunicarlo al **Responsable del Tratamiento / Encargado del Tratamiento**, por correo electrónico a la dirección protecciondedatos@PONOS.es La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, junto con, en su caso, otras informaciones que puedan ser relevantes para resolver la solicitud.

## NOVENA.- VIOLACIONES DE SEGURIDAD

El **Encargado del Tratamiento / Subencargado del Tratamiento** notificará al **Responsable del Tratamiento / Encargado del Tratamiento**, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24h después de que haya tenido constancia de ella, y a través de protecciondedatos@PONOS.es las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, junto con toda la información relevante para la documentación y comunicación de la incidencia. No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

a. Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
b. En su caso, el nombre y los datos de contacto del Delegado de Protección de Datos o de otro punto de contacto en el que pueda obtenerse más información.
c. Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
d. Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles

efectos negativos. Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

## DÉCIMA.- SUBCONTRATACIÓN

Para subcontratar con otras empresas, el **Encargado del Tratamiento / Subencargado del Tratamiento** debe comunicarlo por escrito al **Responsable del Tratamiento / Encargado del Tratamiento**, identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto.

En su caso, el **Encargado del Tratamiento** comunicará este hecho por escrito al **Responsable del Tratamiento**, indicando los tratamientos que el **Subencargado del Tratamiento** pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto.

La subcontratación podrá llevarse a cabo si el **Responsable del Tratamiento** no manifiesta su oposición en el plazo de [10 días].

En todo caso, el **Encargado del Tratamiento / Subencargado del Tratamiento** designará únicamente a proveedores diligentes, con especial atención a su buena reputación y experiencia en la prestación de los servicios subcontratados y la idoneidad de sus medidas técnicas y organizativas.

El subcontratista, que también tendrá la condición de **Encargado del Tratamiento / Subencargado del Tratamiento**, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el Subencargado inicial y las instrucciones que dicte el Responsable del Tratamiento.

Corresponde al **Encargado del Tratamiento / Subencargado del Tratamiento inicial** regular la nueva relación con el **Subencargado del Tratamiento**, suscribiendo un contrato por escrito, en nombre y por cuenta del **Responsable del Tratamiento**, de forma que éste quede sujeto a las mismas condiciones, instrucciones, obligaciones, medidas de seguridad y requisitos formales establecidas en el presente Anexo, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas.

En el caso de incumplimiento por parte del **Subencargado del Tratamiento**, **EL PROVEEDOR** (**Encargado del Tratamiento / Subencargado del Tratamiento inicial**) seguirá siendo plenamente responsable ante el **Responsable del Tratamiento / Encargado del Tratamiento** en lo referente al cumplimiento de las obligaciones.

El **Encargado del Tratamiento / Subencargado del Tratamiento** podrá, durante el término del contrato, sin costes para el **Responsable del Tratamiento / Encargado del Tratamiento**, supervisar, auditar regularmente y tomar las medidas necesarias para que los proveedores subcontratados cumplan con sus obligaciones, informando inmediatamente al **Responsable del Tratamiento / Encargado del Tratamiento** de cualquier incumplimiento detectado o reportado por el proveedor subcontratado, así como de todas las medidas tomadas para solventar cualquier incumplimiento.

## UNDECIMA.- DESTINO DE LOS DATOS

Una vez cumplida la prestación de los servicios contratados, el **Encargado del Tratamiento / Subencargado del Tratamiento**, a elección del **Responsable del Tratamiento / Encargado del Tratamiento**, está obligado a destruir o devolver al **Responsable del Tratamiento / Encargado del Tratamiento** los datos de carácter personal tratados y, si procede, los soportes donde éstos consten. En defecto de la decisión expresa del **Responsable del Tratamiento / Encargado del Tratamiento,** el **Encargado del Tratamiento / Subencargado del Tratamiento** mantendrá debidamente bloqueados los datos.

En caso de que el Responsable del Tratamiento opte por la devolución, el **Encargado del Tratamiento / Subencargado del Tratamiento** debe proceder al borrado total de los datos existentes en los equipos informáticos que ha utilizado para tratar dichos datos de carácter personal.

En caso de que el **Responsable del Tratamiento / Encargado del Tratamiento** opte por la destrucción, una vez destruidos, el **Encargado del Tratamiento / Subencargado del Tratamiento** debe certificar la destrucción por escrito y debe entregar el certificado al **Responsable del Tratamiento / Encargado del Tratamiento.**

No obstante, no se procederá a la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.

