

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



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

SISTEMAS TECNICOS DE
LOTERIAS DEL ESTADO



**SISTEMAS TÉCNICOS DE
LOTERÍAS DEL ESTADO**

I. PRESENTACIÓN

SISTEMAS TÉCNICOS DE
LOTERÍAS DEL ESTADO

1. INTRODUCCIÓN

SISTEMAS TÉCNICOS DE LOTERIAS DEL ESTADO, S.A.Unipersonal, es una sociedad mercantil anónima, de carácter estatal, constituida como medio propio y servicio técnico de la Entidad Pública Empresarial 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.

2. OBJETO DEL CONCURSO

El objeto de este concurso es la contratación de servicios para la realización de pruebas de seguridad informática en la infraestructura y sistemas de información de STL.

Estos servicios tienen como objetivo final identificar el nivel de seguridad de los sistemas de información de STL incluidos dentro del alcance del procedimiento, así como proponer recomendaciones para mejorar su nivel de seguridad.

3. ANTECEDENTES

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. Al finalizar las pruebas se dispondrá de un informe que refleje los resultados de los distintos intentos de intrusión, las vulnerabilidades detectadas junto con una evaluación de la criticidad de dichas vulnerabilidades y las recomendaciones del proveedor para resolver todas las vulnerabilidades encontradas.





SISTEMAS TÉCNICOS DE
LOTERIAS DEL ESTADO

II. ESPECIFICACIONES TÉCNICAS

SISTEMAS TÉCNICOS DE
LOTERIAS DEL ESTADO

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 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.
- LOTE V: Consultaría estratégica de seguridad sobre la red interna de STL.

2. REQUISITOS

CARACTERÍSTICAS DE LAS PRUEBAS

- 2.1 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 auditoría.
- 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.

2.2 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 de código.
- Cross-site scripting.
- Autenticación incompleta y gestión de sesiones.
- Referencias directas a objetos inseguros.
- Inyección SQL
- Configuración incorrecta de la seguridad de aplicaciones.
- Almacenamiento criptográfico inseguro.
- Problemas de acceso a URL restringidas.
- Protección del nivel de transporte insuficiente.
- Redirecciones no validadas.

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

CONDICIONES DE ÉXITO

2.3 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 consigue:

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

- 2.4 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.
- 2.5 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.
- 2.6 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.
- 2.7 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.
- 2.8 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.

PERSONAL TÉCNICO A CARGO DE LAS PRUEBAS

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

CONDICIONES DE REALIZACIÓN Y TÉCNICAS A EMPLEAR

- 2.10 Los ataques para explotar vulnerabilidades remotas se realizarán desde una dirección de red previamente establecida (de forma que puedan quedar excluidas falsas denuncias en caso de que los sistemas de detección de intrusos de la organización den la alarma) y serán supervisados siempre por un empleado de STL que garantizará que no hay apropiación indebida de información en caso de que el ataque sea exitoso.
- 2.11 Los ataques para explotar vulnerabilidades remotas se realizarán, siempre que sea posible, en horario laboral. En caso de que el riesgo de que el ataque tenga éxito implique una posible parada de algún servicio, se podrán realizar fuera del horario laboral, pero siempre deberá ser autorizado por el responsable de STL. No se realizará ningún ataque remoto no supervisado o fuera del horario laboral si el plan de ataque no ha sido específicamente autorizado por el responsable de STL.
- 2.12 Los ataques que impliquen la presencia del proveedor en las dependencias de STL se realizarán siempre en horario laboral y tras la notificación previa al responsable de STL quien, después de ser informado sobre la naturaleza y el propósito del ataque, determinará si es necesaria la compañía de un empleado de STL que garantice que no hay apropiación indebida de información en caso de que el ataque sea exitoso.
- 2.13 El procedimiento de auditoría 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.
- 2.14 Para el test de intrusión en la red interna en una primera fase el atacante conectará físicamente a la red un equipo cualquiera no necesariamente configurado según la política de la organización e intentará realizar los ataques pertinentes sin conocer ningún usuario ni contraseña del directorio de usuarios.

El objetivo de esta primera fase será determinar la capacidad de penetración de un intruso con acceso físico a las tomas de red de la organización, pero sin acceso físico a un equipo controlado por la misma.

