1.- OBJETO

El presente documento tiene por objeto el establecimiento de las directrices de contratación con empresas proveedoras con los que se intercambie información o bien accedan a la información de **INNPO** tanto física como de manera lógica.

2.- POLÍTICA DE CONTRATACIÓN

2.1. Condiciones en la contratación de empresas proveedoras

Para evitar que la contratación de un proveedor o proveedora introduzca posibles vulnerabilidades, como la posibilidad de daño, pérdida o compromiso de los datos o bien la disponibilidad e integridad de aplicaciones se tomarán de manera general las siguientes medidas de seguridad:

- Se firmarán acuerdos de confidencialidad, con las empresas proveedoras de servicios que puedan tener acceso a la información de los sistemas, que contemplen la identificación de las medidas de confidencialidad, integridad y disponibilidad de los activos afectados por el alcance. Las cláusulas que establecen la confidencialidad y la devolución de activos una vez finalizado el acuerdo son obligatorias.
- Además, los contratos deben garantizar la entrega confiable de productos y servicios, que es sumamente importante con empresas proveedoras de servicios de la nube.
- El trabajo a desarrollar por un tercero/a, en el caso de que sea puntual debe ser vigilado de forma continua.
- La adquisición de sistemas, aplicaciones o recursos que vayan a tratar información pero que no tengan la condición de servicios, siguen necesariamente el proceso de homologación, evaluación y seguimiento de empresas proveedoras establecido en ***INNPO***
- Se supervisará el nivel de servicio que se está ofreciendo para comprobar que sea el contratado. En el caso de que se encontraran incidencias en el suministro de los servicios se revisarán los contratos, se comunicará a la tercera parte y de no resolver el problema se tomarán las medidas legales que la Dirección/CEO considere oportuno.
- La persona Responsable del Sistema o quien él/ella determine, está obligado/a a **registrar los incidentes de seguridad** que se detecten en el cumplimiento de los citados contratos, con el fin de poder analizar la calidad de los servicios.
- Después de cambios o si tras analizar sus servicios se detectaran insuficiencias, se deberán mejorar las políticas, procedimientos, instrucciones y controles; así como la realización de una nueva evaluación de riesgos.
- La Dirección de la empresa o en su defecto la persona Responsable de Seguridad decide si es necesario realizar verificaciones de antecedentes determinados con terceras partes.

Para los proveedores de uso de servicios en la nube, además:

- Acuerdos de Nivel de Servicio (SLA) ofrecidos, incluyendo disponibilidad y tiempos de respuesta ante incidentes.
- Capacidades de recuperación ante desastres y continuidad del negocio.
- Mecanismos de seguridad física y lógica implementados por el proveedor.
- Políticas de gestión de acceso, cifrado, y borrado de datos.
- Localización geográfica de los datos y cumplimiento de los requisitos de soberanía de datos.
- Derechos de auditoría.

En su caso, se solicitará a los proveedores potenciales que proporcionen evidencia de sus controles de seguridad (ej. informes de auditoría, certificaciones, respuestas a cuestionarios de seguridad).

2.2. Supervisión y revisión de los servicios ofrecidos por las empresas proveedoras

- Se debe revisar y controlar periódicamente el nivel de los servicios y cumplimiento de las cláusulas de seguridad de parte de las empresas proveedoras y los informes y registros generados por ellos, también se les podría realizar una auditoría al menos una vez al año y de considerarse de que existe un riesgo alto de pérdida de información serán presenciales. Al menos se realizará de manera anual.
- Todos los incidentes de seguridad relacionados con el trabajo de la empresa proveedora deben ser elevados inmediatamente a la persona Responsable del Sistema.
- En caso de que se produzca alguna brecha de seguridad por parte de la empresa proveedora se tomarán las acciones pertinentes, pudiéndose bloquear la relación con la empresa proveedora durante un periodo determinado a criterios de la Dirección.

2.3. Requisitos de seguridad en contratos con terceras partes

- Los acuerdos que comportan el acceso de terceras partes a recursos de tratamiento de la información están basados en un contrato documentado en el que se recogen los requisitos de seguridad e incluyen las políticas y normas de seguridad de INNPO, asegurando la organización mediante la firma de este la no existencia de malentendidos con la tercera parte.
- En la redacción este contrato se debe tener en cuenta los requisitos específicos de seguridad, incluidos en el registro Cláusulas de seguridad para empresas proveedoras en función de los servicios a prestar por la tercera parte.

2.4. Cambios o finalización de servicios de la empresa proveedora

- Se gestionará cualquier cambio propuesto o tras la finalización del contrato. Si es necesario, la persona Responsable de seguridad realizará una nueva evaluación de riesgos antes de aceptar los cambios.

2.5. Eliminación de derecho de acceso y devolución de activos

- Cuando se modifica o finaliza un contrato, se deben eliminar los derechos de acceso para las personas trabajadoras de la empresa proveedora de acuerdo a la Política **POL – 06**: control de accesos
- Además, cuando se cambia o finaliza un contrato, el/la propietario/a del contrato debe asegurarse de que todo el equipamiento, software o información en formato electrónico o papel sea devuelto.

Para los proveedores de uso de servicios en la nube, además:
Se definirá un proceso claro para la terminación de la relación contractual con el proveedor, que incluirá:

- Confirmación de la eliminación segura de todos los datos de los sistemas del proveedor, de acuerdo con los términos contractuales y las políticas de retención de datos.
- Procedimientos para la migración segura de los datos a otro proveedor o a sistemas internos.

2.6 Incumplimiento de la Política

El incumplimiento de esta política puede dar lugar a acciones disciplinarias y puede tener consecuencias legales o contractuales.

En Vélez-Málaga (Málaga), a 20 de mayo de 2025

DIRECCIÓN/CEO