ANEXO 18

ESPECIFICACIÓN TÉCNICA

REQUISITOS DE CIBERSEGURIDAD PARA EL SUMINISTRO DE SISTEMAS DIGITALES Y/O LA PRESTACIÓN DE SERVICIOS RELACIONADOS CON LOS MISMOS

ÍNDICE

1. OBJETO.

1.1 Definir los requisitos de Ciberseguridad que deben quedar asegurados en todas las actividades que afectan al satisfactorio comportamiento en el suministro o el servicio relacionado con sistemas o componentes considerados como Sistemas Digitales.

2. APLICABILIDAD.

Los requisitos de Ciberseguridad serán de aplicación para peticiones de oferta de Montaje/Pruebas, Cambios de Diseño, Servicios y Materiales que contengan sistemas o información en formato digital.

3. REFERENCIAS.

- PG-0.21 “Programa de Ciberseguridad de ANAV” rev. 1.

4. REQUISITOS DE CIBERSEGURIDAD.

4.1 Confidencialidad.

La relación con empresas de suministros y/o servicios que tengan acceso a información sobre Sistemas Digitales, debe estar regulada mediante contratos o cláusulas de confidencialidad.

Siempre que la prestación de servicios suponga el acceso de personal externo a Sistemas Digitales o a información confidencial de ANAV, se considerarán cláusulas y contratos de confidencialidad en la contratación.

4.2 Intercambios de información

En los intercambios de información con los suministradores, los correos electrónicos que contengan información sobre Sistemas Digitales deben ir cifrados, mediante PGP u otro algoritmo compatible, de forma que se asegure la confidencialidad e integridad de los datos enviados y recibidos. Al inicio de cada proyecto se debe realizar el intercambio de claves públicas entre las personas implicadas en el mismo.

4.3 Fiabilidad

Los suministradores deben asegurar por contrato que los productos adquiridos por ANAV están libres de vulnerabilidades comprobables y código malicioso conocido.

Si un suministrador detecta una vulnerabilidad en su producto, debe comunicarlo inmediatamente a ANAV, ya sea en la fase de diseño, implantación o explotación.

Se requiere que los productos adquiridos dispongan de embalajes, precintos o sellos a prueba de manipulaciones.

4.4 Seguridad en las instalaciones del suministrador

Los suministradores deben garantizar la confidencialidad e integridad de la información del proyecto en sus instalaciones. A los suministradores que desarrollen software para Sistemas Digitales se les exigirá la presentación de un Plan de Seguridad general, dónde se detalle qué medidas se toman en su empresa para cumplir con este requisito.

ANAV se reserva el derecho de auditar la Ciberseguridad en las instalaciones de los suministradores de Sistemas Digitales.

4.5 Mantenimiento y actualización

Se deben acordar las responsabilidades del suministrador en lo referido a actualización, mantenimiento y/o soporte a largo plazo del hardware y software de seguridad, incluyendo las actualizaciones de los programas de protección contra código malicioso (antivirus, antimalware, etc.).

No se permitirá el acceso remoto para el mantenimiento o la administración de sistemas ni equipos. Dicha administración deberá realizarse localmente.

Las actividades de los suministradores serán supervisadas y controladas por personal de ANAV.

4.5.1 Actualizaciones

Por norma general, no se admitirá la descarga de componentes software de Internet (nuevas versiones, parches, actualizaciones, etc.). El PROVEEDOR deberá proveer el software en un soporte magnético (CD, DVD, etc.). Si esto no es posible, el PROVEEDOR deberá proveer el *hash* del archivo o emplear otro método que permita verificar la integridad de los contenidos descargados.

El personal de ANAV actualizará y parcheará el software de los sistemas según sus Procedimientos internos de Gestión de Cambios y las recomendaciones del PROVEEDOR. No se instalarán todas las actualizaciones ni los parches que publiquen los fabricantes o desarrolladores de los diferentes componentes, solamente aquellos explícitamente recomendados.

Es responsabilidad del PROVEEDOR probar las actualizaciones y los parches de seguridad en un entorno de pruebas, ya sea suyo o propio de ANAV, antes de entregarlos para su instalación en los sistemas en producción.

4.5.2 Uso de herramientas para el mantenimiento o actualización

En el caso de realizar conexión de soportes de información (Memorias USB, discos duros externos/extraíbles, CD/DVD, etc) y/o dispositivos móviles (Ordenadores portátiles, teléfonos móvies, PDAs, tablets, etc) propios del PROVEEDOR a los Sistemas Digitales de ANAV, si el PROVEEDOR prevé que necesitará algún software específico para visualización, configuración, parametrización y/o extracción de datos del sistema, deberá proveerlo a ANAV con anterioridad a los trabajos para que se instale y se utilice desde los equipos que indique el personal de ANAV.

