

PLIEGO DE PRESCRIPCIONES TÉCNICAS

**SERVICIO DE RENOVACIÓN DE LAS
SUSCRIPCIONES DEL SISTEMA AVANZADO
DE PROTECCIÓN INFORMÁTICA CORTEX
XDR DE PALO ALTO PARA CANAL DE
ISABEL II, S.A.**

CONTRATO Nº: 121/2021

Área: **Planificación, Control y Seguridad**

Empresa Canal de Isabel II, S.A.	Proyecto Servicio de renovación de las suscripciones del sistema avanzado de protección informática CORTEX XDR de Palo Alto para Canal de Isabel II, S.A.	
Elaborado por Área de Planificación, Control y Seguridad	Documento Pliego de Prescripciones Técnicas	Versión V1.0

Índice

1. Antecedentes.....	3
2. Alcance.....	4
2.1. Alcance Técnico	4
2.2. Mantenimiento de Licencias	4
2.3. Soporte Técnico.....	5
2.4. Requisitos de Seguridad para productos Cloud.....	6
3. Formato de las especificaciones técnicas	13

<p>Empresa</p> <p>Canal de Isabel II, S.A.</p>	<p>Proyecto</p> <p>Servicio de renovación de las suscripciones del sistema avanzado de protección informática CORTEX XDR de Palo Alto para Canal de Isabel II, S.A.</p>	
<p>Elaborado por</p> <p>Área de Planificación, Control y Seguridad</p>	<p>Documento</p> <p>Pliego de Prescripciones Técnicas</p>	<p>Versión</p> <p>V1.0</p>

1. Antecedentes

La Subdirección de Sistemas Informáticos (en adelante SSI) de Canal de Isabel II, S.A. (en adelante Canal) gestiona toda la infraestructura informática y de puesto de trabajo. Esta gestión incluye un sistema de protección avanzada tanto de servidores como de equipos de cliente (PC's y portátiles) ante ataques locales que no pasan por cortafuegos y de amenazas intrusión en los sistemas que no son identificados a nivel de firmas de antivirus por no haberse visto antes.

En Canal se eligió la solución TRAPS de Palo Alto para cubrir esta necesidad fundamentada en que era uno de los líderes del mercado. Por este motivo se realizó durante 2017 un piloto de la herramienta en Canal siendo el resultado satisfactorio, al igual que la experiencia de implantación y explotación en los entornos productivos desde 2018, manteniendo este tipo de sistemas como una de las recomendaciones derivadas dentro del ámbito de mejora de la seguridad de la información.

El producto TRAPS ha evolucionado a uno nuevo denominado CORTEX XDR (Detección y Respuesta eXtendida *eXtended Detection and Response* en inglés), del mismo fabricante, Palo Alto, Inc. que dispone de mejores prestaciones que el primero. Este producto presenta dos versiones, Cortex XDR prevent y Cortex XDR PRO, las mayores prestaciones de la versión PRO ha llevado a la decisión de proponer la contratación del producto COTEX XDR PRO.

Empresa Canal de Isabel II, S.A.	Proyecto Servicio de renovación de las suscripciones del sistema avanzado de protección informática CORTEX XDR de Palo Alto para Canal de Isabel II, S.A.	
Elaborado por Área de Planificación, Control y Seguridad	Documento Pliego de Prescripciones Técnicas	Versión V1.0

2. Alcance

2.1. Alcance Técnico

Los servicios para contratar se detallan a continuación:

4943 suscripciones de CORTEX XDR PRO de Palo Alto con un crecimiento estimado del 10%

Para garantizar tanto la disponibilidad de las nuevas versiones de este software como recibir atención en caso de incidencias se considera necesario el servicio de mantenimiento y soporte para todos los productos CORTEX XDR PRO incluidos en el servicio durante la duración del contrato.

El alcance por lo tanto de este contrato es el siguiente:

1. Suscripciones del Software incluido en el servicio.
2. Acceso al cloud de Palo Alto para la administración y explotación del servicio.
3. Mantenimiento y Soporte del software.

Para los servicios prestados en modalidad *cloud (Software as a Service)* se deberán cumplir los requisitos de seguridad detallados en el apartado 2.4 de este documento.

2.2. Mantenimiento de Licencias

El mantenimiento de las licencias le proporcionará el fabricante independientemente de la posible mediación del adjudicatario.