El **Encargado del Tratamiento / Subencargado del Tratamiento** conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el **Responsable del Tratamiento / Encargado del Tratamiento.**

## DUODECIMA.- RESPONSABILIDADES: INCUMPLIMIENTO DE ESTIPULACIONES

Como responsable de la ejecución, el **Encargado del Tratamiento / Subencargado del tratamiento** asume toda responsabilidad civil, sin limitación económica alguna, por todos los daños y perjuicios que se ocasionen a **PONOS** y asegurados de las entidades aseguradoras y/o clientes clientes de **PONOS** que tengan su causa en la ejecución de la prestación y todo ello sin posibilidad de repercutir en **PONOS** responsabilidad de cualquier clase.

Si por incumplimiento del **Encargado del Tratamiento / Subencargado del tratamiento** de las obligaciones consignadas en el presente anexo, alcanzara alguna responsabilidad a **PONOS**, del tipo que fuera, queda obligado el **Encargado del Tratamiento / Subencargado del tratamiento** a resarcir el importe de estas responsabilidades, incluidos gastos judiciales y extrajudiciales y costes que la defensa de **PONOS** ocasionara.

El **Encargado del Tratamiento / Subencargado del tratamiento** no podrá repercutir a **PONOS** multa, sanción o cualquier tipo de responsabilidad que por incumplimiento de alguna de las obligaciones referidas en presente Anexo le impongan las Autoridades competentes y, si fuera el caso, se acuerda expresamente que **Encargado del Tratamiento / Subencargado del tratamiento** indemnizará a **PONOS** de toda cantidad que se viese obligado a pagar por incumplimiento de **Encargado del Tratamiento / Subencargado del tratamiento** de las obligaciones aquí señaladas, aunque ello le venga impuesto a **PONOS** por resolución judicial y/o administrativa.

Respecto de los datos que el **Encargado del Tratamiento / Subencargado del tratamiento** recabe directamente para la finalidad contratada, tan sólo podrá hacer uso de los mismos exclusivamente para ceñirse a lo establecido en el contrato al que se adiciona el presente Anexo. Es por lo anterior, por lo que el **Encargado del Tratamiento / Subencargado del tratamiento** se obliga a cumplir con todas las obligaciones en materia de protección de datos de acuerdo con la normativa que resulte vigente en cada momento, así como la que la complemente o la desarrolle.

## DECIMOTERCERA.- DURACIÓN

El presente anexo se sujeta a los mismos términos de vigencia que los establecidos en el contrato al que se adiciona, ello sin perjuicio de las concretas previsiones y efectos aun finalizada la relación contractual.

## DECIMOCUARTA. - OTRAS DISPOSICIONES

- **a.** Tanto el **Responsable del Tratamiento**, como el **Encargado del Tratamiento** como el **Subencargado del Tratamiento** son responsables de cumplir con las obligaciones establecidas por el RGPD y por cualquier otra normativa sobre protección de datos de carácter personal aplicable.
- **b.** En caso de inconsistencias entre las disposiciones de este Anexo y cualquier otro acuerdo suscrito entre **LAS PARTES**, las disposiciones de este Anexo prevalecerán con respecto a las obligaciones de protección de datos.
- **c.** En caso de que alguna disposición de este Anexo sea nula o inaplicable, el resto de este Anexo seguirá siendo válido y vigente. La disposición nula o inaplicable deberá (i) modificarse según sea necesario para garantizar su validez y aplicabilidad, preservando al mismo tiempo las intenciones de **LAS PARTES** o, si esto no fuera posible, (ii) deberá interpretarse como si la disposición nula o inaplicable no estuviera incluida en el presente Anexo. Esto también se aplicará en caso de que este Anexo contenga alguna omisión.

**d.** Las Partes tienen derecho a solicitar cambios a este Anexo en la medida requerida para satisfacer cualquier interpretación, guía u orden emitida por autoridades competentes de la Unión Europea o de los Estados Miembros, disposiciones nacionales de aplicación u otros desarrollos normativos relacionados con los requisitos RGPD.

## ANEXO II - MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

| **RELACIÓN DEL PERSONAL QUE A CARGO DEL PROVEEDOR TENDRÁ ACCESO A LA INFORMACIÓN** | |
|---|---|
| **NOMBRE** | **APELLIDOS** |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

## ÍNDICE

## MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

El presente Anexo contiene las exigencias de Seguridad de los activos de Información de PONOS en relación a los servicios externalizados.

