AVISO DE CONVOCATORIA PÚBLICA

SELECCIÓN ABREVIADA SUBASTA INVERSA No 002 de 2019

Objeto: MONITOREO A LA INFRAESTRUCTURA Y A LOS ELEMENTOS DE SEGURIDAD IMPLEMENTADOS EN LAS PÁGINAS WEB DEL MINISTERIO.

El Fondo Rotatorio del Ministerio de Relaciones Exteriores, en cumplimiento de lo exigido en el artículo 2.2.1.1.2.1.2 del Decreto 1082 de 2015, informa a la comunidad en general que iniciará proceso de **SELECCIÓN ABREVIADA SUBASTA INVERSA No. 002 de 2019.**

Para efectos de lo anterior, se señala a continuación la información indicada en el artículo 2.2.1.1.2.1.2 del Decreto 1082 de 2015:

1. OBJETO

MONITOREO A LA INFRAESTRUCTURA Y A LOS ELEMENTOS DE SEGURIDAD IMPLEMENTADOS EN LAS PÁGINAS WEB DEL MINISTERIO

1.1. ESPECIFICACIONES TÉCNICAS MÍNIMAS

LAS SIGUIENTES SON LAS ESPECIFICACIONES MÍNIMAS TÉCNICAS QUE DEBEN CUMPLIR LAS PROPUESTAS:

DESCRIPCIÓN	CARACTERÍSTICA
1. CARACTERÍSTICAS GENERALES	1.1. El servicio ofertado para el monitoreo de actividad anómala de Phishing y Pharming en los sitios protegidos debe ser en modalidad 7x24 por 8 meses. El proponente debe garantizar el monitoreo a la infraestructura y a los elementos de seguridad implementados en las páginas web del ministerio de acuerdo con el **Listado No. 1 páginas Web de la Entidad**, que se compone de los siguientes dominios: • cancilleria.gov.co, • colombianosune.com, • consulado.gov.co, • embajada.gov.co • mision.gov.co. • Adicional a los anteriores se deben monitorear y proteger 300 sub-dominios que tiene actualmente el ministerio, así como los que vayan siendo adicionados, tanto a nivel de dominios como de sub-dominios.
	1.2. El servicio debe cubrir todo el ciclo de vida de una alerta, desde que se inicia hasta que se soluciona.
	1.3. La solución debe detectar en tiempo real las conexiones de los sitios protegidos, entregando información, tal como, IP, Fechas, Horas, Información de Geolocalización, URL de conexión, URL de origen, Proxys Anónimos, etc.
	1.4. El servicio de antiphishing y antipharming debe detectar en tiempo real ataques que pretendan enviar información crítica y/o confidencial a través de la URL (por ejemplo: inyectar código SQL)

	1.5. El servicio debe contar con la capacidad de detectar sistemas operativos y navegadores de internet obsoletos, que por no estar soportados por sus respectivos fabricantes tengan un número importante de vulnerabilidades descubiertas.
	1.6. La solución debe proveer detección y bloqueo de conexiones a través de proxies anónimos y/o cualquier otro canal de conexión que atente contra la integridad del sitio protegido.
	1.7. La solución debe proveer detección y bloqueo de conexiones que provengan de fuentes sospechosas en tiempo real.
	1.8. Debe tener la capacidad de analizar el origen de las conexiones, detectando, y bloqueando las que vengan de países riesgosos en cuanto a actividad maliciosa.
	1.9. La solución debe proveer la funcionalidad de recuperación forense de evidencias de ataques informáticos y credenciales robadas siempre que se encuentren disponibles.
	1.10. El servicio de monitoreo debe generar alertas personalizadas de acuerdo con las diferentes variables de conexión presente tales como IP, REFERRER, VARIABLES, etc. con el objeto de generar alertas de acuerdo con patrones específicos de interés para la Entidad.
	1.11. El servicio de monitoreo debe detectar cualquier comportamiento anómalo de navegación y/o uso de los sitios web protegidos, tales como, • Copia del sitio protegido. • Redireccionamiento. • Detectar porcentajes de cambio de contenidos en los archivos de los dominios propiedad del Ministerio antes de 10 minutos de haberse producido el mismo. • Monitorear versiones de todos los cms utilizados por la cancillería ahora y en el futuro, incluyendo los plugins internos instalados en todos los sistemas. • Monitoreo de latencia, detectando cambios sustanciales en tiempo de carga de todos los dominios y subdominios de la cancillería. • Informes mensuales detallados de tiempo de respuesta de cada uno de los dominios y subdominios de los sistemas. • Monitoreo activo de subida de archivos con protección de virus, backdoors, shells y cualquier archivo malicioso, con aviso inmediato y sistema de cuarentena para su posterior análisis.
	1.12. El servicio debe garantizar las desactivaciones de todos los ataques dirigidos a las páginas web, para garantizar una disponibilidad de las páginas web del 99.9%.
	1.13. La solución debe estar en la capacidad de detectar y desactivar amenazas o ataques en contra las páginas web, tales como malware, Man-in-the-Middle y Man-in-the-Browser.
	1.14. El servicio debe proveer información de los incidentes y de gestión general.
	1.15. El servicio ofrecido por el proveedor debe proteger contra ataques de denegación de servicio (DDoS). Mitigación de posibles ataques DDOS para mantener el funcionamiento y la disponibilidad. El proveedor debe prestar un servicio donde los sitios web y las aplicaciones tengan la capacidad de resistencia y la inteligencia de una red escalable para combatir los ataques más grandes y nuevos. Dicha protección contra amenazas no debe degradar el funcionamiento causado por las latencias inducidas por la seguridad y los servicios de