Para los componentes que se instalen en la infraestructura de Canal, el fabricante tiene que:

Empresa Canal de Isabel II, S.A.	Proyecto Servicio de renovación de las suscripciones del sistema avanzado de protección informática CORTEX XDR de Palo Alto para Canal de Isabel II, S.A.	
Elaborado por Área de Planificación, Control y Seguridad	Documento Pliego de Prescripciones Técnicas	Versión V1.0

- Proporcionar la última versión liberada del software, y libre de vulnerabilidades conocidas o reportadas.
- Notificar proactivamente a Canal de Isabel II, S.A. los posibles problemas de seguridad en los productos, así como de la descripción técnica detallada del problema en cuanto tengan conocimiento de ellos.
- Notificar también la disponibilidad de los parches o nuevas versiones que los solucionaran los posibles problemas, incluyendo fechas.

2.3. Soporte Técnico

El Soporte Técnico será proporcionado directamente por el fabricante del software independientemente de los servicios que en este aspecto pueda prestar el adjudicatario. El soporte técnico debe incluir al menos:

- Registro y administración de activos
- Creación y administración de casos de soporte
- Obtención de conocimientos y respuestas a preguntas: Acceso a la documentación y base de datos de conocimientos (incidencias y problemas conocidos, buenas prácticas, etc.) de los productos incluidos en el contrato.
- Acceso completo a la comunidad en vivo
- Acceso a nuevas versiones.
- Acceso a parches o fixes.
- Soporte sobre la configuración y el uso de la herramienta.

Empresa Canal de Isabel II, S.A.	Proyecto Servicio de renovación de las suscripciones del sistema avanzado de protección informática CORTEX XDR de Palo Alto para Canal de Isabel II, S.A.	
Elaborado por Área de Planificación, Control y Seguridad	Documento Pliego de Prescripciones Técnicas	Versión V1.0

2.4. Requisitos de Seguridad para productos Cloud

Los servicios que se proporcionen en modalidad *Cloud*, deberán cumplir los requisitos técnicos de seguridad que se detallan a continuación.

<p>Empresa</p> <p>Canal de Isabel II, S.A.</p>	<p>Proyecto</p> <p>Servicio de renovación de las suscripciones del sistema avanzado de protección informática CORTEX XDR de Palo Alto para Canal de Isabel II, S.A.</p>	
<p>Elaborado por</p> <p>Área de Planificación, Control y Seguridad</p>	<p>Documento</p> <p>Pliego de Prescripciones Técnicas</p>	<p>Versión</p> <p>V1.0</p>

Aspectos técnicos de seguridad mínimos a tener en cuenta	Requisitos	Cuando aplica
<p>Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del anexo A ISO/IEC 27001:2013 (ISO/IEC 27002:2013):</p> <p>9.2.4. Gestión de información confidencial de autenticación de usuarios.</p> <p>9.3.1.1. Uso de información confidencial para la autenticación.</p> <p>9.4.1. Restricción del acceso a la información.</p> <p>9.4.2. Procedimientos seguros de inicio de sesión.</p> <p>13.1.1.1. Controles de red.</p> <p>13.1.2. Mecanismos de seguridad asociados a servicios en red.</p>	<p>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 (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 compresión), SWEET32 (3DES), Logjam (intercambio de claves de menos de 2048 en DH), DROWN (TLS 1.x con soporte a SSLv2), etc.).</p> <p>b) Todos los formularios, incluidos los de inicio de sesión, tienen que estar protegidos contra ataques de fuerza bruta (uso de CAPTCHA, disociación de los campos “usuario” y “contraseña” en pasos distintos, pero dependientes y controlados, dentro del proceso de inicio de sesión, etc.) y tienen que controlar completamente los caracteres introducidos por el usuario para evitar ataques de tipo Cross-Site Scripting, Cross-Site Request Forgery (CSRF), Remote File Inclusion (RFI), Remote Code Execution (RCE), inyección SQL, etc</p>	<p>Siempre</p>
<p>Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del anexo A ISO/IEC 27001:2013 (ISO/IEC 27002:2013):</p> <p>9.2.1. Gestión de altas/bajas de usuarios</p> <p>9.2.2. Gestión de los derechos de acceso asignados a usuarios</p> <p>9.2.5. Revisión de los derechos de acceso de los usuarios.</p> <p>9.2.6. Retirada o adaptación de los derechos de acceso</p> <p>9.4.1. Restricción del acceso a la información</p>	<p>c) El uso de un esquema de BBDD propio para la información propiedad de Canal de Isabel II, S.A.</p> <p>d) 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.</p>	<p>Siempre, en base a la clasificación de los activos de información dentro del alcance de los servicios cloud a contratar por parte de Canal de Isabel II, S.A.</p>

