GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

SERVICIO DE MONITORIZACIÓN Y ELABORACIÓN DE CONTENIDOS PREVENTIVOS PARA EL COLECTIVO DE CIUDADANOS Y EMPRESAS, Y SERVICIO DE IDENTIFICACIÓN, CATEGORIZACIÓN Y ANÁLISIS DE HERRAMIENTAS DE SEGURIDAD GRATUITAS

EXP. 044/13

PLIEGO DE CARACTERÍSTICAS TÉCNICAS

Agosto 2013

ÍNDICE

Nota: Cualquier consulta en relación a este procedimiento de adjudicación debe dirigirse por correo electrónico a la dirección contratacion@inteco.es, indicando:

Asunto: número de expediente.

Cuerpo: nombre de la empresa, datos de la persona que realiza la consulta y texto de la consulta.

El presente documento cumple con las condiciones de accesibilidad del formato PDF (Portable Document Format).

Se trata de un documento estructurado y etiquetado, provisto de alternativas a todo elemento no textual, marcado de idioma y orden de lectura adecuado.

Para ampliar información sobre la construcción de documentos PDF accesibles puede consultar la guía disponible en la sección Accesibilidad > Formación > Manuales y Guías de la página http://www.inteco.es.

1. ALCANCE Y OBJETO DEL CONTRATO

1.1. ANTECEDENTES

La ciberseguridad y la confianza digital son hoy dos de los retos más importantes a los que se enfrentan gobiernos, empresas y ciudadanos. Se trata de aspectos de crucial importancia en un contexto global, interconectado y dependiente de la tecnología como es el actual, e imprescindible para alcanzar la necesaria confianza en el ámbito digital.

En este marco, la ciberseguridad y la confianza digital se posicionan como elementos claves para el desarrollo económico y por ello, la protección frente a las ciberamenazas y el fomento de la seguridad constituyen factores esenciales para el desarrollo de la economía de Internet.

La «*Estrategia Española de Seguridad Nacional 2013*» incluye como una de las líneas de acción estratégicas la implantación de una cultura de ciberseguridad sólida, a través de la concienciación a ciudadanos, profesionales y empresas.

La «Agenda Digital Española» declara expresamente entre sus objetivos el refuerzo de la confianza en el ámbito digital, reconociendo que el establecimiento de un clima de confianza en el ámbito digital es un factor imprescindible para conseguir una implantación efectiva de las TIC en empresas y Administraciones y un uso más intensivo de las mismas por la ciudadanía.

INTECO ha elaborado un «*Programa de Sensibilización, Concienciación, Educación y Formación en Ciberseguridad dirigido a ciudadanos y empresas*» que proporciona cobertura a los planteamientos descritos en la «*Estrategia de Seguridad Nacional 2013»,* en la «*Agenda Digital Española»,* y en el «*Plan de Confianza Digital»* que articula dicha Agenda*,* y que tiene por objetivo reforzar la confianza digital de los ciudadanos y empresas, a través de la generación de contenidos relevantes para el público objetivo identificado y de la prestación de servicios específicos encaminados a satisfacer las necesidades de los destinatarios del programa.

La prestación efectiva de los servicios contemplados para el colectivo de ciudadanos y empresas en el programa requiere, por un lado, una actualización permanente sobre información nacional e internacional en el ámbito de la ciberseguridad, novedades legislativas, nuevas amenazas, actualizaciones y herramientas, etc.; por otro lado, la identificación, categorización y análisis de las herramientas de seguridad gratuitas de uso doméstico que sean relevantes para el usuario de internet.

1.2. OBJETO

El objeto del presente contrato es doble:

- **Servicio de monitorización y elaboración de contenidos preventivos de aspectos de ciberseguridad y confianza en ámbito digital de interés general para los ciudadanos y empresas, mediante el seguimiento de la actualidad en la materia, con**: nuevas amenazas, alertas, actualizaciones y herramientas, noticias

nacionales e internacionales en el ámbito de la ciberseguridad, novedades legislativas, servicios, iniciativas, etc.

- **Servicio de identificación, categorización y análisis de herramientas de seguridad gratuitas de uso doméstico**.

Se podrán subcontratar parte de estos servicios, no suponiendo nunca la subcontratación más del 30% del presupuesto ofertado.

1.2.1. Público objetivo

Para el servicio de monitorización y elaboración de contenidos preventivos, el público objetivo está constituido por ciudadanos usuarios de internet y por empresas principalmente, si bien gran parte de las amenazas y riesgos que hoy afectan a Internet y a las nuevas tecnologías pueden afectar a diferentes sectores y ámbitos.

El servicio de identificación, categorización y análisis de herramientas de seguridad gratuitas, por su parte, va dirigido exclusivamente a ciudadanos usuarios de internet.

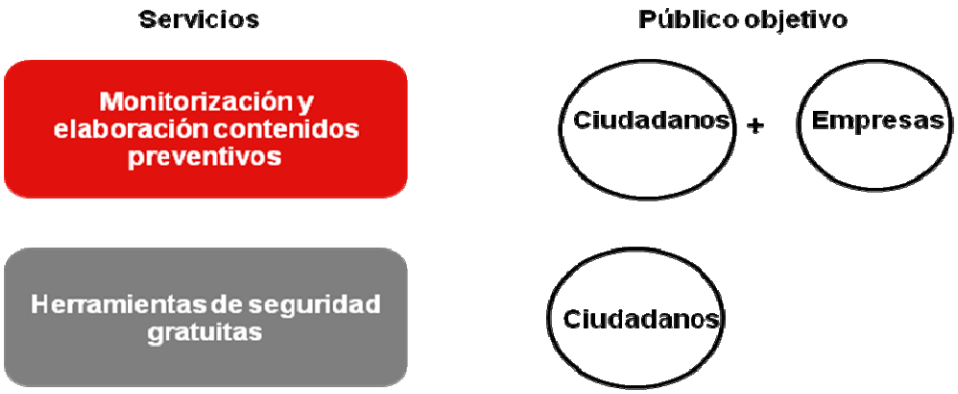

Ilustración 1: Servicios y público objetivo

Tanto los ciudadanos usuarios de Internet como las empresas son colectivos muy heterogéneos en cuanto a intensidad y tipo de usos de las nuevas tecnologías y adopción de herramientas y hábitos de seguridad. Por ello, la definición de públicos objetivos de los servicios requiere un mayor nivel de detalle.