Los requerimientos de seguridad indicados en este Anexo, son de aplicacióna **SEC&TECH4ALL**, por cuanto utilizará los recursos de información y/o datos propiedad de PONOS en el marco del desarrollo de la prestación de servicios encomendada y con la finalidad previamente establecida.

**SEC&TECH4ALL** durante la prestación del servicio, estará obligado a cumplir y a aplicar la política de seguridad recogida en el Manual de Políticas de Seguridad de la información de PONOS, que es detallado en el presente anexo, así como a respetar las características fundamentales de seguridad de la información:

- Confidencialidad.
- Integridad.
- Disponibilidad.

Toda la información que facilite PONOS a **SEC&TECH4ALL** es propiedad de PONOS, y sólo podrá ser utilizada por **SEC&TECH4ALL** para el objeto del presente contrato y no podrá ser cedida a terceros, sin el previo consentimiento por escrito de PONOS.

**SEC&TECH4ALL** deberá adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de la información y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

PONOS podrá realizar por su cuenta y/o solicitar informes de auditorías en los sistemas de información e instalaciones de tratamiento de datos de **SEC&TECH4ALL** que verifiquen el cumplimiento de las políticas y medidas de seguridad exigidas en este contrato, con una periodicidad anual o con carácter extraordinario cuando se realicen modificaciones sustanciales en el sistema de información.

Si PONOS encontrase incumplimientos de seguridad que representen un riesgo alto para la prestación del servicio, según el análisis de riesgos realizado por éste, dependiendo de la gravedad de los mismos, podrá requerir a **SEC&TECH4ALL** la resolución inmediata de los problemas detectados mediante la elaboración de un plan de acciones correctivas a completar en un plazo no superior a 3 meses.

### ORGANIZACIÓN

**SEC&TECH4ALL** deberá contar con una figura de Responsable de Seguridad de la Información establecida formalmente, con el fin de velar por la integridad, seguridad, fiabilidad y disponibilidad de los sistemas, así como del cumplimiento de todas aquellas normativas que sean de aplicación.

**SEC&TECH4ALL** designará un Coordinador que será el encargado de la coordinación de los aspectos de seguridad con el PONOS.

Deberá existir un comité de coordinación mixto, entre **SEC&TECH4ALL** y PONOS, con la participación del Coordinador de Seguridad dSEC&TECH4ALL para desempeñar actividades de seguimiento oportuno y la definición de planes de acción necesarios para garantizar el correcto desempeño de los Servicios.

Será imprescindible el establecimiento de un equipo de Seguridad de la Información en PONOS, que se encargue de la gestión de la seguridad de la información en los sistemas y de la supervisión del correcto desempeño del Servicio en materia de riesgo tecnológico.

**PROCESOS**

2.1. PROCESOS DE TECNOLOGÍA

2.1.1. Infraestructura tecnológica

- El despliegue y mantenimiento de la infraestructura tecnológica del Servicio será responsabilidad dSEC&TECH4ALL excepto para los casos en los que el Servicio requiera infraestructura proporcionada por PONOS.
- SEC&TECH4ALL informará PONOS sobre la infraestructura tecnológica desplegada para darle servicio y permitir las tareas de supervisión/ monitorización establecidas por PONOS.

2.1.2. Ciclo productivo de sistemas - Desarrollo de Sistemas de SEC&TECH4ALL con acceso a datos:

Todos aquellos desarrollos que se realicen con el objeto de prestar servicios a PONOS, serán autorizados por PONOS, debiendo SEC&TECH4ALL:

- Abstenerse de almacenar datos del PONOS sin que el área de Seguridad de la Información de PONOS lo conozca, analice, indique la forma en que puedan ser almacenados, autorice y audite.
- Realizar una revisión de seguridad del código fuente para cualquier software que no haya sido desarrollado por el PONOS, de manera previa a su puesta en producción.
- En caso de que se realicen desarrollos de software para PONOS, SEC&TECH4ALL debe poner a disposición de PONOS todos aquellos desarrollos software hechos a medida, incluyendo código fuente, código objeto, manuales y cualquier otra información relevante.
- No utilizar datos de PONOS reales en las pruebas, en ocasión de que se lleven a cabo los desarrollos autorizados por el PONOS (etc.).
- Asegurar que los desarrollos realizados para la prestación de los Servicios al PONOS sean originales y las herramientas utilizadas no vulneran ninguna normativa, contrato, derecho, interés o propiedad de terceros.
- Establecer los controles de seguridad adecuados en relación con la adquisición de nuevas aplicaciones o sistemas durante la prestación del Servicio. Estos controles deben cubrir como mínimo análisis de viabilidad, autorizaciones, realización de pruebas, aprobaciones del usuario final y una separación adecuada de los entornos previos respecto del entorno de producción.

