

5 - 06 - 19

ENTRADA

PLIEGO DE PRESCRIPCIONES TÉCNICAS

**SERVICIO DE RENOVACIÓN, SOPORTE Y
AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO
KEEP IT SECURE 24 PARA LA PROTECCIÓN
CONTÍNUA DE SISTEMAS DE INFORMACIÓN
PUBLICADOS EN INTERNET**

**PROCEDIMIENTO NEGOCIADO SIN PUBLICIDAD
NO ARMONIZADO AL PRECIO MÁS BAJO**

Nº CONTRATO: 125/2019

Área: Planificación, Control y Seguridad

Fecha: 30 de Mayo de 2.019

Índice

1. Alcance	3
1.1. Objeto del contrato	3
1.2. Servicios Incluidos en el Contrato	3
1.3. Otras condiciones del servicio	4
2. Requisitos Técnicos del Servicio	5
3. Requisitos de Seguridad.....	8
4. Formato de las Especificaciones Técnicas	11

Empresa Canal de Isabel II, S.A.	Proyecto SERVICIO DE RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET CONTRATO 125/2019	Fecha 30/05/2019
Elaborado por Área de Planificación, Control y Seguridad	Documento Pliego de Prescripciones Técnicas	Versión V00

1. Alcance

1.1. Objeto del contrato

El objeto del contrato es la renovación de las suscripciones del servicio online en modo SaaS y llave en mano KEEP-IT-SECURE-24 contratadas actualmente por Canal de Isabel II, S.A. (en adelante Canal) y la posible ampliación de suscripciones de dicho servicio, incluyendo soporte a los mismos por parte del proveedor durante el periodo de vigencia del contrato.

Este servicio cubrirá la auditoría continua y pruebas de penetración para los sistemas de Canal de Isabel II, S.A. publicados en Internet, y la evaluación de forma continua la infraestructura, redes de información, servidores y servicios de Canal de Isabel II publicados en Internet de forma regular y constante.

1.2. Servicios Incluidos en el Contrato

Los Servicios objeto del contrato son los que se detallan a continuación:

- **S1. Servicio de Renovación de suscripciones:** consistente en la renovación de las suscripciones que tenga contratadas Canal, incluyendo soporte a los servicios por parte del proveedor durante el periodo de vigencia del contrato. El número de estas suscripciones oscilará entre 2 y 3 en función de las contratadas por Canal previo al inicio de la prestación del servicio objeto de este contrato.
- **S2. Servicio de ampliación de suscripciones:** consistente en la contratación de nuevas suscripciones al servicio con el fin de cubrir las futuras necesidades, incluyendo soporte a los servicios por parte del proveedor durante el periodo de vigencia del contrato.
 - El crecimiento mínimo esperado es de 2 ó 3 suscripciones (en función del número de partida) más para los años 2 y 3, hasta llegar a 8 suscripciones contratadas por Canal.
 - El crecimiento máximo estimado prevé un aumento de 1 ó 2 (en función del número de partida), 6 y 5 suscripciones respectivamente para cada año de vigencia del contrato, pudiendo llegar a un máximo de 15 suscripciones contratadas por Canal.

Al ser una estimación, para 7 de las suscripciones, este servicio será opcional y se solicitará a decisión únicamente de Canal.

Empresa Canal de Isabel II, S.A.	Proyecto SERVICIO DE RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET CONTRATO 125/2019	Fecha 30/05/2019
Elaborado por Área de Planificación, Control y Seguridad	Documento Pliego de Prescripciones Técnicas	Versión V00

1.3. Otras condiciones del servicio

Debido a la naturaleza del contrato (renovación de suscripciones, ampliación de suscripciones y soporte y mantenimiento de suscripciones de software SaaS) no aplican como requerimientos específicos las consideraciones sociales, ambientales y de innovación, más allá de lo establecido como condiciones especiales de ejecución en el apartado 9.3 del Anexo I del Pliego de Cláusulas Administrativas Particulares.