Público objetivo 1: ciudadanos usuarios de internet

De acuerdo con una clasificación inicial facilitada por el Instituto Nacional de Estadística, 23,5 millones de ciudadanos españoles de entre 16 y 74 años utilizan internet con una frecuencia, al menos, mensual.

Con el fin de obtener una segmentación rigurosa del colectivo genérico de usuarios de Internet, se ha profundizado en el conocimiento de los usuarios a través de un análisis

clúster[1] que permite conocer las características, problemáticas y necesidades particulares de cada subgrupo. Se han identificado cuatro tipos de usuario de internet:

- usuarios hiperusuarios
- usuarios analógicos
- usuarios consumidores de ocio gratuito
- usuarios funcionales

El esquema siguiente resuelve gráficamente la descripción y peso que ocupa cada colectivo en el total de la población española.

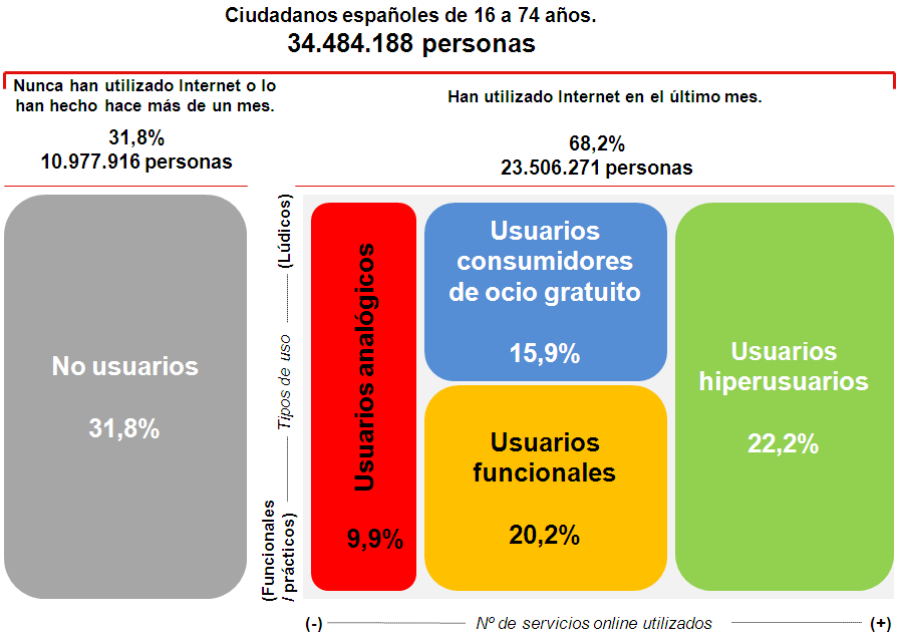

Ilustración 2: Distribución de la población española según uso de Internet; Base: Población española entre 16 y 74 años; Fuente: INE, ONTSI, INTECO

Cada uno de los servicios descritos en el presente pliego va dirigido a uno (o varios) de los usuarios anteriores.

La empresa que resulte adjudicataria recibirá información detallada de las características particulares de cada grupo de usuarios, para adaptar los contenidos, estilo y tono de comunicación a las necesidades específicas de cada segmento.

Público objetivo 2: empresas

[1] El análisis clúster es una técnica estadística multivariable que trata de dividir un conjunto de individuos en diversos sub-grupos, de modo que los nuevos conjuntos resultantes cuenten con un perfil similar. Por lo tanto, en la delimitación de los sub-grupos se fomenta al mismo tiempo la cohesión interna dentro de los grupos y la diferenciación entre grupos.

Dentro del público objetivo: empresas, tenemos que tener en cuenta por un lado empresas de gran tamaño que se les presupone con departamentos de seguridad. Así como empresas de menos de 200 empleados. En este grupo distinguiremos: aquellas que tienen baja o muy baja dependencia TIC, media o alta dependencia TIC, y aquellas que tienen muy alta dependencia TIC. Además, tenemos que tener en cuenta que dentro de estos grupos pueden existir diferentes niveles de madurez (bajo, medio y alto) en lo que a materia de seguridad se refiere.

El servicio de monitorización y elaboración de contenidos preventivos está dirigido, principalmente pero no exclusivamente, a empresas pequeñas y medianas que hacen un uso intensivo de la tecnología, es decir cuyo negocio tiene una media-alta dependencia tecnológica, pero que no tienen personal dedicado a la seguridad TIC; en general tienen presencia web (e intranets) y son por ejemplo: agencias de viajes, empresas de producción y difusión de contenidos y actividades profesionales (clínicas, despachos, gestorías...).

El servicio adecuará su lenguaje a este público. Se trata de trasladarle los conocimientos necesarios para que el empresario sepa qué servicios de seguridad necesita: mantenimiento o el alojamiento de su web, servicios cloud, etc. para que pongan las medidas pertinentes, o bien siga los pasos indicados en el aviso técnico si tiene conocimientos suficientes.

La empresa que resulte adjudicataria recibirá información detallada de las características particulares de cada grupo de usuarios, para adaptar los contenidos, estilo y tono de comunicación a las necesidades específicas de cada segmento.

1.2.2. Objetivos del programa

El objetivo general del «*Programa de Sensibilización, Concienciación, Educación y Formación en Ciberseguridad dirigido a ciudadanos y empresas*» es reforzar la confianza en el ámbito digital de ciudadanos y empresas. Por tanto, los servicios incluidos en este pliego persiguen, en última instancia, elevar la confianza de los ciudadanos y empresas en el entorno digital.

Este objetivo general se desglosa operativamente en una serie de subobjetivos, que concretan y materializan aspectos sobre los que trabajar. En concreto, los servicios de monitorización y elaboración de contenidos preventivos, e identificación, categorización y análisis de herramientas de seguridad gratuitas persiguen los siguientes subobjetivos:

- Ayudar a usuarios y empresas a llevar a cabo un cambio positivo de comportamiento en relación con la adopción de buenos hábitos de seguridad.
- Contribuir a minimizar el número y gravedad de incidencias de seguridad experimentadas por usuarios y empresas, así como aumentar la capacidad de resiliencia de las empresas.
- Facilitar que los usuarios adopten herramientas y medidas de seguridad.