2.1.3 Explotación de la tecnología

- Gestión y reporting de Incidencias de seguridad:
    - SEC&TECH4ALL deberá disponer de un procedimiento de gestión y reporte de incidencias de seguridad, para lo cual, todas las incidencias deben ser gestionadas y transmitidas al PONOS, informando del modo de resolución.
    - SEC&TECH4ALL debe definir un canal de comunicación privado para comunicar situaciones inusuales, incidentes o de cualquier otra índole relacionada a la confidencialidad de la información del PONOS.
    - SEC&TECH4ALL debe informar inmediatamente al área de Seguridad de la Información de PONOS en el caso de que se detecte o se tenga una sospecha de un incidente de seguridad o incumplimiento de las medidas de seguridad exigidas en el presente contrato.

- Mantenimiento de sistemas (en caso de que SEC&TECH4ALL utilice sistemas propios para la prestación del Servicio a PONOS):
    - SEC&TECH4ALL podrá proponer proactivamente la instalación de actualizaciones y parches de seguridad. Dichas actualizaciones y parcheados serán comunicadas y autorizadas por PONOS. Adicionalmente, PONOS solicitará la instalación de actualizaciones y parches si lo considerara necesario.
    - En todo caso, el despliegue de parches deberá probarse en entornos previos, para evitar posibles impactos sobre el servicio.
    - Con independencia del software base que dé soporte a la plataforma y de sus versiones (sistemas operativos, base de datos, servidor web, etcétera) debe existir una política de vigilancia de alertas de seguridad y de actualización de los parches de seguridad publicados por los fabricantes correspondientes.
    - Los tiempos de actuación no deben superar las 24 horas en casos de fallos de seguridad clasificados por el fabricante de carácter grave/alto.
    - SEC&TECH4ALL debe establecer los controles de seguridad adecuados en relación con los cambios que pudieran ser necesario realizar sobre las aplicaciones, o sistemas involucrados en el Servicio. Estos controles deben cubrir como mínimo solicitudes de cambios, análisis de impacto, autorizaciones, realización de pruebas, aprobaciones del usuario final y una separación adecuada de los entornos previos respecto del entorno de producción.
    - La ejecución de cualquier cambio en los sistemas de información asociados al Servicio, debe ser aprobada previamente por PONOS y realizarse garantizando la integridad de la información y la disponibilidad del Servicio.

- Ubicación de datos (en caso de que SEC&TECH4ALL deba almacenar información relacionada con la prestación del Servicio a PONOS en sistemas propios dSEC&TECH4ALL):
    - SEC&TECH4ALL deberá informar a PONOS sobre la ubicación de los datos que serán almacenados antes de la contratación del Servicio. Durante el periodo de duración del Servicio, cualquier cambio en la ubicación de los datos, deberá ser comunicado a PONOS con anticipación y los cambios no podrán ser efectuados hasta recibir la autorización de PONOS.
    - SEC&TECH4ALL deberá implementar mecanismos de control de cambio en los ficheros almacenados en el Servicio, registrando toda la información necesaria que permita la trazabilidad de los eventos.

- Respaldo de la información (en caso de que SEC&TECH4ALL deba almacenar información relacionada con la prestación del Servicio a PONOS en sistemas propios dSEC&TECH4ALL):
    - SEC&TECH4ALL deberá establecer y aplicar una política de realización de copias de respaldo que incluya la seguridad sobre las copias y los procedimientos de prueba y recuperación. Tendrá controles implementados para asegurar la correcta manipulación y transporte de los medios de almacenamiento de las copias de seguridad, asignando responsables, controles de accesos físicos y lógicos, cadena de custodia e inventarios periódicos.
    - SEC&TECH4ALL dispondrá de un Plan de Subsanación de Contingencias, que le permita recuperar el Servicio de sistemas de información formalmente documentado y probado de forma periódica.