Empresa Canal de Isabel II, S.A.	Proyecto SERVICIO DE RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET CONTRATO 125/2019	Fecha 30/05/2019
Elaborado por Área de Planificación, Control y Seguridad	Documento Pliego de Prescripciones Técnicas	Versión V00

2. Requisitos Técnicos del Servicio

2.1 Alcance Técnico

El alcance técnico del servicio cubrirá los siguientes requisitos:

- Servicio Llave en Mano de Persistent Pen-Testing en servidores y aplicaciones para la volumetría definida por Canal, entre 8 y 15 aplicaciones.
- Evaluar la Infraestructura, Redes, Servidores, Servicios y Aplicaciones de forma regular y constante.
- Integrar los Tests de Seguridad en el Proceso de Gestión de Cambios, que contribuya a tener una seguridad reforzada en aplicaciones y servidores antes de la entrada en producción.
- Reducir significativamente los niveles de riesgo a través de un servicio de testeo continuado por un equipo experimentado de Pen-Testers.
- Disponer de un servicio competitivo basado en el modelo KEEP-IT-SECURE-24.
- Beneficiarse de una Plataforma de Gestión de Vulnerabilidades Online que proporciona organización, información y gestión de los resultados reportados.
- Interactuar directamente con el equipo de consultores especialistas, lo cual permitirá un proceso de Pen-Test más eficiente y efectivo.
- Incorporar las lecciones aprendidas, gestionar KPIs y acelerar la resolución de incidentes explotando los outputs guardados en la Plataforma.
- Asegurar la corrección de las vulnerabilidades mediante el servicio de re-Test.

KEEP-IT-SECURE24 proporcionará un equipo de profesionales certificados de alta cualificación que evalúen la seguridad de los sistemas y aplicaciones de Canal de un modo regular y persistente, y proporcionará el acceso a una plataforma de gestión, que permita medir, gestionar y mitigar vulnerabilidades, permitiendo a Canal reducir sus riesgos de modo real y significativo.

2.2 Servicios Previstos

La propuesta de servicios previstos incluirá un alcance flexible en cuanto a volumetría, que podrá ir variando a lo largo de los 3 años de contrato.

- Alcance Técnico: desde 2 APP's a un máximo de 15 APP's
- HackUnits (mínimo mensual): desde 7.200 HU's hasta 35.825 HU's

Empresa Canal de Isabel II, S.A.	Proyecto SERVICIO DE RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET CONTRATO 125/2019	Fecha 30/05/2019
Elaborado por Área de Planificación, Control y Seguridad	Documento Pliego de Prescripciones Técnicas	Versión V00

Los servicios previstos serán los siguientes:

- Pen-Testing regular
- Plataforma de gestión Web
- Número de usuarios de la plataforma: sin límite
- Gestión integrada de las correcciones
- Testeo manual
- Métricas Online
- Reporting

2.3 Entregables

El adjudicatario proporcionará a Canal los siguientes entregables:

- Prestación de Servicios de “Persistent Security Testing” que proporcionará el reporting, las especificaciones de las vulnerabilidades encontradas, recomendaciones para su corrección y retesting post-resolución.
- Una sesión de trabajo Trimestral por video/teleconferencia para discutir los resultados y reorientar objetivos y prioridades.
- Acceso a la Plataforma Online de Gestión de Vulnerabilidades, que permita acceder a la información de vulnerabilidades y gestionarlas.
- Generación de informes y extracción de métricas relacionadas con el Servicio a través de la Plataforma de Servicio.
- Gestión de las prioridades de testeo y de peticiones de pruebas específicas de acuerdo a los procedimientos establecidos.

2.4 Niveles de Soporte

El adjudicatario presentará propuesta de tipos y niveles de Servicio del Soporte teniendo en cuenta los siguientes requisitos.

- Primer nivel de soporte: Dado por el adjudicatario del contrato, partner del fabricante. Él responderá llamadas o emails y los reenviará al siguiente nivel si no encuentra la solución por sí mismo.
- Segundo nivel de soporte: Integrity como fabricante, atenderá y resolverá incidencias que el partner no puede resolver: bug fixing, parches, etc.

Empresa Canal de Isabel II, S.A.	Proyecto SERVICIO DE RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET CONTRATO 125/2019	Fecha 30/05/2019
Elaborado por Área de Planificación, Control y Seguridad	Documento Pliego de Prescripciones Técnicas	Versión V00

Cobertura del servicio:

- Actualizaciones de la versión en curso.
- Parches o correcciones de las versiones instaladas.
- Fallos del servicio.

Métodos de contacto:

- Soporte telefónico.
- Email
- Tickets de soporte

Las horas de atención del soporte serán de 9:00 AM a 6:00 PM, de Lunes a Viernes.