2. REQUISITOS TÉCNICOS

2.1. CONSIDERACIONES PREVIAS

En este apartado se describen los servicios, características y requisitos que conforman el objeto del contrato y que el adjudicatario deberá prestar, no siendo el listado que aparece a continuación una relación exhaustiva de las características de los servicios contratados, sino las líneas generales demandadas por INTECO, cubriendo los principales aspectos a realizar y resultados esperados.

Estos requisitos deben entenderse como mínimos pudiendo los licitadores ampliarlos y mejorarlos en sus ofertas. Las propuestas que ofrezcan características inferiores y que no cubran estos mínimos, no serán tomadas en consideración en el presente procedimiento de adjudicación. El licitador puede ofertar prestaciones superiores a las solicitadas, que se considerarán positivamente en la valoración técnica de la oferta.

El adjudicatario deberá aportar los conocimientos y metodologías, así como apoyarse en las herramientas necesarias para asegurar el resultado óptimo del proyecto. El adjudicatario deberá seguir los principales estándares para cumplir con los criterios de accesibilidad universal y el diseño para todos.

El adjudicatario se obliga a guardar secreto y a hacerlo guardar al personal que emplee para la ejecución del contrato, respecto a toda la información de la Sociedad que con motivo del desarrollo de los trabajos llegue a su conocimiento, no pudiendo utilizarla para sí o para otra persona o entidad.

El servicio de identificación, categorización y análisis de herramientas de seguridad gratuitas se ofrecerá a través del nuevo portal de INTECO. Esta circunstancia podrá tener cierto impacto sobre la ejecución de los trabajos, que deberán adaptarse a las condiciones de carácter técnico y formal definidas para la nueva web. En cualquier caso, INTECO facilitará al adjudicatario los requisitos.

2.2. DESCRIPCIÓN DE LOS TRABAJOS

Los trabajos se orientan en torno a los siguientes dos servicios, cuyas particularidades se detallan en los subepígrafes 2.2.1 y 2.2.2.

- Monitorización y elaboración de contenidos preventivos, mediante el seguimiento de la actualidad en ciberseguridad y confianza digital para el colectivo de ciudadanos y empresas.
- Identificación, categorización y análisis de herramientas de seguridad gratuitas para el entorno doméstico.

Estos trabajos podrán ser subcontratados siempre que el total de la subcontratación no supere el 30% del presupuesto del proyecto.

2.2.1. Monitorización y elaboración de contenidos preventivos

La monitorización y elaboración de contenidos preventivos mediante el seguimiento de la actualidad de aspectos de ciberseguridad y confianza en el ámbito digital de interés general para los ciudadanos y empresas (nuevas amenazas, alertas, noticias nacionales e internacionales en el ámbito de la ciberseguridad, novedades legislativas, actualizaciones y herramientas, servicios, iniciativas, etc.), es clave para ofrecer a ciudadanos y empresas información actualizada y avisos de seguridad relevantes.

El servicio consiste en la identificación de las novedades tecnológicas definidas en el alcance, en el envío semanal de informes de monitorización, así como en la **remisión inmediata de comunicaciones** susceptibles de ser comunicadas de inmediato a ciudadanos y empresas (amenazas, vulnerabilidades, actualizaciones).

Ilustración 3: Servicio de monitorización de contenidos preventivos en ciberseguridad

El alcance del servicio se define del siguiente modo:

- Identificación de amenazas que constituyan un riesgo para el ciudadano o para la empresa españoles. A titulo de ejemplo, el subservicio proporcionará información sobre las siguientes amenazas:

- Campañas de malware de particular gravedad (ejemplo: virus de la policía o ramsonware).
- campañas de phishing especialmente relevantes (por su intensidad o por la novedad de su técnica).
- ataques a plataformas que comprometan la seguridad de los usuarios (ejemplo: ataques a SONY, etc.).
- amenazas específicas de marketplaces (B2B, B2C,..) y tiendas on-line.
- amenazas en redes sociales y plataformas de trabajo colaborativo de uso empresarial (Xing, LinkedIn, Yammer, SocialCast, Reseach gate, Tibbr,..).

- amenazas en plataformas de juego online o grandes fabricantes o desarroladores de juegos online de uso masivo o intensivo por usuarios de Internet.
- amenazas en servicios para interactuar con la eAdministración
- amenazas dirigidas a plataformas móviles (Android, iOS, Blackberry, Windows Phone).
- contra certificados web o relativas a pagos on-line
- que afecten a servicios cloud o a servicios de desarrollo de apps empresariales para móviles, etc.
- filtración de información (usuarios y contraseñas de acceso a servicios, etc.) en servicios como Pastebin, Datalossdb, o similar.
- campañas de *hacktivismo* de cierta relevancia.
- Otras amenazas o riesgos que afecten a servicios, herramientas, etc., que pudieran desembocar en riesgos para usuarios de los mismos.

Recopilará todas aquellas alertas que, por su novedad y dimensión, exigen inmediatez en la comunicación al ciudadano o empresa.

- Recopilación de noticias nacionales e internacionales en el ámbito de la ciberseguridad que resulten de interés a ciudadanos y/o empresas. Se considera que una noticia resulta de interés a ciudadanos y/o empresas si su comunicación al público objetivo permite crear conciencia en él acerca de un riesgo, hacerle consciente de su responsabilidad con respecto a la seguridad online y proporcionarle pautas o herramientas para la resolución del mismo.

- Recopilación de novedades legislativas y jurisprudenciales, con prioridad aquéllas que afecten a España aunque sin descartar novedades relevantes a nivel internacional, que regulen aspectos de ciberseguridad aplicables a ciudadanos y empresas: privacidad, protección de datos, ciberdelincuencia, sociedad de la información, fraude, comercio electrónico, etc.

- Recopilación de publicaciones, estudios e informes relevantes en materia de ciberseguridad, siempre referidos a los públicos objetivo del presente pliego.

- Análisis de malware. En el marco del servicio se realizará un análisis de los virus y troyanos más significativos (por su modus operandi especialmente novedoso, o por ser muy activos y virulentos en España), asegurando proporcionar al usuario la explicación de cómo eliminar dicho malware. Este servicio tendrá su reflejo en la web de INTECO. Un modelo en el que se inspirará este servicio es el de http://losvirus.es/.

