

Sistemas Técnicos de Loterías del Estado
Manuel Tovar, 9
28034 - Madrid



**SISTEMAS TÉCNICOS DE
LOTERÍAS DEL ESTADO**

PROCEDIMIENTO DE SELECCIÓN DE
EMPRESAS DE SERVICIOS PARA LA
EVALUACIÓN DE VULNERABILIDADES Y
TEST DE INTRUSIÓN

SISTEMAS TÉCNICOS DE
LOTERÍAS DEL ESTADO

BASES DE LICITACIÓN QUE HAN DE REGIR EN EL PROCEDIMIENTO DE SELECCIÓN DE EMPRESAS DE SERVICIOS PARA LA EVALUACIÓN DE VULNERABILIDADES Y TEST DE INTRUSIÓN

SECCIÓN I: CONDICIONES GENERALES

1. ANTECEDENTES

SISTEMAS TÉCNICOS DE LOTERIAS DEL ESTADO, S.A.Unipersonal (en adelante STL), es una sociedad mercantil anónima, de carácter público, constituida como medio propio y servicio técnico de la Sociedad Estatal Loterías y Apuestas del Estado y cuyo objeto social abarca los servicios relativos a:

- Gestión de las loterías y apuestas mediante terminales a tiempo real o a través de sistemas telemáticos, informáticos e interactivos que puedan preverse, incluyendo la adquisición, montaje, instalación, mantenimiento y explotación de los sistemas adecuados a la prestación de estos servicios.
- Instalación y mantenimiento de los ordenadores o sistemas centrales de recogida de datos y escrutinio, así como de aquellos elementos de seguridad y comunicación precisos.
- Realización de estudios y trabajos que constituyan un apoyo a la gestión de los juegos de Loterías y Apuestas del Estado, facilitando a esta la asistencia informática que dicha entidad pública empresarial solicite.

La información es un activo con un alto valor para la organización y, en consecuencia, requiere una protección adecuada. Esto es especialmente importante en el creciente ambiente de negocios interconectados por redes de datos en el que la información está expuesta a un mayor rango de amenazas y vulnerabilidades.

En este contexto, Sistemas Técnicos de Loterías, como empresa con una importante infraestructura tecnológica y que gestiona varios servicios ofrecidos a través de Internet, desea contratar la realización por parte de un empresa especialista de pruebas de intrusión y un análisis de vulnerabilidades por parte de un proveedor externo.

La presente contratación se publica en cumplimiento de los principios de publicidad, concurrencia, igualdad, transparencia y no discriminación a los que STL se encuentra sometida como empresa del sector público, de conformidad con el artículo 176 de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público (en adelante LCSP).

2. OBJETO

Teniendo en cuenta los antecedentes expuestos, es objeto del presente concurso la selección de una empresa para la prestación de servicios informáticos con resultado de obra consistentes en la realización de pruebas de seguridad informática en la infraestructura y sistemas de información de STL proporcionando a STL como resultado de las citadas pruebas, los correspondientes test que se pasarán al sistema, los informes de resultados y evaluación y los entregables descritos en el apartado “2.2 Entregables del Servicio” de la Sección IV “Especificaciones Técnicas” del presente Pliego. Las pruebas irán fundamentalmente encaminadas a buscar debilidades en el control de acceso, autenticación, diseño y o programación en la configuración y despliegue de los sistemas.

A tales efectos, es objeto del presente concurso la contratación de las prestaciones que a continuación se describen distribuidas en los siguientes Lotes, a cambio del precio pactado, dentro del plazo señalado y de acuerdo con los requerimientos técnicos y funcionales definidos en este pliego:

- LOTE I: Cuatro pruebas, una por trimestre, de escáner de vulnerabilidades externas sobre dos direcciones IP, que permita probar el cumplimiento PCI-DSS.
- LOTE II: Cuatro pruebas, una por trimestre, de escáner de vulnerabilidades interno para un entorno bajo normativa PCI-DSS constituido por un grupo de veintinueve dispositivos de equipos de comunicaciones y servidores.
- LOTE III: Una prueba de intrusión interna para un entorno bajo normativa PCI-DSS constituido por un grupo de veintinueve dispositivos formado por equipos de comunicaciones, y servidores.
- LOTE IV: Una prueba de intrusión externa sobre el conjunto de servicios que ofrece la organización en un rango aproximado de 75 direcciones IP públicas, dos de las cuales están afectadas por normativa PCI-DSS.
- LOTE V: Prueba de intrusión interna sobre entorno aislado, tres equipos, una red y dos firewall con aproximadamente veinte reglas y veintiséis reglas NAT

Cualesquiera análisis, accesos, intrusiones y/o ataques a la seguridad de los sistemas de información de STL que con motivo del desarrollo de los trabajos del presente Pliego deba llevar a cabo por el adjudicatario, serán realizados con la máxima diligencia y con el único fin de analizar el estado de la seguridad de los sistemas de información, entornos de operaciones, y elementos de comunicaciones de STL de acuerdo con los objetivos señalados en el presente Pliego.

3. RÉGIMEN JURÍDICO Y JURISDICCIÓN

- El contrato objeto del presente procedimiento tiene carácter privado
- El orden jurisdiccional competente para resolver las controversias que puedan surgir entre las partes en relación con este contrato será el civil. En este sentido, las partes se someten expresamente a la competencia y jurisdicción de los Juzgados y Tribunales de Madrid capital con renuncia expresa a cualquier otro Fuero que pudiera corresponderles.
- El contrato se registrará e interpretará de acuerdo con la ley española.

4. VALOR ESTIMADO DEL CONTRATO

El valor estimado máximo del presente contrato es el siguiente para cada uno de los lotes, los precios se consideran con IVA excluido.

- LOTE I:	3.000 €
- LOTE II:	6.000 €
- LOTE III:	15.000 €
- LOTE IV:	25.000 €
- LOTE V:	9.000 €

Tanto en las ofertas que formulen los interesados, como en el presupuesto máximo de contratación, se entenderán comprendidos a todos los efectos los gastos generales, el beneficio industrial, así como los importes de los tributos de toda índole que graven las prestaciones objeto del contrato, excluido el impuesto sobre el valor añadido (IVA) o cualquier otro impuesto indirecto equivalente según corresponda, y que deberán ser identificados y posteriormente repercutidos como partidas independientes.

5. DURACIÓN

La ejecución de los servicios objeto de este procedimiento tendrá una duración de un (1) año máximo para los lotes I y II y de tres (3) semanas máximo para los lotes III, IV y V. Todos los plazos comenzarán a contar desde la firma del contrato.

SECCIÓN II: DE LAS OFERTAS

1. LUGAR Y PLAZO

Los interesados deberán presentar su oferta debidamente identificada en un sobre cerrado a la atención de:

SISTEMAS TECNICOS DE LOTERIAS, S.A.Unipersonal

ATT.: D. José Manuel Hombre Baena (Dpto. Compras)
C/ Manuel Tovar, 9,
28034, Madrid

En el caso de remitirse por correo, el proveedor deberá justificar la fecha de imposición del envío en la oficina de Correos y anunciar a STL la remisión de la oferta mediante telefax (91 348 92 12), en el mismo día. Sin la concurrencia de ambos requisitos no será admitida la proposición si es recibida por STL con posterioridad a la fecha de terminación del plazo señalado.

En el sobre deberá figurar el siguiente rótulo

**PROCEDIMIENTO DE ADJUDICACIÓN DE SERVICIOS PARA LA EVALUACIÓN
DE VULNERABILIDADES Y TEST DE INTRUSIÓN**

El plazo de recepción de ofertas finaliza a las 12 horas del día 12 de Diciembre de 2011.

2. CAPACIDAD DE OBRAR Y SOLVENCIA DE LAS EMPRESAS CONTRATANTES

Las empresas que participen en el procedimiento deberán tener capacidad de obrar, acreditar solvencia económica y técnica y no estar incurso en ninguna de las causas de prohibición de contratar previstas en el artículo 49.1 de la LCSP. Los empresarios deberán contar, asimismo, con la habilitación empresarial o profesional que, en su caso, sea exigible para realizar la actividad o prestación que constituye el objeto del contrato y que éste esté comprendido dentro de su objeto social. A tal fin, los participantes deberán presentar la siguiente documentación:

a) Capacidad de obrar:

Empresas españolas:

- Escritura de constitución o modificación, en su caso, inscrita en Registro mercantil cuando este requisito sea exigible conforme a la legislación mercantil que le sea aplicable. Si no lo fuere, la acreditación de la capacidad de obrar se realizará mediante la escritura o documento de constitución, estatutos o acto fundacional, en el que constaren las normas por las que se regule su actividad, inscritos, en su caso, en el correspondiente registro oficial.
- Los empresarios que deseen concurrir integrados en una unión temporal deberán asimismo indicar los nombres y circunstancias de los que la constituyan y la participación de cada uno, así como que asumen el compromiso de constituirse formalmente en unión temporal en caso de resultar adjudicatarios del contrato.
- Documento Nacional de identidad y poder notarial acreditativo de las facultades de contratación de la persona que firme el contrato.