	seguridad deben ser fáciles de configurar para eliminar los errores de configuración, que introducen nuevas vulnerabilidades. El proveedor del servicio debe informar de forma temprana e inmediata si la Entidad presenta un ataque crítico de este tipo, y así mismo informar las medidas de contención que se implementaron o las que la Entidad debe implementar, estadísticas de gestión, reportes de incidentes.
	1.16. El firewall de aplicaciones web (WAF) debe proteger todos los dominios, aplicaciones y contenidos alojados en los servidores del Ministerio contra ataques de inyección de código SQL, secuencias de comandos en sitios cruzados y solicitudes de falsificación entre sitios.
	1.17. Control para bloquear visitantes sospechosos. El servicio ofrecido por el proveedor debe proteger todos los dominios, aplicaciones y contenidos alojados en los servidores del Ministerio contra ataques de denegación de servicio, intentos de inicio de sesión por fuerza bruta y otros tipos de comportamientos abusivos dirigidos a la capa de aplicación y permitir que todos los recursos de Internet que se encuentren en la red del Ministerio puedan soportar ataques DDoS masivos.
	1.18 El servicio ofrecido por el proveedor debe configurar umbrales, definir respuestas y obtener información valiosa sobre direcciones URL específicas de sitios web, aplicaciones o puntos de conexión de API. Facilitar un control detallado del tráfico HTTP/HTTPS, que complemente las soluciones de protección DDoS y el Firewall de aplicaciones web (WAF). Esto con el fin de eliminar los picos de tráfico y los ataques imprevisibles.
	1.19. El servicio ofrecido por el proveedor debe cifrar tanto tráfico web como sea posible para evitar el robo de datos y manipulaciones. Por lo tanto, ofrecer protección SSL a los contenidos alojados por el Ministerio.
	1.20. El servicio ofrecido por el proveedor debe garantizar que el tráfico de una aplicación web se enrute de manera segura a los servidores correctos para que los visitantes de un sitio no sean interceptados por un atacante intermedio.
	1.21. El servicio ofrecido por el proveedor debe mitigar y bloquear los ataques DDoS basados en DNS flooding.
	1.22. El servicio ofrecido por el proveedor debe mitigar y bloquear los ataques de reflexión, el envenenamiento de caché, las inundaciones de TCP SYN, la tunelización de DNS y el secuestro de DNS para interrumpir el servicio para un dominio particular que se dirige al Sistema de nombres de dominio.
2. FUNCIONALIDADES	2.1. La solución debe contar con una funcionalidad de reconocimiento de ataques de Defacement contra los sitios WEB previniendo cambios en el contenido no autorizados. (prevenir y bloquear) % de cambios a nivel de archivos del CMS en menos de 5 minutos.
	2.2. La solución debe monitorear activamente la veracidad del certificado SSL de los dominios protegidos, identificando de forma temprana posibles cambios, caducidad o riesgo con la Entidad certificadora e informar al supervisor del contrato de manera oportuna.
	2.3. El servicio debe monitorear de forma constante el tiempo de respuesta y los niveles de disponibilidad de los sitios web protegidos desde diferentes locaciones a nivel mundial identificado y bloqueando ataques de denegación de servicio y/o disponibilidad de los sitios.