La gestión de las incidencias se realizará en función de la gravedad de la mismas. Los tiempos de respuesta son los que se detallan continuación, aunque podrán depender de la disponibilidad de acceso a las máquinas, logs, etc. para el análisis y resolución de las incidencias.

- Incidencia Crítica/Alta: 2 horas
- Incidencia Media: 8 horas
- Incidencia Baja: 2 días laborables
- Petición de servicio: 2 semanas

Empresa Canal de Isabel II, S.A.	Proyecto SERVICIO DE RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET CONTRATO 125/2019	Fecha 30/05/2019
Elaborado por Área de Planificación, Control y Seguridad	Documento Pliego de Prescripciones Técnicas	Versión V00

3. Requisitos de Seguridad

El proveedor de servicios Cloud deberá garantizar, al menos, que para el servicio o los servicios Cloud contratados por Canal de Isabel II, S.A.:

- a) El acceso se produce exclusivamente bajo un protocolo que cifre de forma robusta los datos transmitidos entre el cliente y el servidor, con el objeto de garantizar su confidencialidad e integridad (por ejemplo, uso exclusivo de TLS 1.2 o superior, y utilizando sólo suites de cifrado robustas para evitar vulnerabilidades de tipo BEAST (RC4), Lucky13 (RC4), POODLE (SSL 3.0 y TLS 1.0), CRIME (TLS 1.0 compression), SWEET32 (3DES), Logjam (intercambio de claves de menos de 2048 en DH), DROWN (TLS 1.x con soporte a SSLv2), etc.).
- b) El uso de un esquema de BBDD propio para la información propiedad de Canal de Isabel II, S.A.
- c) Que dicho esquema de BBDD sea accedido única y exclusivamente por el/los usuarios de aplicación que vayan a ser utilizados en la conexión del servicio Cloud a dicho esquema de BBDD.
- d) Cifrado robusto de los datos propiedad de Canal de Isabel II, S.A. en la propia BBDD y modelo (cifrado completo o cifrado del dato).
- e) Almacenamiento de los datos de autenticación de los usuarios (por ejemplo, el par usuario/contraseña) en la BBDD mediante el uso de funciones resumen (hash) robustas (al menos, SHA-256) conjuntamente con la obligación de utilizar contraseñas complejas (longitud mínima de 10 caracteres, con obligatoriedad de utilizar caracteres alfanuméricos (mezcla de mayúsculas, minúsculas y números) y no alfanuméricos (por ejemplo, signos de puntuación y ortográficos)). Es obligatorio el uso de funciones de derivación de claves basadas en contraseña (Password-Based Key Derivation Functions) para el almacenamiento de las contraseñas (por ejemplo, PBKDF2).
- f) Exista la posibilidad de uso de:
 - a. Un esquema XML para el intercambio de datos de autenticación y autorización (por ejemplo, SAML 2.0) e implementaciones de seguridad a nivel del mensaje.
 - b. OAuth 2.0 u OpenID Connect como modelos de autorización segura para consumo de servicios web.
 - c. SCIM como modelo para automatizar el intercambio de información de identidad de los usuarios entre distintos dominios de identidad.
- g) Exista la posibilidad de habilitar un segundo factor de autenticación (2FA) para garantizar la identidad de los usuarios del servicio, ya sea mediante el uso de certificados electrónicos

Empresa Canal de Isabel II, S.A.	Proyecto SERVICIO DE RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET CONTRATO 125/2019	Fecha 30/05/2019
Elaborado por Área de Planificación, Control y Seguridad	Documento Pliego de Prescripciones Técnicas	Versión V00

reconocidos (como, por ejemplo, DNle), contraseñas de un único uso (OTP), uso de tokens (hardware o software), etc.

h) Todas las funciones de la aplicación relacionadas con la autenticación, la gestión de las sesiones y la autorización (control del acceso) han sido auditadas contra estándares de seguridad internacionalmente reconocidos (por ejemplo, OWASP) para comprobar que existen y que han sido implementadas correctamente.

i) Se almacena de forma segura (garantía de acceso, recuperación y no modificación) y se revisa de forma regular el registro de eventos de las actividades de los usuarios (errores y eventos de seguridad). Estos registros deberán mantenerse al menos durante cinco (5) años.

j) Comunicará inmediatamente a Canal de Isabel II, S.A. acerca de todas aquellas vulnerabilidades reportadas de forma privada o hechas públicas que afecten a sus sistemas y de las acciones que están siendo llevadas a cabo para eliminar o mitigar dichas vulnerabilidades.