Licitadores extranjeros, miembros de la U.E:

- Inscripción de la sociedad en el registro que sea procedente conforme a la legislación del Estado de origen, así como las autorizaciones que, en su caso y de acuerdo con la legislación de dicho Estado sean precisas.
- Fotocopia del pasaporte del representante apoderado.
- Certificado de residencia fiscal del país de origen

Licitadores procedentes de Estados no miembros de la U.E:

- Informe de la respectiva misión diplomática española que el Estado de procedencia de la empresa extranjera admite a su vez la participación de empresas españolas en la contratación con el sector público.
- Fotocopia del Pasaporte del representante apoderado.
- Certificado de residencia fiscal del país de origen

b) Habilitación profesional

- Documento original o copia autorizada de los títulos o documentos referentes a las autorizaciones o habilitaciones profesionales que, en su caso, resulten necesarias para el ejercicio de la actividad.

c) Solvencia financiera

- Cifras de las últimas cuentas anuales de la entidad, aprobadas y presentadas en el Registro Mercantil o en el Registro oficial que corresponda. Los empresarios no obligados a presentar las cuentas en registros oficiales podrán aportar, como medio alternativo de acreditación, los libros de contabilidad debidamente legalizados.

d) Solvencia técnica

- Relación de suministros / servicios en proyectos similares realizados en los últimos dos años que incluya importe, fechas y destinatario público o privado de los mismos, reservándose STL el derecho a solicitar en cualquier momento la conveniente acreditación de los mismos.
- Certificaciones técnicas.
- Certificaciones de los sistemas de gestión de calidad con arreglo a normas europeas o equivalentes.

e) Acreditación de no concurrencia de prohibición de contratar

- Presentación de testimonio judicial, certificación administrativa o, en caso de no ser posible, bastará declaración responsable de que no concurren prohibiciones de contratar otorgada ante Notario Público, autoridad administrativa u organismo profesional cualificado. Dicha declaración incluirá la manifestación de hallarse al corriente del cumplimiento de las obligaciones tributarias y de la Seguridad Social impuestas por las disposiciones vigentes, sin perjuicio de que la justificación acreditativa de tal requisito deba presentarse, antes de la adjudicación, por el empresario a cuyo favor se vaya a efectuar ésta.
- Cuando se trate de empresas de Estados Miembros de la Unión Europea y esta posibilidad esté prevista en la legislación del Estado respectivo,

esta declaración podrá también sustituirse por una declaración responsable otorgada ante una autoridad judicial.

La documentación relativa a la capacidad de obrar, habilitación profesional y solvencia económica así como la no concurrencia de prohibiciones de contratar que deban constar en el Registro Oficial de Licitadores y Empresas Clasificadas podrá sustituirse por certificación expedida por este último acompañada de una declaración responsable del licitador en la que manifieste que las circunstancias reflejadas en el correspondiente certificado no han experimentado variación.

De igual forma, los certificados comunitarios de clasificación, acreditarán la aptitud de los contratistas en los términos previstos en el artículo 73 de la LCSP.

3. CONTENIDO DE LAS OFERTAS:

-La presentación de la oferta supondrá la aceptación incondicionada de las presentes bases de contratación.

- Los términos de la oferta deberán mantenerse vigentes hasta el momento de la adjudicación.

- Las especificaciones técnicas incluidas en las presentes bases de licitación se entenderán como mínimas y su mejora en la oferta será valorada como tal siempre que suponga una mejora de las necesidades de STL.

-Con independencia de que el licitador pueda adjuntar a su oferta cuanta información complementaria considere de interés, para poder ser valorada, ésta deberá estar firmada y estructurada de la siguiente forma:

Propuesta técnica:

La propuesta técnica incluirá los siguientes apartados:

El proveedor propondrá una lista de vulnerabilidades a comprobar en cada categoría y el responsable técnico de STL aprobará dicha lista teniendo en cuenta la diversidad de los puntos a comprobar.

Los tipos y categorías de ataques para buscar vulnerabilidades pueden abarcar:

Técnicas de caja negra

- Obtención de información sobre servicios no publicados.
- Obtención de información sobre tráfico de información.
- Obtención de información sobre equipos conectados a la red interna de la organización.
- Conexión a servicios no publicados.
- Conexión remota a equipos de la red interna de la organización.
- Conexión remota a equipos de la red interna con acceso de administración.

- Vulnerabilidades de tipo “deface”.
- Vulnerabilidades de tipo “cross-site scripting”.
- Vulnerabilidades de tipo “spoofing”.
- Vulnerabilidades de tipo inyección de SQL.
- Vulnerabilidades de tipo inyección de código.
- Vulnerabilidades derivadas de la validación de entrada/salida.
- Vulnerabilidades derivadas de análisis de tiempos.
- Vulnerabilidades de sincronización.
- Vulnerabilidades de tipo desbordamiento de memoria.
- Vulnerabilidades basadas en secuestro de sesiones.
- Vulnerabilidades en las redes Wi-Fi (wardriving).
- Vulnerabilidades en los equipos de la red local.
- Vulnerabilidades basadas en “sniffing” de red.
- Vulnerabilidades basadas en escaladas de privilegio.
- Vulnerabilidades de registro y auditoria.
- Vulnerabilidades en la gestión de contraseñas.
- Vulnerabilidades locales.

Técnicas de caja blanca

- Ataques con conocimientos de la arquitectura de sistemas.
- Ataques con acceso a los detalles de las aplicaciones implantadas en la organización.
- Vulnerabilidades de abuso contra interfaces de programación de aplicaciones.
- Vulnerabilidades de calidad de código.
- Vulnerabilidades derivadas de la configuración del sistema.
- Vulnerabilidades de los protocolos.
- Vulnerabilidades criptográficas.
- Vulnerabilidades en la gestión de contraseñas

En el caso particular de los sitios Web de la organización la lista de vulnerabilidades deberá incluir, al menos, estudios para los siguientes diez tipos:

- Inyección
- Secuencia de Comandos en Sitios Cruzados (XSS)
- Pérdida de Autenticación y Gestión de Sesiones
- Referencias directas insegura a objetos.
- Falsificación de Peticiones en Sitios Cruzados (CSRF)
- Defectuosa Configuración de Seguridad
- Almacenamiento criptográfico inseguro.
- Fallo de Restricción de Acceso a URL
- Protección Insuficiente en la Capa de Transporte
- Redirecciones y reenvíos no validados

Quedaran fuera de alcance las vulnerabilidades relacionadas con ataques de denegación de servicio e ingeniería social.

Personal técnico a cargo de las pruebas

Las empresas concursantes propondrán un equipo de trabajo que deberá constar de personal técnico cualificado y con experiencia en proyectos de auditoría de seguridad.

Este equipo será supervisado por el responsable de STL durante toda la prestación del servicio.

El proveedor presentará en su oferta un currículum vitae de cada miembro del equipo propuesto con referencias de organizaciones públicas o privadas que hayan recibido servicios similares al propuesto en los que el equipo estuvo implicado.

Metodología

El proveedor presentará y realizará sus servicios siguiendo alguna de las metodologías habituales en el campo de las tecnologías de seguridad de redes y sistemas y del hacking ético.

Por ejemplo, para la actividad específica de verificación de seguridad de los sistemas de información podrán utilizarse las recomendaciones del Informe Especial de NIST 800-42 o las del Informe Especial del NIST 800-115, así como manuales o procedimientos y recomendaciones del SANS Institute, ISAF, ISECOM, ISACA, EC-Council, OWASP, OSSTMM e ISSAF.

Planificación

Las empresas participantes en el concurso deberán presentar una planificación de los servicios ofrecidos con el detalle de las fases, las actividades, la asignación de recursos por parte de la misma y el calendario de realización del servicio para cada uno de los lotes.

Las empresas participantes en el concurso deberán presentar un plan de para la realización de las pruebas de seguridad y un listado de todas las herramientas utilizadas durante la revisión.

En dicha planificación se hará mención a los recursos que STL debe poner a disposición del proveedor cuando esta disposición de recursos sea necesaria.