	2.4. La solución debe monitorear cambios en la resolución de dominio identificando y bloqueando ataques de re direccionamiento de tráfico tales como DNS spoofing / DNS Poisoning.
	2.5. El servicio ofrecido por el proveedor debe garantizar Monitoreo del sitio web en modalidad 7x24. Debe maximizar la experiencia de usuario final con la combinación de: • Monitoreo del tiempo de actividad del sitio web. • carga de página completa, monitoreo de transacciones sintéticas y comprobador de estrés web.
	2.6. El servicio ofrecido por el proveedor debe garantizar Monitoreo de red en modalidad 7x24. Debe asegurar que las redes estén protegidas y sintonizadas con el monitoreo. Las redes de TI deben monitorear permanentemente la red para detectar y resolver rápidamente los problemas y las interrupciones del rendimiento de la misma. Deben proporcionar monitoreo de: • Firewalls. • Protocolos TCP: SMTP, HTTP, Imap, UDP, SIP, etc.. • Monitoreo de ancho de banda de red. • Dispositivos SNMP. • Enlaces WAN.
	2.7. El servicio ofrecido por el proveedor debe garantizar Monitoreo del servidor en modalidad 7x24. La herramienta de monitoreo del servidor debe permitir verificar indicadores clave de rendimiento y detectar problemas de rendimiento del servidor. • Este servicio debe realizar chequeos en menos de un minuto. • Debe tener agentes nativos para Linux. • Debe chequear CPU, memoria, almacenamiento y disco, ancho de banda de red. • Debe chequear Procesos y servicios.
	2.8. El servicio ofrecido por el proveedor debe garantizar el monitoreo de cualquier tipo de sistema y métricas de TI desde un solo panel de control. Debe garantizar: • API fácil de usar con documentación completa. • SDK para todos los lenguajes populares, incluidos Java, Perl, Python, PHP, Ruby, C #.
	2.9. El servicio ofrecido por el proveedor debe garantizar el monitoreo del rendimiento de la aplicación. Debe realizar un seguimiento del rendimiento de los sitios web y de toda la infraestructura subyacente: servidores, redes, aplicaciones y experiencia del usuario.
	2.10 El proveedor debe garantizar la confidencialidad, integridad, autenticidad y disponibilidad de las páginas web de la Entidad, por lo cual debe disponer de un servicio especializado que permita evaluar, analizar, revisar, monitorear y recomendar acerca de los

	diferentes ataques que pueden afectar la disponibilidad y confiabilidad de las páginas web del Ministerio.
3. SOPORTE Y ADMINISTRACIÓN	3. Especificaciones, DNS El manejo del DNS público debe ser administrado y soportado por el proveedor, para asegurarse de que las propiedades web del Ministerio estén en línea y siempre disponibles para cualquier usuario en el mundo.
	3.1. El servicio ofrecido debe contar con reportes, de la actividad anómala de phishing, pharming, malware, MITM, MITB, monitoreo de defacement, disponibilidad, resolución DNS, certificados SSL, estadísticas de gestión, reportes de incidentes.
	3.1.1. El proponente debe informar de forma temprana e inmediata si la Entidad presenta un ataque crítico, así mismo informar las medidas de contención que se implementaron o las que la Entidad debe implementar.
	3.2. Es requerido que se incluyan la documentación de los incidentes, tales como: posibles causas, fuentes de los ataques (tomando en cuenta la evidencia que esté disponible), recolección de evidencia (cuando sea posible) para análisis forense posterior.
	3.3. La solución debe generar reportes que incluyan información sobre conexiones y alertas y los requeridos por la Entidad.
	3.4. El proveedor debe contar con soporte en español.
	3.5. El proveedor seleccionado debe hacer un acompañamiento una vez puesta en producción la solución, para poder detectar posibles mejoras y requerimientos.
	3.6. El proveedor del servicio debe garantizar el cumplimiento de los objetivos de la migración: • Llevar a cabo la migración de los siguientes sitios con sus DNS y configuraciones correspondientes: cancilleria.gov.co, colombianosune.com, consulado.gov.co, embajada.gov.co y mision.gov.co. • Actualización de los servicios con los DNS por parte del cliente. • Puesta en funcionamiento de los sitios con la nueva infraestructura. • No alterar la prestación del servicio al usuario final. • No afectar el Acuerdo de Nivel de Servicio de 99,9% de tiempo al aire de las páginas web del Ministerio. • Prestar de manera eficiente y eficaz el servicio de Monitoreo a la infraestructura y a los elementos de seguridad implementados en las páginas web del ministerio bajo el dominio cancillería.gov.co. La migración debe cumplir con el objetivo de no alterar la prestación del servicio al usuario final, ni afectar el Acuerdo de Nivel de Servicio de 99,9% de tiempo al aire de las páginas web del Ministerio, así como asumir el control de la prestación del servicio de Monitoreo a la Infraestructura y a los elementos de seguridad implementados en las páginas web del ministerio bajo el dominio cancillería.gov.co en las ocho horas que el Ministerio tiene designadas para tal fin.