- Servicio Compartido (en caso de que SEC&TECH4ALL preste Servicio a otras empresas):
    - SEC&TECH4ALL deberá implementar las medidas suficientes para garantizar la seguridad de la infraestructura tecnológica en caso que se encuentre compartida con otros terceros. La infraestructura tecnológica del servicio deberá poseer canales de comunicación cifrados entre otros servicios que ofrezca SEC&TECH4ALL y las conexiones del personal responsable de la administración de la infraestructura. Por ejemplo; SSH, VPN con IPSEC, etc.
    - El almacenamiento de datos del Servicio prestado a PONOS deberá estar aislado físicamente o en su defecto, lógicamente de otros repositorios de almacenamiento ajenos. El Servicio dSEC&TECH4ALL deberá tener la capacidad de cifrar información almacenada, mediante algoritmos fuertes de cifrado.

- Salida de información:
    - SEC&TECH4ALL no deberá permitir la salida de soportes de información ni ficheros a terceros sin la autorización previa del PONOS.

2.1.4 Seguridad de la información

- PONOS será responsable de los siguientes procesos relativos a la seguridad de la información:
    - Gestión y administración de usuarios en los sistemas de información, así como de sus permisos.
    - Monitorización de seguridad de los sistemas. El prestador del Servicio pondrá a disposición de PONOS cuando así lo solicite los procedimientos y controles que implementará para monitorizar y alertar sobre posibles violaciones de la seguridad de los sistemas.
    - Custodia y explotación de los logs de seguridad.
    - Supervisión de la configuración de seguridad de los elementos que forman la infraestructura tecnológica que da servicio al PONOS.

- Gestión de usuarios:
    - No se permitirá la existencia de usuarios genéricos salvo aquellos requeridos por las tecnologías empleadas.

- Control de acceso (en caso de que SEC&TECH4ALL utilice infraestructura propia para la prestación del servicio):
    - Deberán estar disponibles para PONOS, en caso de que lo solicite, los controles que implementará SEC&TECH4ALL para garantizar que todos los elementos con los que prestará el servicio se administran y explotan de forma segura. Esto incluye servidores y equipamiento de redes. Expresamente deberá detallar:

        1. Políticas de usuarios /contraseñas de los operadores y administradores de sistemas o productos, incluyendo expresamente gestores de bases de datos.
        2. Acceso a los sistemas mediante herramientas que protejan la confidencialidad de las contraseñas de los administradores, por ejemplo, SSH en UNIX.
        3. Protección de los sistemas servidores frente a accesos no autorizados.
        4. En casos de acceso a información confidencial, el servicio deberá proveer de la capacidad de autenticación multi-factor.

- SEC&TECH4ALL será responsable de la implantación de medidas de seguridad física para la protección de los sistemas de información ubicados en sus instalaciones ante accesos no autorizados y ante daños físicos.
- SEC&TECH4ALL debe establecer una segregación de funciones adecuada, que establezca las medidas suficientes y necesarias para asegurar que los derechos de acceso (roles y perfiles) para cada usuario del Servicio, se asignan de acuerdo con las necesidades funcionales de cada uno.
- SEC&TECH4ALL debe establecer los controles suficientes y necesarios para asegurar que el acceso lógico a los sistemas que tienen información relevante, se controla de acuerdo con los requisitos establecidos por PONOS.
- SEC&TECH4ALL debe establecer las medidas suficientes y necesarias para asegurar realizar revisiones periódicas sobre los permisos de acceso y los controles de acceso configurados en los sistemas involucrados en el servicio.
- SEC&TECH4ALL debe establecer las medidas suficientes y necesarias para asegurar que accesos remotos al entorno tecnológico sean controlados y monitorizados.
- SEC&TECH4ALL deberá asegurar que la información relacionada al servicio prestado no es transmitida a terceros o recursos tecnológicos no autorizados por PONOS.

- Gestión de vulnerabilidades (en caso de que SEC&TECH4ALL utilice infraestructura propia para la prestación del servicio):
  - SEC&TECH4ALL deberá implementar un proceso de monitorización de vulnerabilidades de la infraestructura tecnológica del Servicio, identificando y tratando las vulnerabilidades oportunamente sin exponer la información del PONOS a dichos riesgos. Adicionalmente, deberá realizar periódicamente evaluación de seguridad de la red interna y perimetral por un tercero independiente.

- Planes de concienciación:
  - SEC&TECH4ALL implementará planes de concienciación en materia de seguridad de la información, que incluyan a todos los empleados que prestan servicio a PONOS.