En una segunda fase, se facilitará al atacante un usuario que el responsable del STL autorizará. El atacante podrá utilizar un equipo propio y/o un equipo facilitado por la organización con la configuración habitual para el perfil del usuario con el que se realizará el test.

El objetivo de esta segunda fase será determinar la capacidad de penetración de los propios empleados de la organización o un atacante que haya obtenido acceso a la red local con el privilegio del usuario facilitado.

Ambas fases de los test de seguridad en la red interna serán de tipo caja negra.

- 2.15 Los procedimientos de auditoria con técnicas de caja blanca serán realizados en la última fase (después de agotar los procedimientos y técnicas de caja negra). Para la aplicación de procedimientos con técnicas de caja blanca el proveedor podrá requerir la colaboración del personal técnico de sistemas y/o desarrollo y recabar información técnica de detalle sobre los sistemas de la organización y su configuración.
- 2.16 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.
- 2.17 Durante la auditoria, la empresa concursante entregara un resumen de las pruebas realizadas así como una ficha por cada test de intrusión realizado que el concursante considere exitoso con la información pertinente para su calificación. El responsable del STL determinara con esta ficha si el test reúne las condiciones de éxito exigidas.
- 2.18 Los LOTES II y III se realizaran en las dependencias de STL.
- 2.19 LOTE V, Se realizará un estudio integral de la seguridad interna de la compañía, localizando las principales debilidades tanto técnicas como de procedimiento. Cabe destacar que STL esta afectado por las siguientes normativas LOPD, PCI-DSS, ISO 27001(SGSI implantado), WLA-SCS, LSSI-LISI. El objetivo de este servicio no es auditar el cumplimiento estricto de cada una de estas normas, debe estar enfocado a dar una visión global del estado de la seguridad interna de la compañía, analizando las soluciones de seguridad implantadas por STL.

METODOLOGÍA

- 2.20 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.

3. ENTREGABLES

LOTE I

Informe de vulnerabilidades externo trimestral para el cumplimiento del Standard PCI-DSS, este informe tendrá que ser realizado por un ASV autorizado.

LOTE II

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

LOTE III y LOTE IV

Al finalizar el trabajo, el proveedor entregará un informe en el que se reflejara cada uno de los test de intrusión que ha realizado, el objetivo, su resultado, así como una valoración del estado de la posible vulnerabilidad y su posible solución.

La empresa valorará cada vulnerabilidad encontrado en función de su criterio según afecte a los sistemas de la siguiente manera:

Leve: si la vulnerabilidad no afecta directa ni indirectamente a ningún dato de carácter personal, ni a ningún elemento crítico para la organización y su negocio, ni a la imagen de la organización.

Grave: si la vulnerabilidad puede afectar a la imagen de la organización, pero no a un elemento crítico de la misma ni a datos de carácter personal.

Crítica: si la vulnerabilidad afecta a algún elemento esencial para la organización o algún dato de carácter personal.

LOTE V

Informe de consultoría, donde queden claramente definidas el conjunto de acciones a ejecutar para la mejora integral de la seguridad con asignación de prioridades.

4. 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.

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

5. INCENTIVO Y CALIDAD

Dado lo especializado del proceso de descubrimiento de fallos de seguridad y para garantizar que los servicios se enfocan en el valor añadido y la localización de vulnerabilidades es necesario algún esquema de incentivos. Para ello, el proveedor deberá detallar en su oferta económica dos propuestas:

- 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.
- 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.

El responsable de STL será el encargado de asegurar que los trabajos se realizan con la calidad adecuada y quedan completamente documentados siguiendo la metodología propuesta por el proveedor.

6. ACUERDO DE CONFIDENCIALIDAD

La empresa adjudicataria y Sistemas Técnicos de Loterías firmarán un acuerdo de confidencialidad a efectos de mantener la reserva sobre todos los datos e informaciones que obtengan durante la ejecución de las pruebas de seguridad, contrayendo la obligación de no suministrar información alguna a terceros, salvo en aquellos casos en que se obtenga autorización previa y por escrito de STL.



III. BASES DEL CONCURSO

SISTEMAS TECNICOS DE
LOTERIAS DEL ESTADO

1. CONDICIONES GENERALES DEL PROCEDIMIENTO

REGULACIÓN: La contratación objeto de este procedimiento se registrá exclusivamente por las normas de derecho privado español y por las instrucciones internas de contratación respecto de bienes y servicios de STL.