Descripción de los entregables de cada fase, cumpliendo con los requisitos mínimos marcados en este pliego.

Cualquier otra información que el oferente considere de interés.

Proposición económica

- La oferta económica incluirá el desglose de los precios por cada lote, IVA excluido, que comprenda:

Para todos los LOTES:

- Una cantidad básica por consultoría que recogerá la realización de todos los test que se van a pasar al sistema, así como la confección de los informes.

Para los lotes LOTES III y IV:

- Un esquema de incentivos dependiente de las vulnerabilidades descubiertas y su tipología. Este esquema de incentivos propondrá unas cantidades a percibir por cada ataque exitoso limitado por un valor que permita determinar un techo presupuestario para el servicio completo

- En todo caso, se entenderá incluido en el precio unitario propuesto por el licitador el coste de cualquier otro canon, tributo o similar que, en su caso, fuese de aplicación al objeto del contrato en el plazo de presentación de ofertas así como los costes de servicios suministrados.
- Los precios de las ofertas deberán estipularse en euros.
- Sistema de descuentos por la asignación de dos o mas lotes a un mismo proveedor.

4. CRITERIOS DE VALORACIÓN DE LAS OFERTAS

En cumplimiento del artículo 176 LCSP, el contrato se adjudicará a la oferta económicamente más ventajosa. Para su determinación, se atenderá a los siguientes criterios:

- Precio del servicio
- Calidad y detalle de la planificación de cada uno de los Lotes
- Experiencia del equipo en proyectos similares

La Puntuación Global de cada oferta estará compuesta por la suma de las siguientes puntuaciones, con un máximo de 100 puntos:

- Precio (Pp): 35 puntos. En el caso de los lotes III y IV se valorará el sistema de incentivos propuesto.
- Calidad (Pc): 65 puntos, de donde
 - Cumplimiento de especificaciones técnicas: 15 puntos
 - Mejoras sobre las especificaciones técnicas: 10 puntos
 - Curriculum vitae de los técnicos participantes: 20 puntos
 - Propuesta Técnica: 20 puntos

La **Puntuación Parcial sobre el Precio (Pp)** se obtiene aplicando la siguiente fórmula:

$$Pp = 35 \text{ Ofm/Ofi}$$

Donde:

- Pp es la puntuación parcial sobre el precio para cada oferta
- Ofm es la oferta más económica
- Ofi es la oferta i que siempre será superior o igual a Ofm

5. PROCEDIMIENTO DE ADJUDICACIÓN:

La adjudicación podrá ser separada por cada uno de los lotes del pliego, las empresas interesadas podrán presentar oferta a uno, a varios o la totalidad de los lotes.

El procedimiento de adjudicación se desarrollará con arreglo a las siguientes fases:

a) Publicación del procedimiento en la Web de STL:

Sin perjuicio del empleo de otros medios de publicidad que STL determine, este procedimiento se publica en el perfil del contratante de la entidad registrado en la Web de STL www.stl.es (11 de noviembre de 2011)

b) Recepción de ofertas:

Con independencia de que STL pueda requerir posteriores aclaraciones o subsanaciones sobre el contenido de las ofertas, el plazo en el que el licitador puede presentar oferta finaliza a las 12 horas del día 12 de Diciembre de 2011.

c) Selección de la empresa contratante por cada lote

Las ofertas que resulten preseleccionadas por acreditar capacidad de obrar y solvencia técnica y económica, serán objeto de valoración con arreglo a los criterios fijados en la cláusula anterior.

d) Firma del contrato

STL requerirá al licitador que haya presentado la oferta económicamente más ventajosa para que presente el certificado de estar al corriente del cumplimiento de las obligaciones tributarias y con la Seguridad Social con carácter previo a la adjudicación y firma del contrato.

STL se reserva el derecho a renunciar a la celebración del contrato en cualquier momento antes de la adjudicación, notificando la renuncia o desistimiento a través del perfil del contratante de la Sociedad.

6. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL INCLUIDOS EN LA OFERTA

En cumplimiento de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de carácter personal (LOPD) y del Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la ley mencionada, se informa de que los datos de carácter personal del representante legal y/o de las personas de contacto que se señalen en la oferta del licitador, serán tratados e incluidos en un fichero de datos de carácter personal, titularidad de STL, cuya finalidad será la gestión del procedimiento de licitación en curso y, en su caso, de la ejecución del contrato, incluyendo: llevar a cabo la apertura de las ofertas presentadas, su valoración de conformidad con el contenido de las presentes bases de contratación,, solicitar cuanta documentación adicional resulte necesaria, atender sus solicitudes de información, comunicarle el acuerdo del Órgano de Contratación relativo a la adjudicación, proceder en su caso a la devolución de la documentación administrativa aportada y del resguardo de la fianza provisional así como para remitir cualquier otra documentación necesaria al respecto y mantenimiento de históricos.

Asimismo, STL informa que de conformidad con la legislación vigente, STL deberá comunicar la información y datos obrantes en el expediente de contratación a los siguientes Organismos y terceros: Jueces y Tribunales, en su caso, cuando fuera requerido legalmente para ello, Junta Consultiva de Contratación del Ministerio de Economía y Hacienda, Intervención General de la Administración del Estado (IGAE) para realización de las auditorias de cuentas correspondientes y en general, el Tribunal de Cuentas, auditores y a cualesquiera otros terceros a quienes, en virtud de la normativa vigente STL tuviese la obligación de comunicar los datos. Igualmente, en el caso en que STL debiera proceder a la publicación de la adjudicación de la contratación en el Boletín Oficial del Estado y en el Diario Oficial de las Comunidades Europeas, los datos personales obrantes en la documentación serán publicados con el mismo alcance. El interesado consiente expresamente el citado tratamiento mediante la entrega a STL de toda aquella documentación en que el interesado haga constar sus datos personales.

En el caso de que en la oferta de los licitadores se incluyan datos de carácter personal de otras personas (bien personas integrantes de la entidad oferentes, bien de otras empresas que forman parte de la oferta presentada), la empresa oferente deberá informar a todas ellas del tratamiento de sus datos personales y recoger su consentimiento para el tratamiento cuando sea necesario de acuerdo con los términos recogidos en la presente cláusula, exonerando de toda responsabilidad a STL.

En consecuencia la cesión de datos personales de terceros a STL, queda condicionada al principio de legitimidad, necesidad y proporcionalidad y a la comunicación de datos pertinentes, no excesivos, actuales y veraces, y requiere con carácter previo que la empresa oferente proceda a informar del contenido del tratamiento según lo expuesto en la presente cláusula y a solicitar el consentimiento a dichos terceros cuando sea necesario de acuerdo con la normativa vigente. Cuando los datos cedidos por la empresa oferente a STL resultaran ser inexactos, en todo o en parte, o incompletos, la empresa oferente deberá cancelarlos y sustituirlos de oficio por los correspondientes datos

rectificados o completados en el plazo de diez días desde que se tuviese conocimiento de la inexactitud -salvo que la legislación aplicable al fichero establezca un procedimiento o un plazo específico para ello- y comunicar en el mismo plazo a STL, la rectificación o cancelación efectuada.

A los efectos antedichos, la empresa oferente deberá conservar los documentos que garanticen las obligaciones establecidas en los apartados anteriores respecto de los interesados de quienes aporte datos personales y quedará obligada a entregar una copia de los mismos a STL si esta última los requiriese.

Asimismo, de acuerdo con lo establecido en el Real Decreto 1720/2007, la entrega por parte del interesado a STL de cualquier documentación que contenga datos de carácter personal deberá garantizar la adopción de las medidas de seguridad pertinentes de acuerdo con el Título VIII del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, y en particular, se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte y comunicación a STL.

STL, como responsable del fichero, garantiza el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos personales facilitados a estos efectos dirigiéndose por escrito, con copia de su DNI a la siguiente dirección: C/ Manuel Tovar, 9, Madrid. Asimismo, en la utilización de los datos personales incluidos en el fichero, STL, se compromete a respetar su confidencialidad y a utilizarlos únicamente de acuerdo con la finalidad especificada anteriormente.