2.1.5 Cumplimiento de estándares, normativas, regulaciones o certificaciones en materia de seguridad:

En caso de que el Servicio trate información sujeta a certificaciones de seguridad, SEC&TECH4ALL deberá presentar a PONOS las certificaciones aplicables cuando lo requiera. Particularmente,

- Si la naturaleza del Servicio prestado almacena o realiza el tratamiento de información sobre tarjetas de créditos/débitos, SEC&TECH4ALL deberá estar certificado con PCI-DSS.
- Si el Servicio prestado almacena o realiza el tratamiento de información personal, deberá cumplir con la legislación aplicable de tratamiento de datos personales.

2.2. PROCESOS DE CONTROL

PONOS podrá realizar revisiones de carácter:

- ordinario, como parte de la evaluación de la prestación del servicio, o

- extraordinario, por motivos de un incidente de seguridad, o en caso de producirse alguna ampliación, regresión de los servicios o darse circunstancias que lleven a PONOS a considerar oportuno el realizarlas.

PONOS realizará estas revisiones en función del patrón de actividad, siguiendo un método de evaluación, alcance, método de seguimiento y periodicidad establecidos por PONOS.

SEC&TECH4ALL deberá prestar cuanta colaboración sea necesaria para dar adecuado cumplimiento a los requerimientos de inspección que pudieran formularle PONOS o las personas o empresas designadas por PONOS.

Adicionalmente, el PONOS ejercerá el control sobre los riesgos tecnológicos asociados al Servicio, recibiendo por parte dSEC&TECH4ALL la siguiente información cuando sea requerida:

- Revisión de informes de auditoría y/o certificaciones, por ejemplo:
  - Informes de auditoría interna /control interno.
  - Informes emitidos por terceros independientes (SOC 2 tipo 2, ISAE 3402, SSAE 16, etc.).
  - Certificaciones de seguridad (ISO 27001, etc.).
  - Certificaciones de calidad del Servicio (ISO 9001, ISO 2000, etc.).

Adicionalmente a los informes presentados, PONOS deberá tener la capacidad de desarrollar un plan de evaluación de controles de riesgo tecnológico y ejecutarlo de acuerdo a los plazos, alcances y procedimientos que se acuerden con SEC&TECH4ALL.

- Supervisión periódica de indicadores de seguridad del Servicio:
  - Los indicadores a supervisar acordados previamente a la firma del contrato y deberán revisarse periódicamente.
  - Acceso a cuadros de mando o consolas por parte de PONOS, que le permitan la monitorización continua del riesgo tecnológico.
- Reporte de eventos relevantes por parte dSEC&TECH4ALL:
  - Incidencias de seguridad.
  - Pruebas de recuperación ante desastres.
- Información sobre la infraestructura tecnológica que da soporte a PONOS (en caso de que SEC&TECH4ALL utilice infraestructura propia para la prestación del servicio):
  - Arquitectura de red.
  - Arquitectura de seguridad perimetral.
  - Servidores y bases de datos.
  - Protocolos de red y comunicaciones.
  - Otros necesarios para que PONOS pueda ejercer adecuadamente las funciones de control.
- SEC&TECH4ALL deberá solventar las debilidades de control identificadas por PONOS en las revisiones realizadas siguiendo los planes de acción acordados.
- Control interno dSEC&TECH4ALL:
  - Éste dispondrá de una función de control interno que velará por el cumplimiento de todos los controles requeridos y de verificar la implantación del modelo de control requerido.
  - El Prestador del servicio describirá y pondrá a disposición de PONOS, cuando así lo solicite, los procedimientos y controles que articulará internamente para asegurar que los requisitos enunciados se cumplen.
- Regresión del Servicio

  - PONOS y SEC&TECH4ALL deberán definir y acordar procedimientos de devolución y en su caso, destrucción segura de la información utilizada por SEC&TECH4ALL durante la prestación del Servicio.
- Controles coordinados con PONOS:
  - PONOS y el prestador del Servicio acordarán los procedimientos para que todo incidente de seguridad sea comunicado diligentemente a PONOS. Se definirán protocolos de comunicación específicos para casos en los que se requiera una actuación inmediata por parte del PONOS para mitigar el impacto de incidentes de seguridad.
  - Control técnico de PONOS. PONOS podrá verificar en cualquier momento el cumplimiento de los requisitos técnicos, tanto mediante visitas a las instalaciones dSEC&TECH4ALL, como haciendo uso de medios seguros de acceso remoto que se pactarán con el prestador del Servicio.
  - Aquellos aspectos que se observen en estas revisiones y que PONOS considere una violación de la presente normativa o que puedan poner en riesgo los sistemas del PONOS serán denunciados a la prestadora del servicio a la que se dará un plazo de tiempo para su resolución con el consiguiente compromiso contractual de que éste de cumplimiento a los aspectos observados según lo acordado con PONOS.

