

1.- OBJETO

El presente documento tiene por objeto el establecimiento de las directrices de contratación con proveedores 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 proveedores

Para evitar que la contratación de un proveedor 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 los proveedores 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 proveedor de servicios de la nube.
- El trabajo a desarrollar por un tercero, 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 proveedores 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 al tercero y de no resolver el problema se tomarán las medidas legales que la Dirección considere oportuno.
- El Responsable de sistema o quien él determine, está obligado 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 el Responsable de Seguridad decide si es necesario realizar verificaciones de antecedentes determinados con terceros.

2.2. Supervisión y revisión de los servicios ofrecidos por los proveedores

- Se debe revisar y controlar periódicamente el nivel de los servicios y cumplimiento de las cláusulas de seguridad de parte de los proveedores 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 del proveedor deben ser elevados inmediatamente al Responsable del sistema/Compras.
- En caso que se produjera alguna brecha de seguridad por parte del proveedor, se tomarán las acciones pertinentes, pudiéndose bloquear la relación con el proveedor durante un periodo determinado a criterios de la Dirección.

2.3. Requisitos de seguridad en contratos con terceros

- Los acuerdos que comportan el acceso de terceros 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 del mismo la no existencia de malentendidos con el tercero.
- En la redacción este contrato se debe tener en cuenta los requisitos específicos de seguridad, incluidos en el registro Cláusulas de seguridad para proveedores en función de los servicios a prestar por el tercero.

2.4. Cambios o finalización de servicios del proveedor

- Se gestionará cualquier cambio propuesto o tras la finalización del contrato. Si es necesario, el responsable del sistema/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 los empleados del proveedor de acuerdo a la Política de control de acceso.
- Además, cuando se cambia o finaliza un contrato, el propietario del contrato debe asegurarse de que todo el equipamiento, software o información en formato electrónico o papel sea devuelto.

La Dirección de **INNPO**



En Vélez Málaga (Málaga) a 24 de Mayo 2024