PRINCIPIOS: A fin de dar cumplimiento a los principios de publicidad, concurrencia, transparencia, confidencialidad, igualdad y no discriminación la selección se llevará a cabo mediante el presente procedimiento, cuya convocatoria se publicará en el apartado "Perfil del contratante" de la página Web de la entidad www.stl.es . Asimismo, esta convocatoria se comunicará a las compañías que, a juicio de STL, tengan capacidad técnica para atender la solicitud.

2. CONFIDENCIALIDAD Y CONFLICTO DE INTERESES:

Los interesados se comprometen a guardar absoluta reserva sobre todos los datos e informaciones que obtengan durante el proceso de licitación, contrayendo la obligación de no suministrar información alguna a terceros, salvo en aquellos casos en que se obtenga autorización previa y por escrito de STL Esta obligación continuará incluso después de concluida la selección.

Tanto STL como el adjudicatario adoptarán las medidas adecuadas para limitar el acceso del personal que realice el servicio a los datos personales e información protegida o a los recursos del sistema de información que los contenga, para la realización de aquellos trabajos que no impliquen, necesariamente, el tratamiento de datos personales.

Igualmente, tras la adjudicación del contrato, el adjudicatario, obedecerá y hará obedecer las directrices en materia de seguridad que STL disponga en lo referente al acceso a datos de carácter personal y mantendrá, y en su caso hará mantener al personal implicado, obligación de guardar secreto respecto a todos aquellos datos que hubiera podido conocer con motivo de la prestación del servicio.

Los interesados aseguran que no se encuentran en ninguna situación

que directa o indirectamente suponga un conflicto de interés para el cumplimiento del objeto de la convocatoria.

INFORMACIÓN ADICIONAL: Los licitadores podrán solicitar cualquier información adicional que consideren necesaria. Esta deberá solicitarse a las siguientes direcciones de contacto:

Contacto técnico

Para cualquier duda o pregunta concerniente a las especificaciones técnicas o a la descripción del alcance o la calidad de los servicios demandados, 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

Se anima a los licitadores a utilizar preferentemente el correo electrónico como canal de comunicación para dudas técnicas.

Contacto administrativo

Para cualquier consulta concerniente al formato de las ofertas, se pone a disposición de los licitadores la siguiente dirección postal y/o correo electrónico.

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 de tipo administrativo.

3. CONTENIDO DE LAS OFERTAS:

La documentación se presentará en castellano.

- Las ofertas deben ser preparadas de una manera sencilla, proporcionando una descripción clara y concisa de las capacidades del licitador para los requisitos exigidos en las presentes Bases.
- Las condiciones establecidas en este documento se considerarán básicas, de modo que cada LICITADOR podrá añadir cuanta información adicional considere útil para la comprensión de su oferta.

1. Documentación General:

Con carácter obligatorio y de forma preceptiva para la consideración de las oferta, los interesados deberán presentar, en documento separado, la siguiente documentación debidamente compulsada:

- Escritura de constitución de la sociedad inscrita en el Registro mercantil y/o Estatutos. (En el caso de licitadores extranjeros, miembros de la UE, ésta se acreditará por su conformidad con la legislación del Estado de origen. En el caso de no miembros de la UE, se acreditará mediante el informe de la Oficina Consular correspondiente.)
- Fotocopia del DNI o pasaporte del licitador
- Declaración responsable de hallarse al corriente de pago en las obligaciones tributarias y con la Seguridad Social
- Memoria de cuentas anuales correspondientes al último ejercicio (para los no obligados a presentar cuentas en el Registro, bastará con los libros de contabilidad debidamente legalizados)

2. Documentación técnica-comercial:

- Memoria técnica de los servicios ofrecidos incluyendo:
 - Planificación de los servicios, con detalle de actividades, la asignación de recursos y el calendario de realización del servicio.
 - Lista de vulnerabilidades a comprobar.