Empresa Canal de Isabel II, S.A.	Proyecto Servicio de renovación de las suscripciones del sistema avanzado de protección informática CORTEX XDR de Palo Alto para Canal de Isabel II, S.A.	
	Documento Pliego de Prescripciones Técnicas	Versión V1.0
Elaborado por		
Área de Planificación, Control y Seguridad		

Aspectos técnicos de seguridad mínimos a tener en cuenta	Requisitos	Cuando aplica
Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del anexo A ISO/IEC 27001:2013 (ISO/IEC 27002:2013): 10.1.1. Política de uso de los controles criptográficos. 10.1.2. Gestión de claves criptográficas.	e) 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)	Siempre
Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del anexo A ISO/IEC 27001:2013 (ISO/IEC 27002:2013): 10.1.1.1. Política de uso de los controles criptográficos. 10.1.2. Gestión de claves criptográficas.	f) Almacenamiento de todos los datos de autenticación de los usuarios en la BBDD mediante el uso de funciones criptográficas seguras 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)), establecer un período máximo de vigencia y validez de las contraseñas (recomendado un máximo de 60 días) y de implementar un histórico de contraseñas (con un mínimo de 6). Es obligatorio el uso de funciones de derivación de claves basadas en contraseña (<i>Password-Based Key Derivation Functions</i>) para el almacenamiento de las contraseñas consideradas como seguras (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, versiones modernas de bcrypt con un <i>work factor</i> de al menos 12, versiones modernas no vulnerables de Argon2 (Argon2d), etc.)	Siempre

Empresa Canal de Isabel II, S.A.	Proyecto	
	Servicio de renovación de las suscripciones del sistema avanzado de protección informática CORTEX XDR de Palo Alto para Canal de Isabel II, S.A.	
Elaborado por Área de Planificación, Control y Seguridad	Documento	
	Pliego de Prescripciones Técnicas	Versión V1.0

Aspectos técnicos de seguridad mínimos a tener en cuenta	Requisitos	Cuando aplica
<p>Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del anexo A ISO/IEC 27001:2013 (ISO/IEC 27002:2013):</p> <p>9.2.4. Gestión de información confidencial de autenticación de usuarios. 9.3.1. Uso de información confidencial para la autenticación. 9.4.1. Restricción del acceso a la información. 9.4.2. Procedimientos seguros de inicio de sesión. 13.1.1. Controles de red. 13.1.2. Mecanismos de seguridad asociados a servicios en red.</p>	<p>g) Exista la posibilidad de uso de:</p> <ul style="list-style-type: none">• 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 <p>h) En caso de existir Web Services que puedan ser consumidos desde Canal de Isabel II, S.A., deben estar securizados a nivel de mensaje, especificando la forma de firmar y cifrar los mensajes de tipo SOAP, a través de la especificación WS-Security. Por tanto:</p> <ul style="list-style-type: none">• Los servicios deben estar autenticados, preferentemente con WS-Security Tokens• Los usuarios deben ser autenticados vía SAML 2.0.• La integridad de la información ha de estar garantizada a través del uso de protocolos seguros (HTTPS 1.2 o superior) o vía WS-Signature.• El no repudio debe estar garantizado a través del uso de WS-Signature o WS-Addressing.• La confidencialidad de la información ha de estar garantizada a través del uso de protocolos seguros (HTTPS 1.2 o superior) o vía WS-Encryption.• Debe hacerse uso de una política de seguridad (WS-Policy).	<p>Siempre que:</p> <ul style="list-style-type: none">• exista la posibilidad de integrar la autenticación y/o la autorización del servicio con proveedores de identidad de terceros• existencia de APIs que puedan ser consumidas

<p>Empresa</p> <p>Canal de Isabel II, S.A.</p>	<p>Proyecto</p> <p>Servicio de renovación de las suscripciones del sistema avanzado de protección informática CORTEX XDR de Palo Alto para Canal de Isabel II, S.A.</p>	
<p>Elaborado por</p> <p>Área de Planificación, Control y Seguridad</p>	<p>Documento</p> <p>Pliego de Prescripciones Técnicas</p>	<p>Versión</p> <p>V1.0</p>