SISTEMAS TÉCNICOS DE
LOTERÍAS DEL ESTADO

7. CONTACTO

Para cualquier consulta concerniente a la descripción del alcance de los servicios, se pone a disposición de los licitadores la siguiente dirección postal y/o correo electrónico:

Nombre:	ROBERTO GONZÁLEZ MÁRQUEZ
Teléfono:	91 348 92 00
Fax:	91 348 92 12
Correo electrónico	roberto.gonzalez@stl.es
Dirección:	C/ Manuel Tovar 9, 28034 Madrid

Para cualquier consulta concerniente al plazo o presentación de las ofertas, se pone a disposición de los licitadores el siguiente contacto:

Nombre:	JOSÉ MANUEL HOMBRE BAENA.
Teléfono:	91 348 91 27
Fax:	91 348 92 12
Correo electrónico	jose.hombre@stl.es
Dirección:	C/ Manuel Tovar 9, 28034 Madrid

Se anima a los licitadores a utilizar preferentemente el correo electrónico como canal de comunicación para dudas tanto de tipo técnico como administrativo.

SECCIÓN III: EJECUCIÓN DEL CONTRATO

1. OBLIGACIONES DE LOS CONTRATISTAS

1.1. Obligaciones del adjudicatario:

Son obligaciones del adjudicatario las siguientes:

- Llevar a cabo el diseño del plan de pruebas. Dicho plan incluirá necesariamente el siguiente detalle:
 - o Actividades a realizar.
 - o Calendario con desglose de las fases.
 - o Lista de vulnerabilidades a comprobar en cada categoría.
 - o Asignación de recursos para cada actividad incluyendo expresamente el listado de todas las herramientas que se utilizarán durante la revisión y test.

- Recursos que STL debe poner a disposición del proveedor cuando esta disposición de recursos sea necesaria.
 - Descripción de los entregables de cada fase, cumpliendo con los requisitos mínimos marcados en este pliego.
 - Cualquier otra información que el oferente considere de interés.
- Además será obligación de los adjudicatarios de los Lotes III y IV la realización de un esquema de incentivos dependiente de las vulnerabilidades descubiertas y su tipología. Este esquema de incentivos propondrá unas cantidades a percibir por cada ataque exitoso limitado por un valor que permita determinar un techo presupuestario para el servicio completo.
 - Llevar a cabo la ejecución del plan de acuerdo al plan de pruebas, especificaciones técnicas y calendario de entregas acordado entre ambas partes.
 - Prestar sus servicios siguiendo alguna de las metodologías habituales en el campo de las tecnologías de seguridad de redes y sistemas y del hacking ético.
 - Solicitar autorización previa y por escrito a STL para la realización de servicios consistentes en ataques que puedan implicar una posible parada de servicio y/o pruebas en la que exista un riesgo significativo de pérdida de servicio.
 - Solicitar autorización previa y por escrito a STL para la utilización de cualquier herramienta no incluida en la oferta.
 - Elaborar y proporcionar a STL toda la documentación, informes y entregables derivados de la ejecución del presente pliego y en particular los descritos en el apartado “2.2 Entregables del Servicio” de la Sección IV “Especificaciones Técnicas” del presente Pliego en idioma español en formato papel y digital (PGP).
 - Centralizar y coordinar las actividades de interlocución.
 - Llevar a cabo el seguimiento y monitorización de las distintas fases y tareas así como asistir a todas las reuniones que STL considere conveniente.
 - Asignar a la ejecución de las prestaciones objeto del presente pliego personal cualificado y con conocimientos en la materia con los niveles y perfiles técnicos acordados entre las partes. A tales efectos, el adjudicatario deberá proponer un equipo de trabajo con personal técnico cualificado y con experiencia en proyectos de auditoría de seguridad. Dicha propuesta incluirá un currículum vitae de cada miembro del equipo propuesto con referencias de organizaciones públicas o privadas que hayan recibido servicios similares al propuesto en los que el equipo estuvo implicado. En caso de que sea necesario sustituir a algún miembro del equipo, el adjudicatario se compromete a seleccionar otra persona del mismo nivel, perfil y cualificación técnica.

- Informar inmediatamente de cualquier riesgo grave detectado durante la ejecución del servicio y que pudiera afectar a la integridad disponibilidad y confidencialidad de los sistemas de STL incluidos en el plan de pruebas.

1.2. Entregas, plazos y penalizaciones:

La prestación de los servicios objeto del presente Pliego deberá realizarse de acuerdo en los plazos y fechas acordados por las partes.

Se considerarán prestados los servicios de cada lote cuando el proveedor proporcione todos los informes y documentación que forman parte de la prestación y en particular el informe final de resultados de acuerdo con los requisitos contenidos en este pliego y pactados entre las partes. A tales efectos:

- En el caso de los lotes I y II existirán 4 entregas, una por cada prueba trimestral.
- En el caso de los lotes III, IV y V, existirá una entrega de acuerdo con el calendario pactado entre las partes dentro del plazo máximo de ejecución del contrato..

Una vez concluidos los trabajos correspondientes a una entrega de un lote, el responsable de STL comprobará que los entregables cumplen con los requisitos marcados en este pliego y STL emitirá, en el plazo de 15 días naturales, el correspondiente certificado de aceptación o rechazo, que será notificado al contratista por correo electrónico o por cualquier medio que permita dejar constancia de dicha notificación.

En caso de rechazo, el adjudicatario se obliga a realizar cuantas actuaciones resulten necesarias, a las especificaciones pactadas en un plazo máximo de 30 días naturales, sin que ello suponga un coste adicional para STL.

La emisión del certificado de aceptación por STL facultará al adjudicatario para facturar el 100% del importe ofertado en el caso de los lotes III, IV y V. Para los lotes I y II la emisión del certificado de aceptación correspondiente a ese trimestre facultará al adjudicatario a facturar el 25% del importe total del lote.

Los plazos de entrega tienen carácter esencial. Su incumplimiento podrá dar lugar a las penalizaciones previstas en la cláusula "Penalizaciones" de las presentes bases de contratación. En el caso de que la demora en la entrega de los informes correspondientes a cada lote exceda de 30 días naturales el plazo previsto, STL se reserva el derecho a resolver el contrato con la correspondiente indemnización de daños y perjuicios.

2. PRECIO Y CONDICIONES DE PAGO

El adjudicatario tendrá derecho al abono del precio pactado previa presentación de factura en la que deberá de constar el número de pedido que le proporcionará STL con la suficiente antelación.

El plazo de pago será de treinta días a partir del día en que se emita el certificado de aceptación de los informes con arreglo a lo previsto en el contrato. Para que STL pueda cumplir con dicha obligación, el proveedor deberá hacerle llegar la factura antes de que se cumplan treinta días desde la fecha de aceptación de cada entregable. El pago se efectuará mediante la oportuna transferencia a la cuenta corriente que el adjudicatario designe.

3. PENALIZACIONES

En virtud de la presente cláusula, que tiene carácter cumulativo y no sustitutivo a los efectos de lo dispuesto en el artículo 1.152 CC, cuando se produzca una demora en el cumplimiento de los plazos de entrega acordados superior a 15 días naturales STL podrá aplicar una penalización del 2 % del importe de facturación por cada día natural de retraso sobre el plazo de entrega establecido en su oferta.

Las penalizaciones indicadas en los párrafos anteriores se establecen para todos los lotes y podrán ser descontadas de las facturas pendientes de pago. El pago de las penas pecuniarias anteriormente previstas no sustituirá al resarcimiento de daños y perjuicios por incumplimiento del adjudicatario, ni le eximirá de cumplir con sus obligaciones contractuales, pudiendo STL exigir conjuntamente el cumplimiento de dichas obligaciones y la satisfacción de las penas pecuniarias establecidas.

5. PROPIEDAD INTELECTUAL DE LA DOCUMENTACIÓN Y ENTREGABLES DERIVADOS DE LA PRESTACIÓN DE LOS SERVICIOS

El adjudicatario expresamente acepta y reconoce que todos los derechos de propiedad intelectual derivados de los trabajos realizados por el adjudicatario para STL en relación con los servicios objeto del presente Pliego (en adelante también obras resultantes de los trabajos realizados) corresponderán única y exclusivamente a STL.

A tales efectos se entenderá por obras resultantes de los trabajos realizados -a título orientativo y sin carácter limitativo- los entregables descritos en el apartado "2.2 Entregables del Servicio" de la Sección IV "Especificaciones Técnicas" del presente Pliego, el plan de pruebas con todos sus contenidos, test, informes de resultado, informes de evaluación, registros de auditoría y cualquier documentación auxiliar; know how; elementos de diseño tales como imágenes, gráficos, vídeos o fotografías; así como cualesquiera otros documentos que se deriven de la prestación de servicios objeto de este pliego. Tendrán igualmente la consideración de obras resultantes de los trabajos realizados, aquellas elaboradas o derivadas de las anteriores.

