

**PLIEGO DE PRESCRIPCIONES TÉCNICAS**

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

**Nº CONTRATO: 149/2022**

# Índice

<b>1. Alcance</b> .....	<b>3</b>
1.1. Objeto del contrato .....	3
1.2. Servicios Incluidos en el Contrato.....	3
1.3. Otras condiciones del servicio .....	3
<b>2. Requisitos Técnicos del Servicio</b> .....	<b>4</b>
<b>3. Requisitos de Seguridad</b> .....	<b>7</b>
<b>4. Formato de las Especificaciones Técnicas</b> .....	<b>9</b>

<b>Empresa</b> Canal de Isabel II, S.A.	<b>Proyecto</b> <b>RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET</b> <b>CONTRATO 149/2022</b>	<b>Fecha</b> 26/05/2022
<b>Elaborado por</b> Área de Planificación, Control y Seguridad	<b>Documento</b> Pliego de Prescripciones Técnicas	<b>Versión</b> 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 9 y 11 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 11 suscripciones contratadas por Canal.
  - El crecimiento máximo estimado prevé un aumento de 4 suscripciones respectivamente para el segundo y tercer año de vigencia del contrato, pudiendo llegar a un máximo estimado de 19 suscripciones contratadas por Canal.

Al ser una estimación, para 8 de las suscripciones, este servicio será opcional y se solicitará a decisión únicamente de Canal.

### 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.

<b>Empresa</b> Canal de Isabel II, S.A.	<b>Proyecto</b> <b>RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET</b> <b>CONTRATO 149/2022</b>	<b>Fecha</b> 26/05/2022
<b>Elaborado por</b> Área de Planificación, Control y Seguridad	<b>Documento</b> Pliego de Prescripciones Técnicas	<b>Versión</b> 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 testeado 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 9 APP's a un máximo de 20 APP's
- Test de Intrusión Persistente para hasta de 9 a 20 IPs y de 9 a 20 apps aplicaciones.
- Esfuerzo estimado: de 20.778 hasta 39.939 Hack Units

Los servicios previstos serán los siguientes:

- Pen-Testing regular
- Plataforma de gestión Web

<b>Empresa</b> Canal de Isabel II, S.A.	<b>Proyecto</b> <b>RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET</b> <b>CONTRATO 149/2022</b>	<b>Fecha</b> 26/05/2022
<b>Elaborado por</b> Área de Planificación, Control y Seguridad	<b>Documento</b> Pliego de Prescripciones Técnicas	<b>Versión</b> V00

- Número de usuarios de la plataforma: sin límite
- Gestión integrada de las correcciones
- Testeo manual
- Métricas Online
- Reporting

En función del ámbito definido, el modelo de servicio que se requiere es el plan denominado *Custom*.

	Custom
Ámbito Tecnológico	De 9 a 19 Apps
HackUnits (Mínimo Mensual)	20778 hasta 38220
Test de Intrusión	✓
Plataforma de Web Gestión	✓
Número máximo de Usuarios Plataforma	Ilimitado
Integración con Gestión de Modificaciones	✓
Ingeniería Social (1)	✓
Resiliencia Ataques 0 Day (2)	✓
Testes Manuales	✓
Métricas Online	✓
Informe	✓
Sesión de Trabajo Mensual 2 Horas (3)	✓

### 2.3 Entregables

El adjudicatario, mediante el servicio Keep-IT-Secre 24 proporcionará a Canal los siguientes entregables:

- Reporte de pruebas de seguridad persistentes que proporcionarán informes, hallazgos de vulnerabilidad, recomendaciones de corrección y re-testing después de la resolución.
- 
- Una sesión de trabajo mensual (online) con el objetivo de debatir los resultados y redefinir los objetivos y prioridades.