- Novedades en herramientas y servicios de seguridad. La empresa que resulte adjudicataría recopilará las nuevas herramientas y aplicaciones de seguridad de interés para los públicos objetivo, o las novedades en cuanto a prestaciones o funcionalidades, con una explicación de las necesidades que satisface la herramienta en cuestión. En el caso de

herramientas de seguridad de carácter gratuito, este servicio enlaza con el servicio descrito en el punto 2.

En este caso, el servicio contemplará no solo la monitorización, sino también los **trabajos de investigación oportunos** para confirmar la gravedad, relevancia y oportunidad del aviso.

Este servicio alimentará el canal "Avisos de seguridad" de la Web de INTECO, que tiene por objetivo informar al usuariode la existencia de amenazas concretas y actuales que pueden afectar a su equipo, junto con consejos para su prevención y reacción.

- **Información sobre vulnerabilidades y «0 day»** que puedan afectar a la seguridad del usuario básico. En concreto, se considerarán las vulnerabilidades que afecten a los productos más utilizados por el ciudadano. De manera no exhaustiva, se incluyen en el alcance del subservicio, al menos los siguientes productos:

Para el colectivo ciudadanos, al menos:

- Microsoft: Windows, Windows Media Player, Internet Explorer (navegador), Outlook.
- Apple: Mac, Safari (navegador), iTunes, QuickTime, iPhone iOS,
- Oracle: Java Runtime Enviroment.
- Adobe: Flash, Reader, Acrobat, Shockwave
- Google: Chrome (navegador), Android (móviles, tabletas, etc).
- Mozilla: Firefox (navegador), Thunderbird.
- Opera: Opera (navegador).

Para el colectivo empresas, al menos:

- Desarrollo Web:
  - Generadores de páginas web (Dreamweaver,...)
  - Gestores de contenidos web / CMS: Wordpress, Joomla, Drupal,...
  - Paquetes de software asociados a servidores web AMP/LAMP/WAMP/MAMP (Linux, Windows, Machintosh, Apache, MySQL, PHP, PERL, PHYTON)
- Software de gestión empresarial:
  - Facturación, Contabilidad, CRM, ERP (Navision,...), gestión documental, intranets,... (Sharepoint, SAP...)
- Equipos de red y de seguridad
  - switches, routers, antivirus, cortafuegos, backup, cifrado...
- Otros:
  - Sistemas operativos puestos de trabajo (Windows XP, W7, W8,...)

- Sistemas operativos / sw de servidores (aplicaciones, correo electrónico, ficheros, ...)
- Suites de oficina o herramientas ofimáticas: Microsoft Office (Word, Access, Excel, Visio, PowerPoint...), Open office, …
- Sistemas de bbdd
- Gestores de correo electrónico (Outlook, Thunderbird, ...)
- Navegadores y Java, JRE
- Adobe
- S.O. y apps empresariales para Móviles y tabletas (redes sociales, herr. de trabajo colaborativo,...)
- Sistemas de almacenamiento, impresoras en red,..

En este caso, el servicio contemplará no solo la monitorización, sino también los trabajos de investigación oportunos para confirmar la gravedad, relevancia y oportunidad del aviso.

Este servicio alimentará el canal "Avisos de seguridad" de la Web de INTECO, que tiene por objetivo informar al usuario de la existencia de amenazas concretas y actuales que pueden afectar a su equipo, junto con consejos para su prevención y reacción.

- Actualizaciones de los productos más utilizados por el ciudadano y las empresas. El objetivo es informar de la última actualización de los productos y facilitar pautas para ayudar al usuario a averiguar qué versión está utilizando y para configurar la actualización automática. De manera no exhaustiva, se incluyen en el alcance del subservicio, al menos, los siguientes productos:

Para el colectivo ciudadanos, al menos:

- Microsoft: Windows, Windows Media Player, Internet Explorer (navegador), Outlook.
- Apple: Mac, Safari (navegador), iTunes, QuickTime, iPhone iOS,
- Oracle: Java Runtime Enviroment.
- Adobe: Flash, Reader, Acrobat, Shockwave
- Google: Chrome (navegador), Android (móviles, tabletas, etc.).
- Mozilla: Firefox (navegador), Thunderbird.
- Opera: Opera (navegador).

Para el colectivo empresas, al menos:

- Desarrollo Web:
  - Generadores de páginas web (Dreamweaver,...)
  - Gestores de contenidos web / CMS: Wordpress, Joomla, Drupal,...

  - Paquetes de software asociados a servidores web AMP/LAMP/WAMP/MAMP (Linux, Windows, Machintosh, Apache, MySQL, PHP, PERL, PHYTON)

- Software de gestión empresarial:
  - Facturación, Contabilidad, CRM, ERP (Navision,...), gestión documental, intranets,... (Sharepoint, SAP...)
- Equipos de red y de seguridad
  - switches, routers, antivirus, cortafuegos, backup, cifrado...
- Otros:
  - Sistemas operativos puestos de trabajo (Windows XP, W7, W8,...)
  - Sistemas operativos / sw de servidores (aplicaciones, correo electrónico, ficheros, ...)
  - Suites de oficina y herramientas ofimáticas: Microsoft Office (Word, Access, Excel, Visio, PowerPoint...), Open office, …
  - Sistemas de bbdd
  - Gestores de correo electrónico (Outlook, Thunderbird, ...).
  - Navegadores y Java, JRE
  - Adobe
  - S.O. y apps empresariales para Móviles y tabletas (redes sociales, herr. de trabajo colaborativo,...)
  - Sistemas de almacenamiento, impresoras en red,..

2.2.1.1. Volumen

- Cantidad: variable, según la frecuencia del contenido. A modo orientativo, se establecen las siguientes cantidades, al menos:
  - Noticias: 20 noticias mensuales.
  - Novedades legislativas: 2 novedades mensuales.
  - Publicaciones: 2 informes mensuales.
  - Malware: 4 o 5 virus mensuales.
  - Herramientas de seguridad: 4 o 5 novedades mensuales.
  - Amenazas: 4 o 5 amenazas mensuales.
  - Vulnerabilidades: 4 o 5 vulnerabilidades mensuales.
  - Actualizaciones: 4 o 5 actualizaciones mensuales.
- Extensión: variable, según contenido.