En caso de utilizar los soportes o dispositivos del PROVEEDOR, éstos se chequearían en busca de código malicioso antes de su uso según los procedimientos establecidos por ANAV. No se aceptarán soportes ni dispositivos cifrados, dado que no se puede chequear su contenido. Si el trabajo se alargara varios días, existirían dos alternativas: chequear los soportes o dispositivos cada día, o bien dejarlos bajo custodia de ANAV, para asegurar que no han sido modificados desde el último chequeo. Además, se comprobaría que no contienen información de la Organización antes de que abandonaran la instalación, salvo autorización explícita.

4.6 Prestación de Servicios

El personal subcontratado para la prestación de un servicio relacionado con Sistemas Digitales debe conocer sus obligaciones en materia de Ciberseguridad para evitar posibles fallos por errores humanos o por actos malintencionados.

NOTIFICACIÓN DEL ESTADO DE CIBERSEGURIDAD

D/Dña _____, en nombre y representación de la empresa _____, con domicilio en _____, y número de Identificación Fiscal _____ , certifica que:

- Todo el personal relacionado con el tratamiento de la información de ANAV:

  ☐ Ha recibido la formación necesaria según sus funciones.

  ☐ Cuenta con un compromiso de confidencialidad documentado en vigor.

- Dispone de la siguiente documentación:

DOCUMENTACIÓN	SI (Ref. Documento) / NO
Políticas seguridad TI	□ SI Ref.: □ NO
Registro de eventos de ciberseguridad	□ SI Ref.: □ NO
Análisis de riesgos TI	□ SI Ref.: □ NO
Procedimiento de gestión de incidentes de ciberseguridad	□ SI Ref.: □ NO
Evaluación de proveedores sobre protección de información (en caso de subcontrataciones)	□ SI Ref.: □ NO
Auditorías en materia de ciberseguridad	□ SI Ref.: □ NO

- Dispone de las siguientes certificaciones:

CERTIFICACIÓN	FECHA VALIDEZ	ENTIDAD EMISORA	ALCANCE
ISO 27001: Seguridad de la información			
Otras Certificaciones: Especificar			

- Las siguientes medidas de seguridad:

MEDIDAS APLICADAS	SITUACIÓN	NIVEL IMPLANTACIÓN
Control de acceso lógico a los sistemas de información (usuario/contraseña, tarjeta,.).	☐ SI ☐ NO	☐ Parcial. ☐ Completo pero no se dispone de procedimiento. ☐ Completo y se dispone de procedimiento.
Registro de accesos a los sistemas.	☐ SI ☐ NO	☐ Parcial. ☐ Completo pero no se dispone de procedimiento. ☐ Completo y se dispone de procedimiento.
Copias de seguridad y recuperación de datos.	☐ SI ☐ NO	☐ Parcial. ☐ Completo pero no se dispone de procedimiento. ☐ Completo y se dispone de procedimiento.
Cifrado de los datos	☐ SI ☐ NO	☐ Parcial. ☐ Completo pero no se dispone de procedimiento. ☐ Completo y se dispone de procedimiento.
Software antivirus	☐ SI ☐ NO	☐ Parcial. ☐ Completo pero no se dispone de procedimiento. ☐ Completo y se dispone de procedimiento.
Firewall en las comunicaciones de la empresa con el exterior.	☐ SI ☐ NO	☐ Parcial. ☐ Completo pero no se dispone de procedimiento. ☐ Completo y se dispone de procedimiento.
Control acceso físico	☐ SI ☐ NO	☐ Parcial. ☐ Completo pero no se dispone de procedimiento. ☐ Completo y se dispone de procedimiento.
Destrucción segura de la información en formato papel y electrónico (discos, USB, etc.) al finalizar el contrato.	☐ SI ☐ NO	☐ Parcial. ☐ Completo pero no se dispone de procedimiento. ☐ Completo y se dispone de procedimiento.

- Compromisos adicionales:

COMPROMISO	SITUACIÓN	MEDIDAS A TOMAR
	□ SI □ NO	
	□ SI □ NO	
	□ SI □ NO	
	□ SI □ NO	

Firmado / Sello empresa

En a de 20

ACUERDO DE CONFIDENCIALIDAD

De una parte, _____ en nombre y representación de ANAV (Asociación Nuclear Ascó-Vandellós II A.I.E.), con domicilio en Ctra. Nacional 340, Km. 1123, L'Hospitalet de l'Infant, y Número de Identificación Fiscal V-58209685. En adelante y a los efectos de este Acuerdo.

Y de otra parte, _____, en nombre y representación de_____, con domicilio _____, y Número de Identificación Fiscal _____. En adelante y a los efectos de este Acuerdo.