<b>Empresa</b> Canal de Isabel II, S.A.	<b>Proyecto</b> <b>RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET</b> <b>CONTRATO 149/2022</b>	<b>Fecha</b> 26/05/2022
<b>Elaborado por</b> Área de Planificación, Control y Seguridad	<b>Documento</b> Pliego de Prescripciones Técnicas	<b>Versión</b> V00

- Acceso a la plataforma on-line de gestión de vulnerabilidades, para recibir y gestionar las vulnerabilidades.
- Obtención de informes y métricas relacionados con el servicio a través de la plataforma de servicios.
- Proporcionar información sobre las prioridades a evaluar y solicitar pruebas específicas de acuerdo con el proceso de gestión de cambios de la organización.
- Gestión de las prioridades de testeo y de peticiones de pruebas específicas conforme 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.

### 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

<b>Empresa</b> Canal de Isabel II, S.A.	<b>Proyecto</b> <b>RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET</b> <b>CONTRATO 149/2022</b>	<b>Fecha</b> 26/05/2022
<b>Elaborado por</b> Área de Planificación, Control y Seguridad	<b>Documento</b> Pliego de Prescripciones Técnicas	<b>Versión</b> 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.:

- disponer de certificación del Esquema Nacional de Seguridad nivel medio
- O**
- garantizar los requisitos de seguridad relacionados a continuación:
    - a) El acceso se produce exclusivamente bajo un protocolo seguro que cifre de forma robusta los datos transmitidos entre el cliente y el servidor, con el objeto de garantizar su confidencialidad, integridad y disponibilidad
    - 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 utilizando al menos un generador de números pseudoaleatorios basado en HMAC-SHA1, 5.000 iteraciones para la parte cliente y 100.000 iteraciones para la parte servidora)
    - f) Exista la posibilidad de uso de:
      - 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.
      - OAuth 2.0 como framework de autorización y OpenID Connect (OIDC) como protocolo de autenticación en las APIs existentes.
      - SCIM como modelo para automatizar el intercambio de información de identidad de los usuarios entre distintos dominios de identidad RS007.
    - g) Exista la posibilidad de habilitar al menos un segundo factor de autenticación (2FA) para garantizar la identidad de los usuarios del servicio, ya sea mediante el uso de certificados electrónicos 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, WASC) para comprobar que existen y que han sido implementadas correctamente

<b>Empresa</b> Canal de Isabel II, S.A.	<b>Proyecto</b> <b>RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET</b> <b>CONTRATO 149/2022</b>	<b>Fecha</b> 26/05/2022
<b>Elaborado por</b> Área de Planificación, Control y Seguridad	<b>Documento</b> Pliego de Prescripciones Técnicas	<b>Versión</b> V00

- i) Se almacenará de forma segura (garantía de acceso, recuperación y no modificación) y se revisará 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) El proveedor 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, así de las acciones que están siendo llevadas a cabo para eliminar o mitigar dichas vulnerabilidades



<b>Empresa</b> Canal de Isabel II, S.A.	<b>Proyecto</b> <b>RENOVACIÓN, SOPORTE Y AMPLIACIÓN DE SUSCRIPCIONES DEL SERVICIO KEEP IT SECURE 24 PARA LA PROTECCIÓN CONTÍNUA DE SISTEMAS DE INFORMACIÓN PUBLICADOS EN INTERNET</b> <b>CONTRATO 149/2022</b>	<b>Fecha</b> 26/05/2022
<b>Elaborado por</b> Área de Planificación, Control y Seguridad	<b>Documento</b> Pliego de Prescripciones Técnicas	<b>Versión</b> 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.

Firmado electrónicamente por  
JESUS PLAZA RUBIO  
el día 19-09-2022 11:00:33

Jefe del Área de Planificación, Control y Seguridad

Firmado electrónicamente por  
ÁNGEL RODRÍGUEZ GARCÍA  
el día 19-09-2022 11:02:28

Subdirector de Sistemas Informáticos

Firmado electrónicamente por  
MÓNICA FIERRO MARTÍN  
el día 19-09-2022 12:40:23

Directora de Recursos