Aspectos técnicos de seguridad mínimos a tener en cuenta	Requisitos	Cuando aplica
<p>Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del anexo A ISO/IEC 27001:2013 (ISO/IEC 27002:2013):</p> <p>9.2.4. Gestión de información confidencial de autenticación de usuarios.</p> <p>9.3.1. Uso de información confidencial para la autenticación.</p> <p>9.4.1. Restricción del acceso a la información.</p> <p>9.4.2. Procedimientos seguros de inicio de sesión.</p> <p>13.1.1. Controles de red.</p> <p>13.1.2. Mecanismos de seguridad asociados a servicios en red.</p>	<p>i) Exista la posibilidad de habilitar al menos un segundo factor de autenticación (2FA) para garantizar la identidad de los usuarios del servicio, yasea mediante el uso de certificados electrónicos reconocidos (como, por ejemplo, DNle), contraseñas de un único uso (OTP), uso de tokens (hardware o software), etc.</p>	<p>Siempre</p>
<p>Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del Anexo A ISO/IEC 27001:2013 (ISO/IEC 27002:2013):</p> <p>12.6.1. Gestión de las vulnerabilidades técnicas.</p> <p>12.6.2. Restricciones en la instalación de software</p> <p>18.2.1. Revisión independiente de la seguridad de la información.</p> <p>18.2.2. Cumplimiento de las políticas y normas de seguridad.</p> <p>18.2.3. Comprobación del cumplimiento.</p>	<p>j) 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</p>	<p>Siempre</p>

<p>Empresa</p> <p>Canal de Isabel II, S.A.</p>	<p>Proyecto</p> <p>Servicio de renovación de las suscripciones del sistema avanzado de protección informática CORTEX XDR de Palo Alto para Canal de Isabel II, S.A.</p>	
<p>Elaborado por</p> <p>Área de Planificación, Control y Seguridad</p>	<p>Documento</p> <p>Pliego de Prescripciones Técnicas</p>	<p>Versión</p> <p>V1.0</p>

Aspectos técnicos de seguridad mínimos a tener en cuenta	Requisitos	Cuando aplica
<p>Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del Anexo A ISO/IEC 27001:2013 (ISO/IEC 27002:2013):</p> <p>12.4.1. Registro y gestión de eventos de actividad</p> <p>Pueden existir requisitos legales adicionales en lo relativo a la conservación de los registros y eventos. Consultar con el DPD.</p>	<p>k) 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</p>	<p>Siempre</p>

Empresa Canal de Isabel II, S.A.	Proyecto		Versión V1.0
	Servicio de renovación de las suscripciones del sistema avanzado de protección informática CORTEX XDR de Palo Alto para Canal de Isabel II, S.A.		
Elaborado por Área de Planificación, Control y Seguridad	Documento		
	Pliego de Prescripciones Técnicas		

Aspectos técnicos de seguridad mínimos a tener en cuenta	Requisitos	Cuando aplica
Evaluación objetiva del requisito en base a los dominios, objetivos de control y controles del Anexo A ISO/IEC 27001:2013 (ISO/IEC 27002:2013): 12.6.1. Gestión de las vulnerabilidades técnicas. 12.6.2. Restricciones en la instalación de software 18.2.1. Revisión independiente de la seguridad de la información. 18.2.2. Cumplimiento de las políticas y normas de seguridad. 18.2.3. Comprobación del cumplimiento.	1) 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	Siempre

Empresa Canal de Isabel II, S.A.	Proyecto Servicio de renovación de las suscripciones del sistema avanzado de protección informática CORTEX XDR de Palo Alto para Canal de Isabel II, S.A.	
Elaborado por Área de Planificación, Control y Seguridad	Documento Pliego de Prescripciones Técnicas	Versión V1.0

3. Formato de las especificaciones técnicas

Las especificaciones técnicas se atenderán al formato establecido en el apartado 6 del Anexo I del Pliego de Cláusulas Administrativas del presente procedimiento.

Firmado electrónicamente por
 Jesús Plaza Rubio
 el día 24-05-2021 14:01:07

Firma: Jefe Área Proponente, Jesús Plaza Rubio
 ÁREA DE PLANIFICACIÓN, CONTROL Y SEGURIDAD

Firmado electrónicamente por
 Ángel Rodríguez García
 el día 25-05-2021 09:55:34

Firma: Subdirector de SISTEMAS INFORMÁTICOS Ángel Rodríguez García
 SUBDIRECCIÓN SISTEMAS INFORMÁTICOS

Firmado electrónicamente por
 Mónica Fierro Martín
 el día 25-05-2021 12:01:36

Firma: Directora de RECURSOS Mónica Fierro Martín
 DIRECCIÓN DE RECURSOS