- Currículum vitae de cada miembro del equipo propuesto con referencias de organizaciones publicas o privadas que hayan recibido servicios similares al propuesto en los que el equipo estuvo implicado.
- Metodología a utilizar y listado de herramientas.
- Plan de aseguramiento de calidad de los servicios ofrecidos así como certificados acreditativos del cumplimiento de normativa de calidad y estándares acreditados por organismos conformes a las normas europeas.
- Declaración que acredite el personal, volumen de plantilla y número de técnicos de los que disponga el licitador.
- Perfil y experiencia de las personas propuestas por el **LICITADOR** para la ejecución de los servicios ofrecidos.
- Relación de servicios similares ya ejecutados o en proceso de ejecución por el LICITADOR, si los hubiere, indicando: empresa en que se realizó la entrega de servicios, fecha de finalización, etc.
- Cualquier otra información que el oferente considere de interés.

3. Documentación económica:

- Los precios se indicarán en euros
- Cada oferta contemplará el importe global y, de forma unitaria, de cada uno de los LOTES (I, II, III, IV y V), con el máximo detalle, siendo posible la adjudicación individual de cada uno de los lotes a diferentes empresas.
- En el caso de ofertar soluciones alternativas, se incluirán cuantas proposiciones económicas sean precisas.

3. PRESENTACIÓN DE LAS OFERTAS:

La documentación exigida para participar en el concurso habrá de entregarse en mano o remitirse por correo certificado antes de las 12:00 horas (hora local) del día 7 de septiembre de 2010, a la siguiente dirección:

Dpto. Compras
Att. D. José Manuel Hombre Baena

Los licitadores remitirán las ofertas en formato impreso y en formato digital en un sobre en el que conste, en lugar visible, la inscripción:

“PROCEDIMIENTO DE ADJUDICACIÓN DE SERVICIOS PARA LA EVALUACIÓN DE VULNERABILIDADES Y TEST DE INTRUSIÓN”

4. CRITERIOS GENERALES DE VALORACIÓN DE LAS OFERTAS:

Los factores relevantes para la determinación de la oferta u ofertas seleccionadas tendrán en cuenta las siguientes cuestiones generales:

- Referente a la oferta
 - Cumplimiento de todos los requisitos exigidos en este documento, ya sean de carácter formal técnico, o, económico.
 - Mejoras complementarias o añadidas.
- Referente al oferente
 - Experiencia previa en el servicio demandado.
 - Solvencia técnica y recursos disponibles.
 - La experiencia del equipo de personas a cargo de las pruebas.
- Referente a los productos
 - Los criterios técnicos y la calidad de la propuesta en cuanto a cantidad y diversidad de vulnerabilidades a comprobar.
 - La metodología propuesta.
 - La presentación de certificaciones relacionadas con la seguridad de las TIC (por ejemplo ISO-27000 a nivel de la organización que presta los servicios o certificación CISA, CISM, CISSP, CEH, CHFI, GIAC, CCSP, OPST, OPSA de los miembros del equipo propuesto).
- Aspectos económicos
 - El coste total de los servicios que deberá recoger el precio base por

consultoría y el programa de incentivos asociado a cada categoría de vulnerabilidad.

- Periodo de garantía ofertado.
- Propuesta financiera y modos de pago.
- Contraprestaciones.

STL se reserva el derecho a:

- Rechazar cualquier oferta o todas ellas e interrumpir el proceso de licitación sin obligación o compromiso con ninguno de los licitadores
- Conceder un contrato según los términos iniciales de la oferta recibida, sin cabida para negociación o entrega de nuevas ofertas finales
- Rechazar una oferta que no aporte toda la información solicitada en este procedimiento
- Rechazar una oferta que se aleje de lo razonable en lo que respecta a las prácticas técnicas y comerciales habituales en el mercado
- Entablar negociaciones con uno o más proveedores seleccionados con vistas a la firma del contrato.

5. ADJUDICACIÓN

Terminado el análisis de las diferentes ofertas, STL seleccionará la oferta que pudiera resultar adjudicataria, con cuyo titular se procederá a la eventual adaptación del Contrato a la oferta ganadora.

Será posible la adjudicación individual de cada uno de los lotes de servicios a diferentes empresas.

6. MODELO DE PAGO

Cada análisis/fase/trimestre se pagará a la finalización de la misma hasta un 95% del precio estipulado.

Se retendrá un 5% de cada facturación que se hará efectivo a la finalización del periodo de contratación y una vez terminados todos los análisis comprometidos.