4. EXPERIENCIA PERSONAL	Para garantizar el soporte, gestión y monitoreo se debe garantizar que el proponente cuenta con el siguiente personal, por lo cual debe anexar el formato de ANEXO DE EXPERIENCIA DEL PERSONAL PROPUESTO, incluir la hoja de vida y copia de las certificaciones: ➢ Un (1) Gerente de Proyecto, con experiencia de al menos tres años como gerente de proyecto. ➢ Personal para la administración de servidores: Mínimo tres (3) años de experiencia específica en proyectos relacionados con el objeto del contrato a través de certificaciones expedidas por el proponente. ➢ Personal para los servicios de monitoreo: Mínimo tres (3) años de experiencia específica en proyectos relacionados con el objeto del contrato a través de certificaciones expedidas por el proponente.
5. HORARIOS	Todas las labores de configuración y puesta en funcionamiento, que impliquen negación de algún servicio informático, se realizarán programados conjuntamente entre el proponente adjudicatario y la Entidad. Estos tiempos podrían ser horas nocturnas, sábados o domingos, sin incurrir en costos adicionales para la Entidad.
6. INFORMES	• El proponente adjudicatario debe entregar un informe y reporte de Gestión Mensual. Este es un Informe Gerencial en el que se observe el comportamiento del servicio prestado por el PROPONENTE ADJUDICATARIO. Incluye la disponibilidad del servicio y su comportamiento mes a mes. • El proponente adjudicatario debe realizar una reunión de seguimiento mensual para monitorear y revisar el cumplimiento de los acuerdos establecidos.

2. MODALIDAD DE SELECCIÓN

Para determinar la modalidad de selección que aplica al presente proceso, se tiene en cuenta lo señalado en los artículos 2.2.1.2.1.2.1 y 2.2.1.2.1.2.6 del Decreto 1082 de 2015: **Selección Abreviada por Subasta Inversa.**

3. PRESUPUESTO OFICIAL

Valor Estimado del contrato: El presupuesto oficial para la presente contratación será hasta la suma de **CIENTO NOVENTA Y DOS MILLONES NOVECIENTOS CUARENTA Y UN MIL PESOS M/CTE ($ 192.941.000) incluido el valor del IVA**.y demás impuestos, tasas, contribuciones y costo directos e indirectos a los que haya lugar.

Dicho presupuesto se encuentra respaldado en el Certificado de Disponibilidad Presupuestal No.34319 del 04 de marzo de 2019, por valor de **CIENTO NOVENTA Y DOS MILLONES NOVECIENTOS CUARENTA Y UN MIL PESOS M/CTE ($ 192.941.000)** expedido por el funcionario encargado de las operaciones presupuestales del Fondo Rotatorio del Ministerio de Relaciones Exteriores, para la vigencia 2019.

4. PLAZO DE EJECUCIÓN

El plazo para ejecutar el contrato resultante de este proceso será hasta el 31 de diciembre de 2019 días calendario, contados a partir de la aprobación de la garantía única de cumplimiento, previa expedición del registro presupuestal.

El lugar de entrega del soporte y servicios: El lugar de ejecución del contrato resultante de este proceso será en la Ciudad de Bogotá D.C., Sede Principal del Ministerio de Relaciones Exteriores Calle 10 No. 5-51 Palacio San Carlos.