EXPONEN

I.- Que con motivo de la licitación _____ las partes firmantes o compañías vinculadas, pueden facilitarse mutuamente ciertos datos, información y/o documentos relativos a sus productos, tecnología, know-how, secretos comerciales, actividades de marketing, desarrollo de productos y de negocio, y otros de similar naturaleza, que tienen carácter de privadas y confidenciales para el EMISOR y/o RECEPTOR, según proceda (de ahora en adelante llamados "Información Confidencial").

II.- Que en el presente Acuerdo la expresión "EMISOR" significa la parte que facilita Información Confidencial.

III.- Que en el presente Acuerdo la expresión "RECEPTOR" significa la parte a quien se facilita o recibe Información Confidencial.

ESTIPULACIONES

PRIMERA.- Cualquier Información, fuese cual fuere su naturaleza (bien técnica, comercial, financiera, operacional o de otro tipo), en cualquier forma o soporte (ya sea verbal, escrita, grabada o de cualquier otro tipo), que pudiera ser facilitada por el EMISOR al RECEPTOR en relación con el Proyecto descrito en el expositivo del presente contrato, será considerada como "Información Confidencial", incluyéndose en esta categoría aquella información que fuese generada a partir de la Información Confidencial.

SEGUNDA.- El RECEPTOR se compromete a aceptar la Información Confidencial en un marco de confianza y a no facilitarla a ningún tercero ni utilizarla para su propio beneficio sin obtener el previo consentimiento escrito del EMISOR.

Sin perjuicio de lo anterior, el EMISOR podrá facilitar libremente la Información Confidencial a otras entidades del Grupo a que pertenece el EMISOR que acepten obligarse por las estipulaciones de presente Contrato.

TERCERA.- El RECEPTOR se obliga asimismo a:

a) tratar la Información Confidencial como estrictamente confidencial,

b) guardar la Información Confidencial, bien sea escrita, grabada o en cualquier otro soporte, separada de cualquier otra información de la que pudiera disponer el RECEPTOR;

c) utilizar o transmitir la Información Confidencial exclusivamente para los fines del Proyecto;

d) utilizar procedimientos de control de dicho uso o transmisión de la Información Confidencial; el RECEPTOR no realizará copia de la Información Confidencial sin el previo consentimiento escrito del EMISOR, excepto aquellas copias que sean necesitadas por el RECEPTOR para un estudio interno;

e) restringir el acceso a la Información Confidencial únicamente a aquellos empleados suyos que necesiten conocerla para los fines del Proyecto, y asegurarse de que dichos empleados conocen las obligaciones que les resultan aplicables en virtud de lo establecido en el presente documento;

f) no facilitar Información Confidencial a tercero alguno sin el previo consentimiento escrito del EMISOR, y asegurar que, en caso de haber obtenido dicha autorización, que dicho tercero firma un compromiso de confidencialidad con el EMISOR en términos equivalentes a los del presente documento. Todo ello sin perjuicio de lo establecido en el segundo párrafo de la estipulación segunda del presente contrato.

CUARTA.- Cualquier publicidad o información a los medios de comunicación con respecto incluso a la simple existencia del Proyecto o del presente contrato o su contenido, deberá ser previamente aprobada por escrito por ambas partes.

QUINTA.- El EMISOR será en todo momento el titular exclusivo de la Información Confidencial, que estará protegida legalmente. En el caso de que dicha Información Confidencial sea mejorada, revisada o modificada en cualquier modo, continuará siendo de la exclusiva propiedad del EMISOR.

SEXTA.- En ningún caso se entenderá implícito en modo alguno que el hecho de que el EMISOR facilite Información Confidencial significa la concesión de licencia o la cesión de cualquier naturaleza a favor del RECEPTOR de cualesquiera derechos de patente, marca, modelo de utilidad, diseño, copyright, o derecho alguno de propiedad industrial o intelectual.

SÉPTIMA.- Ninguna de las partes utilizará el nombre, marca, nombre comercial, o cualesquiera otros derechos de propiedad industrial o intelectual de la otra parte, sin el previo consentimiento escrito de ésta.

OCTAVA.- A la simple solicitud y elección del EMISOR, el RECEPTOR procederá a destruir o devolver al EMISOR toda Información Confidencial, bien sea escrita, grabada o en cualquier otro soporte que se pudiera encontrar recogida. En el caso de que la Información Confidencial debiera ser destruida, el RECEPTOR facilitará al EMISOR un certificado escrito de que tal destrucción se ha realizado, en el plazo de quince (15) días naturales a partir del momento en que el EMISOR hubiese solicitado dicha destrucción. La destrucción o devolución de la Información Confidencial no relevará al RECEPTOR de su obligación de tratar dicha Información Confidencial como estrictamente confidencial.