## 2.3. ANÁLISIS DE RIESGOS

SEC&TECH4ALL debe realizar un proceso de análisis de riesgos contemplando los riesgos involucrados en el servicio prestado a PONOS de forma periódica y cuando se produzcan cambios relevantes en el entorno tecnológico. También debe supervisar la efectividad de las acciones definidas para el tratamiento de los riesgos.

MEDIDAS TECNOLÓGICAS

3.1. USUARIOS Y PUESTOS DE USUARIOS (en caso de que los usuarios y/o puestos de usuario sean gestionados por el Proveedor)

- Tener identificación inequívoca de los usuarios. No deberán compartirse códigos de usuario entre personas. En todo momento, los códigos de usuario usados para acceder a las aplicaciones deberán permitir al prestador del Servicio identificar inequívocamente a la persona que accede.
- Tener registro actualizado de usuarios. El prestador del Servicio deberá mantener un registro actualizado para cada sistema o aplicación. El registro reflejará la asociación de cada código de usuario con la persona que lo tiene asignado.
- El registro deberá reflejar todos los cambios en el mapeo: altas, bajas y posibles modificaciones.
- Procesado inmediato de las bajas de usuarios. Las bajas de usuarios deberán ejecutarse de forma inmediata mediante las herramientas de administración de las aplicaciones, inhabilitando el acceso a éstas con el código de usuario dado de baja.
- Tener instalado solamente el software imprescindible para la adecuada prestación del Servicio.
- Contar con protección antivirus que deberá mantenerse operativa y actualizada en todo momento.
- Disponer de mecanismos de registros de la actividad usuaria.
- Carecer de dispositivos de salida tales como USB, unidad lectora/grabadora de CD/DVD u otros que permitan la extracción de datos del mismo.
- Tener restringido el acceso a Internet o a cualquier tipo de conexión que posibilite la fuga de información de los datos tratados en los mismos.
- Los usuarios NUNCA serán administradores locales de sus puestos.

3.2. AUTENTICACIÓN

- El acceso de administradores a sistemas de información deberá realizarse empleando canales cifrados y autenticación fuerte.
- En caso de que el servicio requiera atender a clientes, se realizará la autenticación de los clientes mediante mecanismos de doble factor, al menos para la ejecución de operaciones o consulta de información confidencial.

3.3. COMUNICACIONES (en caso de que el Proveedor preste servicio desde sus instalaciones):

- Las comunicaciones a través de redes públicas deberán estar cifradas.
- La conexión del CPD del Proveedor con la red interna de PONOS sólo se podrá llevar a cabo estableciendo las medidas de control que determine el área de Seguridad de la Información, tras un análisis detallado de las necesidades.
- Las comunicaciones con el CPD de PONOS estarán redundadas.
- Deberá estar a disposición de PONOS, cuando así lo solicite, un mapa completo de la red de la prestadora del Servicio en que se identifiquen perfectamente todos los elementos de comunicaciones que intervengan, así como los elementos de seguridad.
- Se contará con al menos las siguientes medidas de seguridad perimetral: Firewall, Sistemas de Detección y Prevención de Intrusos (IDS/IDPS), Zona, Desmilitarizada (DMZ), Redes Privadas Virtuales (VPN).

3.4. MECANISMOS DE SEGURIDAD

- Todos los sistemas de autenticación de usuarios, almacenamiento de credenciales, almacenamiento de logs y de criptografía deberán ser proporcionados o aprobados previamente por PONOS.
- El Proveedor no almacenará credenciales de clientes ni de usuarios en la base de datos u otro medio.

3.5. SEGREGACIÓN DE ENTORNOS (en caso de que el Proveedor utilice infraestructura propia para la prestación del Servicio):

- El entorno de producción debe estar segregado física o lógicamente de los entornos no productivos, de modo que exista control en el intercambio de información entre ellos.
- Los entornos no productivos no pueden contener datos reales.
- La red de usuarios deberá estar segregada de la red de sistemas centrales, permitiéndose la conectividad mínima necesaria para el acceso de los usuarios a los sistemas que necesiten para realizar sus funciones.