Forma de pago:

La ENTIDAD pagará al CONTRATISTA el valor del contrato una vez se encuentre aprobado el P.A.C. (Programa Anual Mensualizado de Caja), así:

- Se cancelará en mensualidades vencidas de acuerdo con los servicios de soporte efectivamente prestados y verificado el cumplimiento del objeto del contrato, el cual se cancelará dentro de los diez (10) días hábiles siguientes previa presentación de la factura el certificado de cumplimiento a satisfacción expedida por el supervisor del contrato, informe de actividades y demás trámites administrativos a que haya lugar.

  Si las facturas no han sido correctamente elaboradas o no se acompañan los documentos requeridos para el pago y/o se presentan de manera incorrecta, el término para éste sólo empezará a contarse desde la fecha en que se aporte el último de los documentos y/o se presenten en debida forma. las demoras ocasionadas por estos conceptos serán responsabilidad del contratista y no tendrán por ello derecho al pago de intereses o compensación de ninguna naturaleza.

Supervisión: La supervisión en la ejecución del contrato, la ejercerá la Oficial de Seguridad de la Información y Comunicaciones de la Dirección de Gestión de Información y Tecnología o quien haga sus veces, quien es designado por el competente contractual.

5. CRONOGRAMA DEL PROCESO

El Fondo Rotatorio del Ministerio Relaciones Exteriores dispondrá del siguiente cronograma para el trámite del presente proceso de selección:

DESCRIPCIÓN	FECHAS
Publicación Aviso de Convocatoria Pública en el Portal Único de Contratación – SECOP, Proyecto de Pliego de Condiciones y Estudios Previos	21 de marzo de 2019
Observaciones al Proyecto de Pliego de Condiciones	Del 21 al 28 de marzo de 2019
Manifestación de interés limitación convocatoria Mipymes	01 de abril de 2019
• Respuesta a observaciones al proyecto de Pliego de Condiciones si hubiere lugar. • Acto Administrativo de Apertura, publicación del Pliego de Condiciones Definitivo en el Portal Único de Contratación – SECOP II. • Inicio del plazo para presentar propuestas. • Limitación o no a MiPymes de proceso de selección.	02 de abril de 2019
Plazo para que los interesados presenten observaciones al Pliego de Condiciones Definitivo	Hasta 04 de abril de 2019
Respuesta a observaciones al Pliego de Condiciones Definitivo si hubiere lugar	08 de abril de 2019
Publicación de Adendas si hubiere lugar	08 de abril de 2019

DESCRIPCION	FECHAS
Presentación de Propuestas y Cierre del proceso	09 de abril de 2019 **HORA: 8:00 a.m.** Plataforma SECOP II
Verificación requisitos habilitantes y de la propuesta	Del 09 al 10 de abril de 2019
Traslado Informe de verificación	Del 11 al 15 de abril de 2019
Publicación del informe de habilitados y respuesta a las observaciones	16 de abril de 2019
Apertura del Sobre Económico, revisión de propuestas económicas y verificación de la propuesta económica más baja.	17 de abril de 2019 **HORA: 9:00 a.m.** Plataforma SECOP II
Realización de la Subasta Inversa Electrónica	17 de abril de 2019 **HORA: 03:00 p.m.** Plataforma SECOP II
Adjudicación del contrato	Dentro de los tres (3) días hábiles siguientes a la realización de la subasta inversa electrónica.
Firma del Contrato	Dentro de los tres (3) días hábiles siguientes a la adjudicación.
Publicación del Contrato en el Portal único de Contratación	Dentro de los (3) días hábiles siguientes a la suscripción del contrato.

6. PRESENTACIÓN DE LAS PROPUESTAS

Los proponentes deben presentar sus Ofertas de MANERA DIGITAL a través de la plataforma de SECOP II, con los formatos contenidos en los anexos del presente proceso, en la fecha establecida en el Cronograma, y acompañadas de los documentos solicitados. Las Ofertas estarán vigentes por el término de noventa (90) días calendario, contados desde la fecha de presentación de Ofertas establecida en el Cronograma.

En caso de discrepancias entre números y letras prevalecerá la información en letras.

El idioma del proceso de selección es el castellano, y por lo tanto, se solicita que todos los documentos y certificaciones a los que se refiere el pliego de condiciones emitidos en idioma diferente al castellano, sean presentados en su idioma original y en traducción simple al castellano.