La titularidad de derechos de propiedad intelectual sobre las obras resultantes atribuirá a STL la plena disposición y el derecho exclusivo a la explotación de las mismas con exclusión de cualesquiera personas físicas y/o jurídicas, incluido el adjudicatario.

En concreto, corresponderán a STL, sin carácter limitativo, los derechos de reproducción total o parcial de las obras resultantes; de traducción, adaptación, arreglo o cualquier otra transformación o modificación de las obras, ya produzcan como resultado versiones sucesivas u obras derivadas, así como la reproducción del resultado de tales transformaciones, que podrán ser realizadas directamente por STL o bien por terceros autorizados por ésta en cuanto titular exclusivo del derecho; cualquier forma de distribución o comercialización de las obras y su comunicación pública; siendo STL quien, si así lo decidiera, editará y divulgará las obras bajo su propio nombre.

En consecuencia, el adjudicatario deberá entregar a STL todas las obras resultantes de los trabajos tanto en soporte papel como en soporte electrónico y/o cualesquiera otros soportes en que se contengan las obras resultantes.

El adjudicatario no podrá hacer uso en otros proyectos de la documentación y obras resultantes de los trabajos realizados, si no es por autorización expresa y por escrito de STL.

La cesión de derechos tanto de propiedad intelectual contemplada en la presente cláusula se entenderá efectuada en los más amplios términos, con la máxima duración legalmente permitida hasta el paso a dominio público de los derechos y para un ámbito territorial mundial. El adjudicatario manifiesta expresamente que se encuentra debidamente legitimado para realizar dicha cesión, y que mantendrá indemne a STL por el incumplimiento de dicha garantía.

El adjudicatario garantiza el cumplimiento de la normativa sobre propiedad intelectual manifiesta que se encuentra debidamente legitimado para la ejecución del objeto del presente pliego y cesión de la propiedad de los soportes en que se encuentren las obras resultantes así como la propiedad intelectual de éstas y no vulnera ninguna previsión legal en materia de propiedad intelectual, contrato, derecho o propiedad de terceros manteniendo indemne a STL de cuantas consecuencias se deriven del incumplimiento de dicha garantía y exonerando a STL de cualquier tipo de responsabilidad frente a terceros que pudiera derivarse por el incumplimiento de dicha garantía.

A tales efectos, el adjudicatario responderá ante STL del ejercicio pacífico de los derechos de propiedad contemplados en esta cláusula, comprometiéndose a no contraer sobre tales derechos compromisos o gravámenes de ninguna especie que atenten contra los derechos que a STL o a terceros les correspondan. Al respecto, el adjudicatario será responsable frente a STL de todas las cargas pecuniarias que pudieran derivarse para STL a favor de terceros con motivo de acciones, reclamaciones o conflictos derivados del incumplimiento de lo señalado en esta cláusula por parte del adjudicatario.

Asimismo y a efectos de la garantía otorgada en los apartados anteriores, el adjudicatario declara tener las autorizaciones que en su caso correspondan al objeto de no incurrir en vulneración alguna respecto de los derechos de propiedad intelectual para permitir el goce de los derechos a STL en los términos reseñados en esta cláusula así como a cualesquiera otros derechos reconocidos por la Ley, obligándose a presentar a STL cuanta documentación le

sea requerida por ésta a fin de probar la existencia de las autorizaciones que en cada caso resulten pertinentes.

En particular, el adjudicatario garantizará y se comprometerá a realizar cuantas declaraciones y actos sean necesarios tanto mediante fe pública notarial como con carácter privado ante el Registro de la Propiedad Intelectual para acreditar que STL es el legítimo titular de las obras resultantes (originales y/o derivadas) desarrolladas por el adjudicatario en ejecución de los trabajos objeto del presente pliego y en particular a poner a disposición de STL cualesquiera declaraciones de los empleados que intervengan en el desarrollo de las obras resultantes por STL con el fin de garantizar la legitimidad de la cesión que el adjudicatario realiza a STL así como la titularidad de STL de los derechos sobre las mismas.

Remuneración

El precio o remuneración por la cesión de derechos de propiedad intelectual contemplada en esta cláusula se entiende pagado a tanto alzado en el precio total de la prestación de los servicios objeto de contratación.

Idioma y formato

El idioma utilizado para la elaboración de los entregables será el español. Todos los entregables que formen parte del resultado de los trabajos objeto de este pliego tendrán que estar identificados al menos por un título. Asimismo de cada entregable se entregará a STL duplicado del mismo en formato papel y digital (PGP).

6. PROPIEDAD INDUSTRIAL

El adjudicatario no podrá hacer uso del nombre, logotipo o cualquier signo distintivo o material que le haya facilitado STL para el cumplimiento de las obligaciones derivadas de la ejecución de los trabajos objeto del presente pliego y en su caso el contrato que las partes suscriban, fuera de las circunstancias y fines del objeto de ambos documentos, ni una vez terminada la vigencia del mismo.

Asimismo el adjudicatario garantiza el cumplimiento de la normativa sobre propiedad industrial y manifiesta que se encuentra debidamente legitimado para la ejecución del objeto del presente pliego y cesión de la propiedad y derechos de uso del nombre, logotipo o cualquier signo distintivo o material o productos objeto del mismo, y no vulnera ninguna previsión legal en materia de propiedad industrial, contrato, derecho o propiedad de terceros manteniendo indemne a STL de cuantas consecuencias se deriven del incumplimiento de dicha garantía y exonerando a STL de cualquier tipo de responsabilidad frente a terceros que pudiera derivarse por el incumplimiento de dicha garantía.

La cesión de cualesquiera derechos de propiedad industrial que en su caso sea necesario para la ejecución de los trabajos objeto del presente pliego se realizará por el adjudicatario con carácter no exclusivo, transferible, a perpetuidad hasta su paso a dominio público y sin limitación territorial alguna.

El adjudicatario manifiesta que se encuentra debidamente legitimado para garantizar la cesión de derechos de propiedad industrial otorgada en el apartado anterior y que no vulnera ninguna previsión legal, contrato, derecho o propiedad de terceros ni, en modo alguno, constituye competencia desleal, manteniendo indemne a STL de cuantas consecuencias se deriven del incumplimiento de dicha garantía.

7. AUTORIZACIONES Y LICENCIAS DE LAS HERRAMIENTAS UTILIZADAS PARA LA PRESTACIÓN DE LOS SERVICIOS Y DESARROLLO DE LOS TRABAJOS

En el caso en que el adjudicatario utilice para el desarrollo de los trabajos objeto de este pliego respecto de la realización de las pruebas de seguridad, herramientas comerciales de terceros, queda obligado a poner a disposición de STL los términos y condiciones de las licencias de cesión de derechos de propiedad intelectual e industrial y documentación asociada al efecto, antes de la formalización del contrato y a más tardar, en el mismo momento de su firma.

En caso en que tras la entrega por el adjudicatario a STL de las licencias y documentación asociada respecto de la cesión de derechos de propiedad intelectual e industrial, STL constatare que los términos no garantizan la disponibilidad de las herramientas para la ejecución de los servicios objeto del presente Pliego, el adjudicatario quedará obligado a obtener las licencias y autorizaciones precisas al efecto y a entregarlas a STL de forma que en caso contrario STL quedará facultada para resolver unilateralmente el contrato en cualquier fase de su ejecución por incumplimiento del adjudicatario, así como para exigir la responsabilidad por daños y perjuicios que en su caso corresponda.

8. TRANSFERENCIA DE TECNOLOGÍA

El adjudicatario guardará el debido secreto empresarial acerca de todo el know how o saber hacer resultante de la ejecución de los servicios que sean contratados por STL de acuerdo con lo previsto en el presente pliego, manteniendo dicha información en reserva y secreto por el adjudicatario y no siendo revelada de ninguna forma, en todo o en parte, a ninguna persona física o jurídica que no sea parte del contrato.

Sin carácter limitativo y a los efectos del presente pliego se entenderá por know how o saber hacer todos los aspectos derivados de la ejecución de las prestaciones del presente pliego relacionados con conocimientos útiles que permiten la satisfacción de necesidades de STL; que permiten a STL tener ventajas competitivas en el mercado y que tienen carácter industrial, tecnológico y/o comercial. En particular, cualesquiera aspectos relacionados con las prestaciones del presente pliego sobre desarrollo o perfeccionamiento tecnológico ya patentado o susceptible de serlo, valoraciones sobre la viabilidad técnica y comercial de las prestaciones del presente pliego, aspectos relacionados con la explotación del proyecto contratado en alguna de sus formas, antecedentes del proyecto, test, vulnerabilidades, informes de

resultados y evaluaciones, los conocimientos adquiridos en particular para la utilidad, aplicación y satisfacción de las necesidades de STL, en virtud de la experiencia de dicha entidad o la prestación de servicios para dicha entidad, y cuantos datos de tipo técnico y comercial tenga a su disposición el adjudicatario relativos a la ejecución de las prestaciones del presente pliego, incluyendo en particular todos los conocimientos (de productos o procedimientos) que pueden proporcionar una ventaja competitiva a STL en la competencia económica, abarcando tanto los conocimientos tecnológicos como los industriales y los comerciales.