2.2.1.2. Hitos

- Mes 1: Aprobación del modelo de trabajo: definición de esquema y enfoque del informe de monitorización, definición de los procesos para la comunicación de avisos urgentes, identificación de fuentes.
- Mes 2 a 12: Envío periódico de los informes de monitorización.
- Mes 2 a 12: Envío de avisos de seguridad: amenazas, vulnerabilidades y actualizaciones. Este servicio no responde a una periodicidad fija, se procederá a comunicarlo de manera inmediata en cuanto se detecte la alerta.

2.2.1.3. Interacciones

Se definirá en la reunión de lanzamiento el proceso de trabajo y los flujos de comunicación.

2.2.1.4. Entregables

- Informes de monitorización, que recogerán las novedades de noticias, novedades legislativas, publicaciones, malware y herramientas de seguridad. Los informes vendrán acompañados de toda la información complementaria relevante (enlaces, imágenes, etc.).
- Avisos y alertas de seguridad puntuales, en número variable, cada vez que se detecte una amenaza, malware o actualización cuya comunicación requiere actuación inmediata. Los avisos vendrán acompañados de toda la información complementaria relevante (principalmente imágenes, pantallazos, etc.)

2.2.2. Identificación, categorización y análisis de herramientas de seguridad gratuitas

En la actual web de INTECO y de OSI existe una sección de “Útiles gratuitos”, que enlaza a la descarga de distintas herramientas de seguridad gratuitas. (Ver: http://cert.inteco.es/software/Proteccion/utiles_gratuitos/ y http://www.osi.es/es/recursos/utiles-gratuitos).

Este servicio tiene por objetivo sentar las bases para una nueva sección de “Herramientas de seguridad gratuitas”, sencilla y usable, que permita al usuario decidir qué herramientas necesita (categoría) y cuál/es utilizar (marca).

Para ello, se configura un servicio que ofrecerá una relación de categorías de herramientas de seguridad de utilidad para el ciudadano doméstico (antivirus, anti-espías, analizadores de URL, herramientas de control parental, etc.). El servicio asegurará una descripción clara y pormenorizada de cada una de las categorías de herramientas, que incluirá aspectos como, por ejemplo, cuál es la utilidad de la herramienta, contra qué riesgos protege y en qué casos es recomendable su utilización. *(En la fase de diagnóstico de las necesidades de los usuarios de Internet españoles se concluye que entre los usuarios con menos conocimientos se aprecia un elevado desconocimiento, o al menos falta de certeza sobre las herramientas*

de seguridad: desconocen para qué sirven muchas herramientas, no saben si su antivirus posee funcionalidades adicionales, etc.).

Una vez que el ciudadano sabe qué tipo de herramienta necesita, puede acceder a una batería de herramientas gratuitas dentro de cada categoría. Para cada una de ellas, se ofrecerán las siguientes variables de análisis (a título de ejemplo):

- Denominación de la herramienta.
- Sistema/s operativo/s con los que funciona.
- Si se trata de una herramienta gratuita de manera permanente o si existe un período limitado de prueba gratuita y, en este caso, a cuánto asciende dicho período.
- Idioma.
- Prestaciones adicionales. En la actualidad, las herramientas de seguridad tienden a incorporar diferentes funcionalidades, lo que hace imposible definir categorías estancas. (por ejemplo, los antivirus incorporan antiespías). Por ello, la solución que se propone es un sistema de etiquetado de cada herramienta. El campo "Prestaciones adicionales" recogerá todas las etiquetas aplicables a cada una.
- Valoración. Sistema de valoración de las herramientas a partir de las votaciones de los usuarios. *(Esta circunstancia es irrelevante para el adjudicatario).*
- Descarga. Enlace a la página oficial de descarga. (Tener en cuenta que, para dispositivos móviles, deberá enlazarse al market oficial.)
- Videotutorial. Enlace al vídeo donde se proporcionan pautas para su instalación. La realización del videotutorial no está incluido en el alcance del pliego; sí está incluida la localización de videotutoriales suministrados por el fabricante donde se facilita al usuario las instrucciones de instalación o actualización.

Los trabajos esperados son, por tanto, los siguientes:

- Diseño del servicio: establecimiento de categorías, definición de aspectos a analizar de cada herramienta.
- Análisis de herramientas: la empresa adjudicataria realizará un análisis de las herramientas detectadas que recogerá una valoración de la efectividad real de las mismas.
- Mantenimiento y actualización, para asegurar la vigencia de los contenidos en todo momento.

2.2.2.1. Volumen

- Cantidad: aproximadamente, 80 herramientas de seguridad.
- Extensión: no aplica.

2.2.2.2. Hitos

- Meses 1 y 2:
  - Propuesta y aprobación de las categorías de herramientas.
  - Propuesta y aprobación de la batería de herramientas a analizar. Podrá considerarse como punto de partida las herramientas actualmente publicadas en la sección "Útiles gratuitos" de OSI y de INTECO-CERT, más las nuevas herramientas detectadas a través del servicio de monitorización.
  - Propuesta y aprobación de modelo de "Informe de análisis de herramientas".
- Meses 3 y 4: Análisis de herramientas. En esta fecha se debe haber realizado la valoración de, al menos, 20 herramientas de seguridad gratuitas.
- Meses 5 a 12: Análisis de herramientas (aproximadamente, 60 herramientas de seguridad). Mantenimiento y actualización del servicio.

2.2.2.3. Interacciones

No aplica.

2.2.2.4. Entregables

- Informe de análisis de herramientas (aprox. 80).

2.3. EQUIPO DE TRABAJO

2.3.1. Composición

Teniendo en cuenta los servicios descritos en el epígrafe 2.2., la empresa adjudicataria aportará el equipo y los recursos técnicos adecuados para la realización de los trabajos definidos.

Entre los miembros del equipo propuesto, el adjudicatario aportará necesariamente la figura de un Jefe de Proyecto o Coordinador, que constituirá el enlace con INTECO a efectos de interlocución.