La presentación de las propuestas se efectuará a través de la de la plataforma de Secop II, en la cual se relacionarán las propuestas presentadas, indicando el orden de entrega, fecha y hora, o si por el contrario no se presenta ningún oferente. La presentación de la propuesta constituye un compromiso entre el proponente y la Entidad, según el cual dicha propuesta, permanece abierta para su evaluación y aceptación durante la vigencia de la garantía de seriedad de la propuesta, so pena de hacerla efectiva si el proponente la retira, salvo que este retiro obedezca a la configuración de una causal de inhabilidad o incompatibilidad sobreviniente.

Nota- información confidencial. A pesar de que la naturaleza de la información solicitada para la presentación de las propuestas no tienen la vocación de constituir información que pueda ampararse en la reserva o el secreto protegido por la ley, los proponentes son responsables de advertir lo contrario en el caso en que las propuestas contuvieren información confidencial, privada o que configure secreto industrial, de acuerdo con la ley colombiana, indicando tal calidad y expresando las normas legales que lo fundamentan.

En todo caso, la Entidad se reserva el derecho de revelar dicha información a sus agentes o asesores, con el fin de evaluar la propuesta.

7. PROYECTO DE PLIEGO DE CONDICIONES Y ESTUDIOS Y DOCUMENTOS PREVIOS

El proyecto de pliegos de condiciones para este proceso de contratación, así como los estudios y documentos previos que sirvieron de base para su elaboración, se podrán consultar en el Portal Único de Contratación-Sistema Electrónico de la Contratación Pública - www.colombiacompra.gov.co, SECOP II, cualquier observación frente al desarrollo del proceso se recibirá a través de la plataforma.

8. ACUERDOS Y TRATADOS COMERCIALES EN MATERIA DE CONTRATACIÓN PÚBLICA

Los Acuerdos Comerciales son los tratados internacionales vigentes celebrados por el Estado Colombiano, que contienen derechos y obligaciones en materia de compras públicas. Es deber de la Entidad realizar un análisis acerca de la aplicación de los Acuerdos Comerciales al presente proceso de contratación, para lo cual se deberá diligenciar el siguiente cuadro, a partir de lo establecido en el **Manual para el manejo de los Acuerdos Comerciales en Procesos de Contratación**, publicado por Colombia Compra Eficiente en su página Web.

ACUERDO COMERCIAL		ENTIDAD ESTATAL INCLUIDA	PRESUPUESTO DEL PROCESO DE CONTRATACIÓN SUPERIOR AL VALOR DEL ACUERDO COMERCIAL	EXCEPCIÓN APLICABLE AL PROCESO DE CONTRATACIÓN	PROCESO DE CONTRATACIÓN CUBIERTO POR EL ACUERDO COMERCIAL
Alianza Pacífico	Chile	Si	No	Si*	No
	México	Si	No	Si*	No
	Perú	Si	No	Si*	No
Canadá		Si	No	Si*	No
Chile		Si	No	Si*	No
Corea		Si	No	Si*	No
Costa Rica		Si	No	Si*	No
Estados AELC		Si	No	Si*	No
Estados Unidos		Si	No	Si*	No
México		Sí	No	Si*	No
Triángulo Norte	El Salvador	Si	No	Si*	No
	Guatemala	Si	No	Si*	No
	Honduras	Si	No	Si*	No
Unión Europea		Si	No	Si*	No
Comunidad Andina		Si	No	Si*	No

9. CUMPLIMIENTO DE REQUISITOS PARA PARTICIPAR EN EL PROCESO

ABIERTO EL PROCESO, EL PROPONENTE DEBERÁ DAR CUMPLIMIENTO A LOS REQUISITOS JURÍDICOS, TÉCNICOS, ECONÓMICOS Y FINANCIEROS ESTABLECIDOS DENTRO DEL PLIEGO DE CONDICIONES.

El presente aviso se emite y publica el día

CARLOS RODRIGUEZ BOCANEGRA
Secretario General

Elaboró: Diego Alberto Arias Diaz. Abogado del Grupo Interno de Trabajo de Licitaciones y Contratos
Revisó: Melissa Montoya Quirama. Coordinadora del Grupo Interno de Trabajo de Licitaciones y Contratos