El adjudicatario facilitará a STL toda la documentación disponible relativa a los antecedentes de los servicios prestados, datos, conocimientos y metodologías de tipo tanto técnico como comercial que tenga a su disposición y en definitiva, la transferencia del know how empleado en la realización de las prestaciones del presente pliego. Dicha entrega a STL se realizará a la ejecución total del proyecto, y se materializará en la entrega de todos los documentos relacionados con el proyecto y servicios prestados:

El adjudicatario acepta que el precio establecido en el presente pliego por la prestación de servicios incluye cualquier autorización o cesión para la explotación en exclusiva por STL del know how empleado y cualesquiera conocimientos sistemáticos y metodologías surgidos a partir del desarrollo de los servicios contratados, incluyendo la transferencia de tecnología necesaria para la satisfacción o consecución de los fines y objetivos propuestos en el presente pliego con relación al proyecto, así como la cesión en exclusiva de cualesquiera secretos empresariales a STL conocidos, obtenidos y/o derivados de la ejecución de los servicios realizados por el adjudicatario, al amparo del presente contrato.

9. PERSONAL

Todas las personas físicas o jurídicas que presten sus servicios a la empresa adjudicataria estarán vinculadas exclusivamente con ella, sin que STL ostente ninguna responsabilidad, directa o subsidiaria, que se derive de las mencionadas relaciones laborales, civiles y/o mercantiles, comprometiéndose la empresa adjudicataria a cumplir íntegramente la legislación vigente en materia de seguros, Seguridad Social, Seguridad e Higiene en el Trabajo, Laboral en general y Fiscal.

A los efectos previstos en la vigente Ley del Estatuto de los Trabajadores, la empresa adjudicataria declara que mantiene a todos sus trabajadores en alta en la Seguridad Social y que está al corriente de pago de las cuotas de Seguridad Social, asumiendo cualquier responsabilidad que se pueda derivar en materia de Seguridad Social o de infracción laboral. La empresa adjudicataria se compromete a entregar a STL acreditación de los extremos anteriores a la firma del contrato y con periodicidad cuatrimestral.

El contrato que se formalice entre STL y la empresa adjudicataria no establecerá ninguna relación laboral entre STL y los trabajadores de la empresa

adjudicataria o aquellas personas que ésta contrate para llevar a término el objeto del contrato.

La empresa adjudicataria garantiza la más absoluta indemnidad frente a STL por cualquier responsabilidad que pudiera derivarse de las relaciones con su personal y, en su caso, con el personal subcontratado. No obstante, si por incumplimiento de estos compromisos se derivara alguna responsabilidad para STL, el adjudicatario responderá por dichas responsabilidades, incluidos cualesquiera gastos y/o costas judiciales que ocasionare la defensa de STL.

El personal de la empresa contratante que eventualmente se desplace a las dependencias de STL se someterá a las normas de seguridad en el trabajo y de prevención de riesgos laborales establecidas por este último. STL quedará exonerado de cualquier responsabilidad sobre el personal de la empresa contratante en materia de riesgos laborales por la inobservancia por parte de dicho personal de las normas de seguridad en el trabajo y de prevención de riesgos laborales establecidas por STL para sus propias dependencias.

La adjudicataria se obliga a informar al personal que forme parte del proyecto del contenido del tratamiento de sus datos personales de conformidad con lo establecido en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal así como a entregar a dicho personal el texto informativo en materia de protección de datos que en su caso sea proporcionado por STL en cumplimiento del artículo 5. La adjudicataria queda obligada a devolver a STL el original de dicha comunicación firmada por los trabajadores a fin de acreditar la recepción del texto informativo y cumplimiento del deber de información por STL a éstos.

10. CONFIDENCIALIDAD DE LA INFORMACIÓN

El adjudicatario vendrá obligado a guardar la más estricta confidencialidad sobre el contenido del contrato que las partes suscriban, así como los datos o información de cualquier naturaleza a la que pueda tener acceso o generar como consecuencia de la ejecución del mismo, pudiendo únicamente poner en conocimiento de terceros aquellos extremos que la STL autorice por escrito y a usar dicha información a los exclusivos fines de la ejecución de los trabajos objeto del pliego.

En particular, toda la información obtenida durante las pruebas de seguridad de cualquiera de los lotes permanecerá en todo momento en propiedad de STL y además de ser tratada como altamente confidencial por el adjudicatario, cualquier registro electrónico relacionado con las pruebas de seguridad deberá ser conservado y permanecer protegido mediante técnicas de encriptación.

Tendrá la consideración de “Información Confidencial” sin que esta enumeración tenga carácter limitativo, la existencia misma del contrato que suscriban las partes, todo su contenido, los resultados y objetivos perseguidos en su ejecución, test, informes de resultado, evaluación y/o de cualquier otra naturaleza, cualquier registro electrónico o no relacionado con las pruebas de seguridad así como toda aquella información relativa a secretos comerciales,

documentos, acuerdos, datos, software y cualquier otra información referida a aspectos técnicos, comerciales, financieros o cualesquiera otros relativos a STL, SELAE, la Red de ventas y las actividades de todas ellas. El compromiso que adquiere el adjudicatario de respetar lo descrito como Información Confidencial, permanecerá vigente incluso finalizada la ejecución del contrato que suscriban las partes sin límite temporal.

El adjudicatario asume la responsabilidad de comunicar el presente acuerdo de confidencialidad a todos sus empleados y colaboradores eventuales.

El adjudicatario se compromete a admitir cualquier tipo de control y auditoria que STL desee realizar durante el tiempo en que obren en su poder los datos, informaciones, documentos, ficheros o programas titularidad de STL, para comprobar el cumplimiento por parte del adjudicatario de las obligaciones y compromisos asumidos en el presente documento.

La empresa adjudicataria no podrá durante la vigencia del contrato o en cualquier momento después de su resolución (independientemente de su causa), directa o indirectamente, hacer uso, divulgar, comunicar a cualquier persona, firma, sociedad u organización cualquiera de la Información Confidencial que hubiera llegado a estar en su posesión.

Asimismo, no podrá durante la vigencia del contrato o en cualquier momento después de su resolución (independientemente de su causa), copiar o reproducir en cualquier modo o mediante cualesquier otro medio, documentación, CD-Rom, cintas o cualquier otro material que contuviese Información Confidencial.

La adjudicataria igualmente deberá informar a su personal sobre este punto.

A la finalización del contrato el adjudicatario quedará obligado a la entrega a STL de todos los entregables derivados de la ejecución de los servicios objeto del presente Pliego, incluidos registros de auditoría y a la destrucción de cualquier información obtenida o generada como consecuencia de la prestación de los servicios objeto del presente Pliego que pudiera estar en posesión del adjudicatario, incluidos los registros y pistas de auditoría.

El deber de confidencialidad contemplado en esta cláusula únicamente desaparecerá en aquellos supuestos en los siguientes supuestos:

- Que resulte accesible al público u obre ya en poder de terceros por causa distinta del incumplimiento de la obligación de confidencialidad por una del adjudicatario;
- Que sea necesaria para exigir o permitir el cumplimiento de los derechos u obligaciones derivados del pliego o el contrato que las partes suscriban o para información de los asesores o auditores del adjudicatario, siempre y cuando ambos se comprometan a mantenerlo con carácter confidencial mediante pacto expreso o de acuerdo con sus normas profesionales; o

- Cuya revelación responda al cumplimiento de una obligación legal o de una orden de naturaleza judicial o administrativa y siempre que el adjudicatario hubiera recibido la orden correspondiente informe de ello previamente por escrito a STL.

11. CONFIDENCIALIDAD Y SEGURIDAD DE LOS DATOS DE CARÁCTER PERSONAL

El adjudicatario queda obligado a garantizar y dar cumplimiento a las obligaciones de confidencialidad y seguridad derivadas de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (en adelante LOPD) y el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la LOPD (en adelante RDLOPD).