2.3.2. Perfil técnico del equipo de trabajo

Los profesionales que, como equipo principal, sean responsables de la ejecución del trabajo, deberán disponer de la cualificación, experiencia y titulación adecuadas a la naturaleza de los trabajos. Se considera que, de manera global, el equipo debe contar con las siguientes competencias y conocimientos:

- **Conocimientos técnicos en ciberseguridad**.
- **Experiencia en monitorización y elaboración de contenidos.**
- **Experiencia en vigilancia tecnológica.**
- **Competencias técnicas en análisis de herramientas de seguridad.**

El equipo de trabajo deberá contar con la formación adecuada para desempeñar las tareas y servicios del mismo. **Las ofertas de empresas licitadoras que no estén en condiciones de acreditar estos conocimientos mínimos y necesarios, no serán consideradas en el concurso**.

En la valoración de estas competencias, se prestará atención especialmente a la acreditación que presente la empresa licitadora para justificar su conocimiento (titulaciones oficiales, experiencia y certificaciones que aporten los miembros del equipo).

El equipo de trabajo propuesto por el licitador deberá garantizar en su conjunto la cobertura de todas las competencias anteriores.

El **Jefe de Proyecto** designado por la empresa adjudicataria deberá ejercer de **coordinación e interlocución** permanente durante la ejecución del contrato **sin perjuicio de otras funciones establecidas dentro de los servicios del presente pliego** como parte del equipo de trabajo. El Jefe de Proyecto aportará al menos 5 años de experiencia en gestión de proyectos, de los cuáles al menos 2 en proyectos de seguridad.

2.4. MEDIOS TÉCNICOS APORTADOS POR INTECO

En relación con los medios materiales, INTECO pondrá a disposición del adjudicatario los siguientes medios técnicos o materiales lo que se permite un control por parte de INTECO y una ejecución eficiente y eficaz de los trabajos:

- **OpenKM:** Herramienta para la gestión de documentación.

3. METODOLOGÍA

Las empresas licitadoras detallarán la metodología de trabajo que proponen. En cualquier caso, las metodologías propuestas deben estar alineadas con los siguientes aspectos:

- Evaluación y mejora constante.
- Rigor en la identificación de fuentes de monitorización y en el trabajo de investigación posterior de avisos de seguridad.
- Método de trabajo basado en la reflexión y búsqueda de excelencia.
- Fluidez en la comunicación cliente – proveedor.

4. PLANIFICACIÓN

La planificación definitiva del proyecto se determinará a partir de la reunión de lanzamiento. Los siguientes subepígrafes detallan una primera aproximación temporal a la ejecución del proyecto.

Las empresas licitadoras aportarán en su oferta una propuesta de planificación del proyecto.

4.1. REUNIÓN DE LANZAMIENTO

La reunión de lanzamiento se celebrará dentro de las dos semanas siguientes a la adjudicación del contrato.

Esta reunión dará comienzo efectivo a la ejecución de los trabajos. En la reunión se abordarán los siguientes temas:

- Presentación de los equipos de trabajo de INTECO y del adjudicatario.
- Identificación de perfiles y roles de cada miembro del equipo.
- Presentación de la metodología a usar por el adjudicatario en cuanto a organización y seguimiento de los trabajos, gestión de riesgos y gestión del cambio que garantice la calidad y efectividad del proyecto.
- Revisión de la propuesta de planificación presentada en la oferta (la planificación definitiva se determinará la primera quincena del contrato de forma conjunta con INTECO).
- Cualquier otro punto de interés para el proyecto.

4.2. REUNIONES DE SEGUIMIENTO

Se celebrarán reuniones de seguimiento con periodicidad mensual entre la empresa adjudicataria e INTECO. El objetivo de estas reuniones es la realización de un seguimiento periódico de las tareas asociadas al contrato, el análisis de posibles desviaciones y, en su caso, la propuesta de medidas correctivas.

Las reuniones podrán celebrarse de manera presencial en las instalaciones de INTECO o a través de videoconferencia u otros medios telemáticos.

En cada una de dichas reuniones se revisará el *Informe Técnico de Seguimiento*, que será elaborado por la empresa adjudicataria con carácter mensual, y constituye uno de los entregables del proyecto. El informe recogerá, al menos, los siguientes aspectos:

- Grado de cumplimiento de los trabajos e hitos establecidos para cada uno de los servicios.
- En su caso, relación de riesgos detectados que puedan comprometer el cumplimiento de los objetivos e hitos marcados, así como una propuesta de acciones para su mitigación o eliminación.
- Indicadores de referencia.

- Trabajos realizados en cada área y en cada proyecto por parte del personal técnico, así como los resultados obtenidos.
- Trabajos planificados para el siguiente periodo y objetivos que se pretenden cumplir para cada uno de los servicios.
- Identificación de mejoras que se puedan aplicar para el cumplimiento de los objetivos del servicio.
- Grado de avance económico por partidas del contrato.
- Cualquier otro punto de interés para el proyecto.

Además de la celebración de reuniones periódicas mensuales, INTECO podrá solicitar la celebración de reuniones de coordinación con periodicidad semanal, que se celebrarán igualmente en las instalaciones de INTECO o a través de medios telemáticos.

Además el adjudicatario deberá elaborar toda la documentación necesaria en base a las distintas actuaciones objeto del contrato. Toda actividad debe quedar perfectamente documentada y registrada.

INTECO podrá determinar los procedimientos y herramientas a utilizar para poder llevar a cabo la planificación, seguimiento y control del proyecto.

4.3. CIERRE DEL PROYECTO Y MEMORIA FINAL

A la finalización del proyecto, la empresa adjudicataria presentará una *Memoria Final*, que constituye uno de los entregables del proyecto. Este documento constituye un informe justificativo del alcance efectivo de los trabajos realizados, con detalle de entregables, recursos consumidos, objetivos e hitos conseguidos, lecciones aprendidas y propuesta de recomendaciones de actividades y objetivos a alcanzar en el servicio en los siguientes meses.

Junto con la Memoria Final, la empresa adjudicataria entregará una relación con toda la documentación generada, para que INTECO pueda hacerse cargo de los servicios y herramientas que son objeto de este pliego con garantías.

5. DIRECCIÓN Y SEGUIMIENTO DE LOS TRABAJOS

Corresponde a la Dirección Técnica del proyecto la completa supervisión y dirección de los trabajos, la propuesta de las modificaciones convenientes o, en su caso, la propuesta de la suspensión de los mismos si existiese causa suficientemente motivada.