3.6. SEGURIDAD DE SERVIDORES (en caso de que el Proveedor utilice infraestructura propia para la prestación del servicio):

- Los servidores estarán plataformados de acuerdo a buenas prácticas reconocidas y sólo tendrán activos los servicios necesarios.
- Los servidores necesarios para la prestación del Servicio a ser posible deberán estar segmentados lógicamente.
- Se deberá de garantizar la protección de los datos y asegurar que no son visibles excepto para el Cliente.
- Los servidores se encontrarán adecuadamente cerrados/precintados, al objeto de que cualquier manipulación pueda ser detectada visualmente.
- Los servidores necesarios para la prestación del Servicio deberán tener instalado solamente el software imprescindible para la adecuada prestación del Servicio.
- Los servidores deberán contar con protección antivirus que deberá mantenerse operativa y actualizada en todo momento.
- Seguridad perimetral:
    - El servidor que aloje la aplicación deberá estar protegido de accesos de terceros mediante cortafuegos.
    - El servidor de base de datos deberá instanciarse en un sistema distinto al de ejecución de la aplicación, habilitando únicamente la comunicación con el servidor donde se aloje la aplicación, es decir, no deberá ser directamente accesible desde Internet.
    - En caso de que existan aplicaciones expuestas a Internet, el acceso a las mismas debe estar apantallado por un dispositivo que funcione como proxy inverso, ubicado en una DMZ protegida por una doble barrera de cortafuegos.

3.7. SEGURIDAD EN EL USO DEL CORREO ELECTRÓNICO (en caso de que el Proveedor realice envíos de correo en nombre de PONOS o con información que hace referencia a éste):

Cuando el Proveedor de Servicios realiza envíos de correo en nombre de PONOS o con información que hace referencia a éste, debe cumplir los siguientes requisitos:

**Requisitos Generales:**

Las siguientes medidas son consideradas obligatorias para cualquier iniciativa que utilice el canal e-mail:

- Las direcciones web (URL) incluidas en los correos electrónicos y los contenidos de los mismos deben ser supervisados previamente por el Área de Seguridad de la Información de PONOS.
- El Área de Seguridad de la Información de PONOS debe conocer los datos de cliente que se van a incluir en los correos. Éstos no deben ser confidenciales ni secretos y este departamento determinará si deben ser enmascarados y de qué modo.
- Deberán quedar rastros y evidencias (logs) de cuándo y a quién se envían los correos desde el servidor de correos utilizado para el envío de los correos electrónicos, tanto si se realiza en la infraestructura de PONOS como en la dSEC&TECH4ALL.
- En los registros de actividad (logs) deberá quedar registrada la fecha y hora de envío, cuenta origen con la que se envía el correo y destinatarios del correo.
- Los correos deben incluir los avisos/recomendaciones acordadas con el área de Seguridad de la Información de PONOS.
- Los correos deberán ser emitidos con un dominio registrado a nombre de PONOS.
- El departamento de Mensajería (en el caso de ser PONOS quien realiza el envío) o SEC&TECH4ALL, deberá arbitrar mecanismos de control sobre las listas negras de SPAM para controlar que los dominios de PONOS no aparezcan.
- Los correos enviados a clientes deben pasar los controles necesarios para estar libres de virus. Es decir, los correos deberán explorarse con las herramientas de antivirus existentes en PONOS o, en caso de externalizarse, en SEC&TECH4ALL.

**Requisitos Recomendados:**

- Es recomendable implementar el SPF, un control de verificación a nivel DNS que permite asegurar que el correo se ha emitido desde ese Servidor de Correo y no desde otro suplantado. Este control además mitiga el riesgo de SPAM a través de este servidor.
- Si el documento enviado tiene ofertas personalizadas para los clientes, tanto en PDF como en el cuerpo del mensaje, es requisito que a la parte personalizada se le asigne un Nº REFERENCIA asociado al documento (único por cada documento).
- El email debe ser redactado o diseñado con información personalizada para el cliente. La información personalizada no debe ser confidencial ni secreta, y dependiendo de qué tipo de información presente, ésta podría necesitar ser enmascarada. Los datos a incluir deben ser supervisados y acordados con el área de Seguridad de la Información de PONOS.