A tales efectos, respecto de las prestaciones objeto del pliego que no requieran del acceso a datos de carácter personal por parte del adjudicatario, en cumplimiento del artículo 83 del RDLOPD, el adjudicatario queda obligado a garantizar y acreditar que el personal a su cargo ha sido suficientemente instruido sobre la prohibición de acceder a los datos de carácter personal de los que STL y/o SELAE sean responsables, y la obligación de secreto respecto a los datos que dicho personal hubiera podido conocer con motivo de la ejecución de los servicios objeto del presente pliego.

Por el contrario, en la medida en que las prestaciones y el cumplimiento del objeto del presente pliego impliquen un acceso del adjudicatario a datos de carácter personal, el tratamiento de dichos datos por parte del adjudicatario deberá realizarse en la forma y condiciones siguientes:

- El acceso del adjudicatario a los datos del fichero para la prestación del servicio no tendrá la consideración legal de comunicación o cesión de datos a los efectos de lo previsto en la LOPD, sino de acceso por cuenta de tercero según lo previsto en el artículo 12 de la citada Ley Orgánica.
- Los datos del fichero serán propiedad y responsabilidad exclusiva de STL y/o de SELAE, extendiéndose esta titularidad a cuantas elaboraciones realice el adjudicatario con ocasión del cumplimiento del contrato.
- A los efectos de la prestación del servicio por parte del adjudicatario a STL, el primero tendrá la condición de encargado del tratamiento y se sujetará al deber de confidencialidad y seguridad de los datos personales a los que tenga acceso conforme a lo previsto en la normativa que resulte aplicable, obligándose específicamente a lo siguiente:
 - o A utilizar y aplicar los datos personales a los exclusivos fines de cumplimiento del objeto del presente pliego.
 - o A adoptar las medidas de índole técnica y organizativa necesarias establecidas en el artículo 9 de la LOPD y en las normas reglamentarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento o acceso no

autorizado habida cuenta del estado de la tecnología, la naturaleza de los datos objeto de tratamiento y los riesgos a que los mismos estén expuestos, ya provengan de la acción humana o del medio físico o natural. En todo caso se obliga a aplicar las medidas de seguridad del nivel que correspondan en función de los datos a tratar de conformidad con lo previsto en el título VIII del RDLOPD.

- A mantener la más absoluta confidencialidad sobre los datos personales a los que tenga acceso para la prestación de servicios así como sobre los que resulten de su tratamiento cualquiera que sea el soporte en el que se hubieren obtenido.
- A no comunicar o ceder los datos contenidos en el/os ficheros a otras personas, ni siquiera para su conservación, debiendo destruir los datos personales a los que haya tenido acceso, así como los resultados derivados de su tratamiento, al igual que cualquier soporte o documentos en los que conste algún dato de carácter personal objeto de tratamiento, salvo que STL y/o SELAE requieran su devolución.
- A guardar deber de secreto de todos los datos de carácter personal que el adjudicatario conozca o a los que tenga acceso en ejecución del contrato.
- Igualmente se obliga a custodiar e impedir el acceso a los datos de carácter personal a cualquier tercero ajeno. Las anteriores obligaciones se extienden a toda persona que pudiera intervenir en cualquier fase del tratamiento por cuenta del adjudicatario.
- A comunicar y hacer cumplir a sus empleados las obligaciones establecidas en los apartados anteriores y, en particular, las relativas al deber de secreto y medidas de seguridad. El adjudicatario se comprometerá a comunicar a STL, de forma inmediata, cualquier fallo en su sistema de tratamiento y gestión de la información que haya tenido o pueda tener como consecuencia de la puesta en conocimiento de terceros de información confidencial obtenida durante la ejecución del contrato.

- Sin perjuicio de lo anterior, en todo caso y en la medida en que los servicios objeto de adjudicación impliquen un acceso y/o tratamiento de datos de carácter personal, el adjudicatario queda obligado a formalizar el contrato de acceso a datos a que se refiere el artículo 12 de la LOPD y concordantes de su reglamento de desarrollo en el que se recogerán todas las obligaciones al respecto.

En caso de que el adjudicatario precise subcontratar con terceros la realización de los servicios adjudicados en los términos indicados anteriormente, lo pondrá en conocimiento de STL así como los datos que identifiquen a la empresa antes

de proceder a la subcontratación. En tal caso, STL autorizará la subcontratación siempre que se cumplan las siguientes condiciones:

- Que el tratamiento de datos de carácter personal por parte del subcontratista se ajuste a las instrucciones vertidas por STL.
- Que el adjudicatario y la empresa subcontratista formalicen un contrato de seguridad y confidencialidad para el acceso y/o tratamiento de datos de carácter personal en los términos previstos en el artículo 12 de la LOPD y concordantes del RDLOPD; contrato que será puesto a disposición de STL a su solicitud para verificar su existencia y contenido. En este caso, el subcontratista será considerado encargado del tratamiento a los efectos previstos en la legislación vigente en materia de protección de datos de carácter personal, siéndole de aplicación lo previsto en el artículo 20.3 del RDLOPD.

El adjudicatario se compromete a admitir cualquier tipo de control y auditoria que STL desee realizar durante el tiempo en que obren en su poder los datos personales y/o sistemas de información que los contengan, para comprobar el cumplimiento por parte del adjudicatario de las obligaciones y compromisos asumidos en el presente documento.

12. SUBCONTRATACIÓN

El adjudicatario no podrá subcontratar las prestaciones objeto del contrato sin la previa autorización escrita de STL. En caso de que se formalice la referida autorización, el subcontratista quedará obligado sólo ante el contratista principal que asumirá, por tanto, la total responsabilidad de la ejecución del contrato frente a STL.

13. CESIÓN DEL CONTRATO

Ninguna de las Partes podrá ceder ni transmitir los derechos y obligaciones derivados del presente Contrato sin el previo consentimiento por escrito de la otra. No obstante, no será necesario dicho consentimiento en caso de fusión, escisión, segregación o cualquier otra reorganización societaria de STL o cuando ésta última realice la cesión a favor de una entidad del mismo grupo, entendiéndose por tal lo previsto en el artículo 42 del Código de Comercio.

En los supuestos de sucesión del contratista se estará a lo previsto en el artículo 73 bis de la Ley 30/2007, de 30 de octubre, de Contratos del Sector Público.

14. RESOLUCIÓN

STL tendrá derecho a resolver de forma unilateral el contrato en caso de incumplimiento grave de las obligaciones asumidas por el adjudicatario. A estos efectos, tendrán en todo caso la consideración de incumplimiento grave del adjudicatario las siguientes causas:

- La demora en la entrega de los informes de más de 30 días naturales prevista en la cláusula primera de la presente Sección.
- 3 rechazos consecutivos de los informes objeto del presente contrato.
- La falta de entrega a STL de las licencias y autorizaciones necesarias que legitimen uso de herramientas comerciales para la prestación de los servicios objeto del presente Pliego.
- La falsedad de las manifestaciones efectuadas en el contrato.
- La subcontratación o la cesión del contrato sin autorización de STL.

No obstante, pese a la extinción del Contrato, seguirán en vigor respecto a los efectos particulares previstos en ellas, los preceptos relativos a Propiedad intelectual, Confidencialidad y Protección de datos.



SECCIÓN IV: ESPECIFICACIONES TÉCNICAS

1. ALCANCE

El proveedor someterá a los sistemas de información de STL abarcados por este concurso a diversos tipos de ataque para comprobar la resistencia de las medidas de seguridad implantadas en la organización ante vulnerabilidades que afecten a la confidencialidad, disponibilidad e integridad de la información.

Las pruebas irán fundamentalmente encaminadas a buscar debilidades en el control de acceso, autenticación, diseño y o programación en la configuración y despliegue de los sistemas.

La ejecución de los servicios objeto de este procedimiento tendrá una duración de un año (1) máximo para los lotes I y II y de cuatro (4) semanas para los lotes III, IV y V. Todos los plazos comenzarán a contar desde la firma del contrato y abarcará los siguientes lotes de servicios y periodicidades:

- LOTE I: Cuatro pruebas, una por trimestre, de escáner de vulnerabilidades externas sobre dos direcciones IP, que permita probar el cumplimiento PCI-DSS.
- LOTE II: Cuatro pruebas, una por trimestre, de escáner de vulnerabilidades interno para un entorno bajo normativa PCI-DSS constituido por un grupo de veintinueve dispositivos de equipos de comunicaciones y servidores.
- LOTE III: Una prueba de intrusión interna para un entorno bajo normativa PCI-DSS constituido por un grupo de veintinueve dispositivos formado por equipos de comunicaciones, y servidores.
- LOTE IV: Una prueba de intrusión externa sobre el conjunto de servicios que ofrece la organización en un rango aproximado de 75 direcciones IP públicas, dos de las cuales están bajo normativa PCI-DSS
- LOTE V: Prueba de intrusión interna sobre entorno aislado, tres equipos, una red y dos firewall con aproximadamente veinte reglas y veintiséis reglas NAT

2. REQUISITOS

2.1. REALIZACIÓN DE SERVICIO

De carácter general para todos los lotes I, II, III, IV:

- Las herramientas comerciales empleadas para la realización de las pruebas de seguridad deberán incluir sus licencias, las mismas podrán ser solicitadas por el responsable de STL.