Para la supervisión de la marcha de los trabajos, INTECO indicará al comienzo del proyecto la persona designada como Director/a Técnico/a del proyecto. Sus funciones en relación con el presente Pliego serán:

a) Velar por el adecuado cumplimiento de los servicios contratados.

b) Emitir las certificaciones parciales de recepción de los mismos.

c) Fijar reuniones periódicas entre la Sociedad y el adjudicatario con el fin de determinar, analizar y valorar las incidencias que, en su caso, se produzcan durante la ejecución del contrato.

Independientemente de las reuniones ya establecidas en el Plan de Proyecto, el Director de Proyecto podrá convocar cuantas reuniones de seguimiento del proyecto considere oportunas para asegurar el cumplimiento del calendario del proyecto así como la correcta consecución de los objetivos propuestos. El adjudicatario será responsable de la redacción y distribución de las correspondientes actas de reunión.

Con el fin de garantizar que se satisfacen las necesidades y prioridades establecidas por el Director de Proyecto, este marcará las directrices de los trabajos a realizar, siendo estas directrices de obligado cumplimiento por parte del adjudicatario.

Durante el desarrollo del proyecto se podrán solicitar, como parte de las tareas de seguimiento y control, entregas intermedias que permitan tanto la verificación del trabajo realizado, como reducir y evitar riesgos a lo largo del proyecto.

La rectificación de los trabajos no aceptados no se computará como horas de trabajo realizadas por el adjudicatario.

Las rectificaciones derivadas de decisiones sobrevenidas que no tengan como origen errores u omisiones del adjudicatario se computarán y abonarán como horas de trabajo dentro del proyecto.

6. FORMA DE EJECUCIÓN

6.1. LUGAR DE REALIZACIÓN DE LOS TRABAJOS

El centro habitual de trabajo serán las oficinas de la propia empresa, manteniendo en su caso una conexión remota con la infraestructura informática de INTECO descrita en el apartado 2.4. Medios técnicos aportados por INTECO, así como reuniones en remoto o presenciales que se indiquen por INTECO.

6.2. CONTROL DE CALIDAD

Sin perjuicio de las obligaciones asumidas en su oferta, el adjudicatario, a través del supervisor designado a tal efecto, deberá seguir los procedimientos de aseguramiento de la calidad existentes en la ejecución del contrato.

El adjudicatario reconoce el derecho de la Sociedad para examinar por medio de auditores, externos o propios, el fiel cumplimiento de los trabajos por él realizados.

INTECO tendrá derecho a llevar a cabo auditorías de las actividades de los adjudicatarios para asegurarse de que la ejecución de los trabajos se lleva de acuerdo con lo establecido en el presente Pliego. Todo el material e información requerida para dichas inspecciones y auditorías por los representantes de la Sociedad estará disponible sin restricciones. La Sociedad notificará al adjudicatario con dos semanas de antelación la auditoría y con un día de antelación la inspección a realizar, y el adjudicatario tendrá la obligación de:

- Facilitar el acceso al material solicitado por el grupo auditor.
- Designar personas responsables que acompañen a los auditores.
- Facilitar un entorno de trabajo adecuado en el mismo lugar en que tiene lugar la auditoría.
- Cooperar con el auditor.
- Participar en las reuniones que convoque el auditor.
- Analizar los datos encontrados para que el informe sea real.
- Emprender rápidamente acciones correctoras y/o preventivas.
- Emitir una respuesta oficial para cada uno de los defectos que haya detectado el grupo de auditores.

6.3. OBLIGACIONES DE INFORMACIÓN Y DOCUMENTACIÓN

Durante la ejecución de los trabajos objeto del contrato, el adjudicatario se compromete, en todo momento, a facilitar a las personas designadas por el Director Técnico, la información y documentación que éstas soliciten para disponer de un pleno conocimiento de las circunstancias en que se desarrollan los trabajos, así como de los eventuales problemas que puedan plantearse y de las tecnologías, métodos y herramientas utilizados para resolverlos.

Asimismo, el adjudicatario estará obligado a asistir y colaborar, a través del personal que designe a este propósito, en las reuniones de seguimiento del proyecto definidas por el Director Técnico, quién se compromete a citar con la debida antelación al personal del adjudicatario.

Como parte de las tareas objeto del contrato, el adjudicatario se compromete a generar la documentación de los trabajos realizados, de acuerdo con los criterios que establezca en cada caso el Director de Proyecto. Toda la documentación generada por el adjudicatario durante la ejecución del contrato será propiedad exclusiva de INTECO sin que el contratista pueda conservarla, ni obtener copia de la misma o facilitarla a terceros sin la expresa autorización por escrito de INTECO, que la concederá, en su caso y con expresión del fin, previa petición formal del adjudicatario.

En este sentido, el adjudicatario deberá informar al Director Técnico sobre distintos aspectos relacionados con el funcionamiento y la calidad de los servicios prestados. Entre ellos será necesario presentar un informe, en el formato y con la periodicidad que defina el Director Técnico, de cumplimiento de los servicios y que contendrá entre otros los siguientes puntos, si proceden:

- Trabajos realizados y resultados obtenidos en el período vigente.
- Trabajos planificados para el siguiente periodo.
- Identificación de mejoras que se puedan aplicar para el cumplimiento de los objetivos de los proyectos en los que esté involucrado.

Salvo indicación expresa en contrario, las especificaciones, informes, diagramas, planos, dibujos y cualquier otro documento relativo al objeto del contrato, serán aportados en castellano, cualquiera que sea el soporte y/o formato utilizado para la transmisión de información.

El adjudicatario proporcionará, sin coste adicional para la Sociedad, una copia en soporte informático portátil (CD-ROM, DVD, llave USB, etc.) con toda la documentación generada durante la prestación de los servicios objeto del contrato.

6.4. HITOS DE FACTURACIÓN

Se definen los siguientes hitos de facturación:

- Hito 1: Cierre del diseño de servicios (20%): Mes 2.
- Hito 2: Elaboración de los primeros materiales y contenidos (5%): Mes 3.
- Hito 3: Elaboración de resto de materiales y contenidos (40%): Esta cantidad se abonará mensualmente, del siguiente modo:
    - Mes 4: 5%.
    - Mes 5: 5%.
    - Mes 6: 5%

- Mes 7: 5%
- Mes 8: 5%
- Mes 9: 5%
- Mes 10: 5%
- Mes 11: 5%

- Hito 4: Cierre de proyecto (35%). Mes 12.