NOVENA.- Las restricciones relativas al uso, reproducción, transmisión o acceso a la Información Confidencial a que se refiere el presente contrato, no serán de aplicación en los casos en que la información:

a) después de haber sido facilitada como Información Confidencial, deviniese accesible públicamente en publicación impresa o en publicaciones de general circulación, sin que en dicha circunstancia hubiese intervenido incumplimiento alguno del presente contrato; o

b) se encontrare legalmente en posesión del RECEPTOR ya en el momento en que hubiese sido facilitada por el EMISOR, o que hubiese sido obtenida independientemente por el RECEPTOR con anterioridad a haberle sido facilitada por el EMISOR, y sin utilización alguna de la Información Confidencial recibida del EMISOR; o

c) que el RECEPTOR demuestre haber obtenido la Información legalmente de modo no restringido de cualquier tercero que no estuviese sujeto por obligaciones de confidencialidad similares con el EMISOR; o

d) que deba ser obligatoriamente facilitada en virtud de disposición legal o por resolución válidamente emitida por cualquier autoridad administrativamente competente, tribunal u órgano jurisdiccional, legalmente facultado para obligar a tal disponibilidad, siempre y cuando, en todo caso, que el RECEPTOR así requerido para ello, notifique inmediatamente al EMISOR de la recepción de tal requerimiento, a fin de que el EMISOR pueda evaluar si existe posibilidad de eludir el mismo o pueda prestar cualquier apoyo razonablemente solicitado por el RECEPTOR (a cargo del RECEPTOR).

DÉCIMA.- la Información Confidencial se facilita de buena fe, pero sin compromiso alguno, o garantía de cualquier tipo, expresa o implícita, relativa a la utilidad, validez, exactitud o integridad de la Información Confidencial.

DECIMOPRIMERA.- Cada una de las partes responderá frente a la otra parte de cualquier daño directo debido a dolo, derivado del incumplimiento de cualesquiera obligaciones del presente contrato, excluyendo expresamente cualquier tipo de responsabilidad por daños indirectos o eventuales. Habida cuenta que el simple incumplimiento del presente contrato puede causar a la otra parte daños irreparables, la parte perjudicada tendrá derecho a reclamar las correspondientes indemnizaciones, además de cualquier otra acción legal que le pudiera corresponder.

DUODÉCIMA.- El presente contrato sólo podrá ser modificado o corregido por escrito firmado por representante legal de ambas partes.

DECIMOTERCERA.- Los derechos y deberes derivados del presente contrato, se otorgan y asumen “intuitu personae”, y no podrán ser cedidos o transmitidos a tercero alguno sin la previa autorización escrita de la otra parte.

DECIMOCUARTA.- El presente contrato es obligatorio para las partes y obligan a sus respectivos sucesores legales en las respectivas actividades, incluyendo cualquier persona jurídica resultante de una fusión, adquisición o cualquier otra reestructuración que pudiera sufrir cualquiera de las firmantes. Asimismo obligará a las entidades vinculadas o asociadas de las Partes, incluyéndose en tales conceptos incluso la matriz de las mismas o cualquier otra entidad legal que tal matriz controle directa o indirectamente, o que se encuentre bajo el control directo o indirecto de cualquiera de las partes, por disponer de la mayoría del capital o de los derechos de voto, siempre que participen activamente en la ejecución del proyecto descrito en el Exponen I.

DECIMOQUINTA.- En el caso de cualesquiera de las estipulaciones del presente contrato deviniese o fuere considerada o declarada inválida, nula, ilegal o no aplicable fuese cual fuere la razón para ello, las restantes disposiciones no serán afectadas, quedando válida y plenamente aplicables. En el caso de que una sola estipulación del contrato resultase afectada por dicha causa, las partes intentarán reemplazar dicha estipulación de modo amistoso, por otra que recoja en la mayor medida posible lo establecido en la que hubiese sido declarada inválida.

DECIMOSEXTA.- El presente contrato se regirá por la legislación común civil española.

Para todo lo relativo a la interpretación o ejecución de lo establecido en el presente Contrato, ambas partes se someten a la jurisdicción de los Juzgados y Tribunales de Barcelona, con renuncia expresa de cualquier otro fuero que les pudiera corresponder. Asimismo ambas partes acuerdan que el idioma para comunicaciones relativo a la ejecución o interpretación de lo establecido en el presente contrato, será el español-castellano.

DECIMOSÉPTIMA.- El RECEPTOR quedará obligado por las estipulaciones contenidas en el presente Contrato durante un periodo de cinco (5) años a partir de la fecha de recepción de cualquier Información Confidencial relativa al Proyecto, incluso aquella que hubiere sido facilitada con anterioridad a la firma de este documento.

Y en prueba de conformidad con todo lo anterior, ambas partes firman el presente documento, en duplicado ejemplar, ambos a un solo efecto, en el lugar y fecha indicados en el encabezamiento.

Por _____. Por ANAV

En a de de 20