El acceso a un servicio proporcionado por un proveedor de servicios Cloud será siempre a través del software dispuesto en la maqueta corporativa instalada en un equipo corporativo (fijo o portátil). No se accederá a través de clientes pesados proporcionados por terceros, incluyendo el software proporcionado por el propio proveedor de servicios Cloud.

Canal de Isabel II, S.A. realizará las siguientes gestiones, a través de la correspondiente solicitud de acceso cursada en la aplicación corporativa de solicitudes e incidencias, para garantizar a los usuarios de Canal de Isabel II, S.A. autorizados el acceso al servicio Cloud a través de:

1. El control de acceso a través de pertenencia a grupos de usuarios en el Directorio Activo.
2. Los permisos que sean necesarios en los sistemas corporativos de control de acceso existentes.

En este punto, el proveedor de servicios Cloud deberá proporcionar, al menos, la siguiente información:

1. Requisitos técnicos para el acceso al servicio o servicios Cloud que proporciona y que hayan sido contratados por Canal de Isabel II, S.A.
2. Requisitos de ancho de banda de acceso a Internet para la parte cliente.
3. Usuarios de prueba con las autorizaciones estrictamente necesarias, para poder realizar correctamente las verificaciones que correspondan (funcionales, técnicas, de seguridad, etc.).

El servicio prestado por el proveedor de servicios Cloud, por defecto, no se integrará de ninguna manera con los Sistemas de Información de Canal de Isabel II, S.A. En caso de que desde la Subdirección de Sistemas Informáticos se estime la viabilidad de una posible integración, con objeto de poder evaluar la dimensión y el alcance de la misma, se revisarán, al menos, los siguientes puntos:

Empresa Canal de Isabel II, S.A.	Proyecto SERVICIO DE RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET CONTRATO 125/2019	Fecha 30/05/2019
Elaborado por Área de Planificación, Control y Seguridad	Documento Pliego de Prescripciones Técnicas	Versión V00

- Funcionamiento del proveedor de servicios Cloud (certificaciones, niveles de madurez, procesos, etc.).
- Posibilidades técnicas y costes de integración con los sistemas de información de Canal de Isabel II, S.A. (tecnologías, seguridad, etc.), teniendo en cuenta la infraestructura tecnológica y de comunicaciones de Canal de Isabel II, S.A.
- Nivel de control que el negocio tendrá sobre los servicios Cloud proporcionados.
- Nivel de seguridad implementado por el proveedor de servicios Cloud.
- Nivel de dependencia y requisitos del servicio corporativo de Internet.

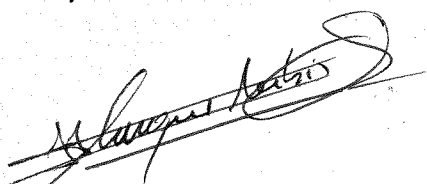
Dicha evaluación se recogerá en un informe que será entregado al Comité de Coordinación de Seguridad de la Información (en adelante, CCSI) para su conocimiento y correspondiente evaluación. Sólo en caso de aceptación por parte del CCSI se procederá a informar cumplidamente al dueño de los datos para su autorización final y, sólo entonces, se iniciarán las tareas de la integración, que se englobarán dentro de un proyecto y serán gestionadas como tal, siguiendo la metodología de gestión de proyectos adoptada por Canal de Isabel II, S.A.

Empresa Canal de Isabel II, S.A.	Proyecto SERVICIO DE RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET CONTRATO 125/2019	Fecha 30/05/2019
Elaborado por Área de Planificación, Control y Seguridad	Documento Pliego de Prescripciones Técnicas	Versión V00

4. Formato de las Especificaciones Técnicas

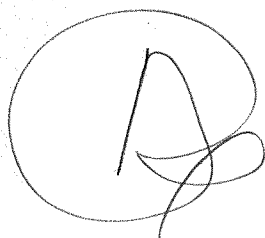
La oferta técnica se atenderá al formato establecido en el apartado 6 del Anexo I del Pliego de Cláusulas Administrativas del presente procedimiento.

Mayo de 2019



Enrique Rubio Donis

Jefe del Área de Planificación, Control y Seguridad



Ángel Rodríguez García

Subdirector de Sistemas Informáticos



Pablo Galán González

Director de Recursos