La facturación de los trabajos realizados se efectuará sobre la base de una adecuada prestación del servicio por parte del adjudicatario, en la que mediante reporte mensual el mismo informe a INTECO de la consecución de los diferentes objetivos.

En las reuniones periódicas se evaluarán todas aquellas incidencias habidas que se hubieran originado en el cumplimiento de los objetivos planificados. Cuando a juicio del Director Técnico, tales incidencias fueran imputables al adjudicatario, por falta de responsabilidad, incompetencia, desidia u otras causas de índole similar, avisará al departamento Económico-Financiero de INTECO y la facturación resultante quedará minorada por el importe que corresponda de acuerdo a las penalizaciones establecidas en el presente Pliego.

7. PRESENTACIÓN DE LAS OFERTAS TÉCNICAS

7.1. DATOS GENERALES

La presentación de la documentación para su admisión como licitador supone la aceptación de lo dispuesto en la Instrucción de Contratación de la Sociedad incluida en el Perfil de Contratante y publicada en la web, así como todas las disposiciones del presente Pliego.

De todos los datos que se aporten por el licitador, INTECO podrá exigir la correspondiente justificación documental o aclaraciones antes de la adjudicación, condicionando ésta a que dicha justificación o aclaraciones sean suficientes a juicio de la Sociedad.

En el sobre nº 2 no debe recogerse la oferta económica, pues es un criterio de adjudicación cuantificable; solo deben incluirse los documentos técnicos expresados en el punto siguiente. La inclusión en el sobre nº 2 de los documentos que deben constar en el sobre nº 3 es causa de exclusión.

7.2. FORMATO DE LA PROPUESTA TÉCNICA (SOBRE Nº 2)

Los licitadores deberán presentar una propuesta técnica que deberá contener los siguientes apartados y en el mismo orden:

7.2.1. Descripción de los servicios

Este apartado tendrá **una extensión máxima de 30 páginas** y deberá incluir:

- **I.** Visión general sobre el proyecto.
- **II.** Visión particular de cada uno de los dos servicios incluidos en el marco del contrato (epígrafes 2.2.1 y 2.2.2). En concreto:
    - a. Monitorización y elaboración de contenidos preventivos.
        - i. Descripción general del servicio.
        - ii. Metodología de trabajo específica para el servicio donde se mencione, al menos:
            1. Relación de fuentes disponibles, públicas y/o privadas, para llevar a cabo la monitorización y vigilancia de cada uno de los contenidos incluidos en el alcance del servicio.
            2. Procedimiento de investigación de amenazas y vulnerabilidades para confirmar su envergadura y la oportunidad o no de la creación de un aviso de seguridad.
            3. Procedimiento de comunicación de amenazas, vulnerabilidades y actualizaciones que exijan inmediatez en su comunicación a ciudadanos y empresas.
        - iii. Propuesta de planificación para la ejecución de los trabajos.

iv. Propuesta de métricas de calidad.

v. Modelos o ejemplo de un contenido:

1. Informe de monitorización: esquema general, recomendaciones en cuanto a contenido y periodicidad, descripción del tratamiento propuesto para cada uno de los servicios.
2. Comunicación de una amenaza.
3. Comunicación de una vulnerabilidad.
4. Comunicación de una actualización.

b. Identificación, categorización y análisis de herramientas de seguridad gratuitas.

i. Descripción general del servicio.

ii. Metodología de trabajo específica para el servicio donde se mencione, al menos:

1. Procedimiento propuesto para el análisis y valoración de las herramientas de seguridad.
2. Procedimiento propuesto para asegurar la actualización constante del servicio.

iii. Propuesta de planificación para la ejecución de los trabajos.

iv. Propuesta de métricas de calidad.

v. Modelo o ejemplo de un Informe de análisis de herramientas.

A la hora de formular esta propuesta deberán tener en cuenta los criterios a valorar conforme al Anexo VI.

7.2.2. Cronograma

La oferta incluirá una propuesta de planificación global de los trabajos y servicios, teniendo en cuenta los requisitos definidos en el apartado 2.

7.2.3. Equipo de trabajo

Deberán describirse los perfiles del equipo de profesionales y los medios propuestos por el licitador en el proyecto.

El Jefe de Proyecto no se incluirá en el equipo de trabajo al ser examinado en el apartado de solvencia técnica.

Se valorará, la composición global del equipo, de manera que cubran las necesidades descritas en el epígrafe 2.3.2. Perfil técnico del equipo de trabajo.

Con objeto de homogenizar la presentación de las diferentes ofertas, la empresa licitadora incluirá en el epígrafe “Equipo de trabajo” dos tablas:

- En la primera tabla mencionará, para cada uno de los perfiles profesionales que compongan el equipo, qué competencias posee (sí / no)

- En la segunda tabla mencionará, para cada uno de los perfiles profesionales que compongan el equipo, de qué manera se acredita dicha competencia. La acreditación podrá consistir en: titulación, tiempo de experiencia, certificaciones de seguridad (ISACA, ISC2, EC-COUNCIL, SANS, etc.), etc.

Competencias (sí / no)	Perfil 1	Perfil 2	…	Perfil n
Conocimientos técnicos en ciberseguridad.				
Experiencia en monitorización y elaboración de contenidos preventivos.				
Experiencia en vigilancia tecnológica				
Competencias técnicas en análisis de herramientas.				

Acreditación de las competencias (título, tiempo de experiencia, certificaciones, etc.)	Perfil 1	Perfil 2	…	Perfil n
Conocimientos técnicos en ciberseguridad.				
Experiencia en monitorización y elaboración de contenidos preventivos.				
Experiencia en vigilancia tecnológica.				
Competencias técnicas en análisis de herramientas.				

8. CRITERIOS DE VALORACIÓN

La puntuación correspondiente a la calidad técnica de las ofertas presentadas se determinará según los criterios recogidos en el correspondiente apartado del Pliego de Características Generales. Ver ANEXO VI Criterios de Valoración del Pliego de Características Generales

Vº Bº DIRECTOR GENERAL

INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN, S.A.