- Todos los Lotes se realizaran en las dependencias de STL incluido el LOTE IV haciendo uso de tecnologías ADSL proporcionadas por STL o tecnología 3G propias de la empresa participante
- La realización de todos los lotes serán supervisados siempre por un empleado de STL que garantizará que no hay apropiación indebida de información en caso de que un sistema sea comprometido
- Los servicios proporcionados se realizarán siempre en horario laboral y tras la notificación previa al responsable de STL, en caso de que el riesgo de ataque tenga éxito e implique una posible parada de servicio, se podrán realizar fuera del horario laboral, pero siempre deberá ser autorizado por el responsable de STL. No se realizará ningún ataque no supervisado o fuera del horario laboral si el plan de ataque no ha sido específicamente autorizado por el responsable de STL.
- Cualquier prueba de seguridad en la que exista un riesgo significativo de pérdida de servicio deberá ser comunicada y aprobada por el responsable de STL.
- Antes de la realización del servicio se revisara el plan entregado en la oferta y las herramientas incluidas en el mismo, la utilización de cualquier herramienta no incluida en la oferta tendrá que ser aprobada por el responsable de STL.
- Toda La documentación será entregada en soporte digital (PGP)

Requisitos específicos por LOTE

LOTE I

- Este Lote debe realizarlos un proveedor aprobado de escaneo (ASV) certificado por el consejo de normas de seguridad de la industria de tarjetas de pago (PCI SSC)
- Se indicara específicamente que herramienta va a ser utilizada para el análisis de vulnerabilidades así como la ultima actualización de pluggins de la misma

LOTE II

- Se indicara específicamente que herramienta va a ser utilizada para el análisis de vulnerabilidades así como la ultima actualización de pluggins de la misma

LOTE III

- Las pruebas de penetración incluirán capa de red y capa de aplicación y cumplirán el requisito 11.3 PCI-DSS en su totalidad.

LOTE IV

- El procedimiento de auditoria sobre la seguridad perimetral implicará un ataque de tipo caja negra (esto es sin información sobre su diseño)

para intentar acceder a la red interna y a la DMZ sorteando las restricciones de seguridad implantadas en los firewalls.

- Las pruebas de penetración incluirán capa de red y capa de aplicación y cumplirán el requisito 11.3 PCI-DSS en su totalidad para las dos IP's afectadas por esta normativa.

LOTE V

Por requisitos de confidencialidad, solo se entregaran los requisitos de este lote a las empresas interesadas con el fin de evitar distribución pública de los mismos.

CONDICIONES DE ÉXITO LOTE III y IV

Se considerará un ataque exitoso cuando el atacante consiga:

- Anular alguna medida de seguridad.
- Alterar la configuración o el funcionamiento de un dispositivo con riesgo para la seguridad del sistema.
- Sortear un control de acceso o autorización.
- Acceder a información no autorizada.
- Acceder con permiso de escritura a información no autorizada.

En el caso de los ataques de caja blanca el éxito de un ataque se considera, además cuando el atacante consiga:

- Vulnerar la seguridad de la organización afectando a la autenticación de usuarios o a la confidencialidad de la información o al control de acceso.

Cada ataque exitoso deberá aportar una nueva brecha de seguridad y no ser una simple variación de otra vulnerabilidad previamente ya catalogada como un ataque exitoso.

No se considerarán ataques exitosos los que utilicen técnicas de fuerza bruta para abrir ficheros o acceder a sistemas protegidos salvo cuando éstos impliquen recursos limitados y tiempo inferior a una semana.

Se considerarán ataques exitosos los basados en diccionarios para abrir ficheros o acceder a sistemas protegidos salvo cuando éstos impliquen tiempo superior a una semana o recursos no limitados.

En caso de que se haya accedido a un fichero protegido con contraseña o se disponga de un método de ataque por fuerza bruta y/o ataque basado en diccionarios, en el informe se reflejará la vía de ataque propuesta y el tiempo estimado para su conclusión con éxito.

La auditoria no cubrirá aspectos de disponibilidad o integridad del sistema de información en tanto en cuanto éstos no tengan que ver directamente con la previsión de ataques intencionados. Es decir, los mecanismos de restauración de copias de seguridad y/o recuperación de sistemas ante caídas o fallos no formarán parte del test de intrusión.

No se consideran ataques exitosos los resultados de un escáner de vulnerabilidades informando sobre las mismas si no son explotadas.

Por cada ataque con éxito el proveedor entregara una ficha para ser validada por el responsable de STL y que cumplirá con los requisitos citados en este punto.

2.2. ENTREGABLES DEL SERVICIO

LOTE I

Informe de análisis de vulnerabilidades externo trimestral para el cumplimiento del Standard PCI-DSS

LOTE II

Informe de análisis de vulnerabilidades interno trimestral para el cumplimiento del Standard PCI-DSS.

LOTE III

El auditor interno proporcionara a STL un informe escrito y en soporte digital, el informe contendrá los siguientes entregables mínimos:

- Un resumen ejecutivo dirigido a personal no técnico y estrictamente escrito desde una perspectiva de negocio.
- Una descripción detallada de las vulnerabilidades encontradas y los pasos necesarios para su mitigación. Las vulnerabilidades se numeraran para utilizarlas como referencia y se asociaran al dispositivo correspondiente.
- El Test de penetración interno se realizara en distintas capas de la arquitectura, el informe final reflejara claramente la capa de la arquitectura desde donde se realizaron las distintas pruebas.
- Conclusiones / Recomendaciones
- Apéndices – Incluirán las salidas de todos los test realizados sobre los distintos sistemas, y proporcionaran las evidencias para dar soporte a las reclamaciones incluidas dentro del informe, esto permitirá a las distintas unidades de negocio identificar y verificar las pruebas de cualquier reclamación hecha y facilitara la acción correctiva que pudiera ser necesaria.
- Para determinar la gravedad de cada una de las vulnerabilidades se usara la puntuación base del estándar abierto CVSSv2 (Common Vulnerability Score System).

LOTE IV

Se generaran dos informes individuales para este lote:

- El primero hará referencia a dos direcciones IP afectadas por normativa PCI-DSS teniendo que cumplir estrictamente el punto 11.3 de PCI-DSS que separa las pruebas de penetración externas en capa de red y capa de aplicación.
- El segundo informe englobara el resto de servicios que ofrece la compañía y que abarca este lote IV

El auditor externo proporcionara a STL un informe escrito y en soporte digital el informe contendrá los siguientes entregables mínimos:

- Un resumen ejecutivo dirigido a personal no técnico y estrictamente escrito desde una perspectiva de negocio.
- Una descripción detallada de las vulnerabilidades encontradas y los pasos necesarios para su mitigación. Las vulnerabilidades se numeraran para utilizarlas como referencia y se asociaran al dispositivo correspondiente.
- Conclusiones / Recomendaciones
- Apéndices – Incluirán las salidas de todos los test realizados sobre los distintos sistemas, y proporcionaran las evidencias para dar soporte a las reclamaciones incluidas dentro del informe, esto permitirá a las unidades de negocio identificar y verificar las pruebas de cualquier reclamación hecha y facilitara la acción correctiva que pudiera ser necesaria.
- Para determinar la gravedad de cada una de las vulnerabilidades se usara la puntuación base del estándar abierto CVSSv2 (Common Vulnerability Score System).

LOTE V

Por requisitos de confidencialidad, solo se entregaran los requisitos de este lote a las empresas interesadas con el fin de evitar distribución pública de los mismos.

2.3. CONFIDENCIALIDAD

La información obtenida durante las pruebas de seguridad de cualquiera de los lotes será tratada como altamente confidencial y permanecerá en todo momento en propiedad de STL, cualquier registro electrónico relacionado con las pruebas de seguridad tendrá que permanecer protegido mediante la encriptación de los mismos.

A la finalización del servicio todos los documentos y registros electrónicos deberán ser destruidos de forma segura.