

INFORME SOBRE LA MODIFICACIÓN NO PREVISTA QUE SE PROPONE EFECTUAR EN EL CONTRATO SUSCRITO EL 15 DE ENERO DE 2021 ENTRE RADIO TELEVISIÓN MADRID, S.A.U. (en lo sucesivo, RTVM) e ICA INFORMÁTICA Y COMUNICACIONES AVANZADAS S.L. (en lo sucesivo ICA)

I.- Consideraciones previas

En el mes de septiembre de 2020, RTVM convocó una solicitud pública de ofertas para la contratación del Servicio Gestionado de Mantenimiento y Soporte de Seguridad Perimetral a tres (3) años conforme a las necesidades descritas en los Pliegos de Prescripciones Técnicas que rigieron dicha licitación.

Tras recibirse una (1) oferta, de la empresa ICA, se procedió a su análisis y valoración, comprobándose que su propuesta daba cobertura a todos los requerimientos objeto del alcance. Posteriormente, la Comisión de Contratación propuso como adjudicataria a la empresa ICA.

El contrato entró en vigor el 15 de enero de 2021, siendo su alcance el descrito en los Pliegos de Condiciones Jurídicas y Técnicas que se adjuntan al mismo.

II.- Descripción de la necesidad de la modificación contractual

Escenario

Durante la mañana del 6 de octubre de 2023, se pudo constatar que ciertos sistemas informáticos sufrían claros problemas de funcionamiento y en algunos casos mostraban una nota de rescate unida al cifrado masivo de ficheros.

De forma preventiva, el personal de la Subdirección de Sistemas restringió las comunicaciones en las redes afectadas, evitando con ello un daño mayor en el resto de sus activos y procedió al apagado de todos los sistemas para limitar las acciones del atacante y evitar una posible propagación del incidente.

Ese mismo día, el equipo de respuesta a incidentes de Telefónica Tech (**DFIR Team**: Digital Forensics & Incident Response | Cybersecurity & Cloud) fue activado, de forma coordinada con el equipo de ICA y el propio equipo de la Subdirección de Sistemas de RTVM, y se creó un grupo de trabajo mixto que comenzó a facilitar las actuaciones de contención bajo el asesoramiento mediante distintos puntos de control del equipo de DFIR.

RTVM ha ido siguiendo una secuencia preestablecida de pasos destinados a contener y erradicar la amenaza, por un lado, y a sentar las bases para el restablecimiento de los servicios principales en los que se apoyan sus operaciones actualmente, por otro.

Medidas de contención y erradicación

En términos generales, las principales medidas tomadas el día del incidente y ejecutadas desde entonces han sido:

- Despliegue en los sistemas de la red corporativa, de los agentes de una plataforma de EDR, que el grupo de Telefónica TECH comenzó a monitorizar en modo 24x7 con el objetivo de detectar posibles alertas relacionadas con el incidente, y para dar apoyo a la erradicación de forma proactiva.

- Corte de las comunicaciones hacia el exterior permitiendo únicamente el tráfico de aquellos servicios confiables que permitan realizar la monitorización por parte de la plataforma EDR y aquellos servicios críticos para no afectar a las necesidades del negocio.
- Recuperación de copias de seguridad de los activos críticos de la infraestructura para poder partir de una situación confiable.
- Registro de todos los IoC (indicadores de compromiso) que se encuentren en la investigación e inclusión de estos, tanto en la plataforma EDR, como en el actual sistema de seguridad perimetral.

Medidas para mantener el nivel de seguridad post-incidente.

En el momento actual, se considera necesario al menos mantener el nivel de seguridad en el que se ha posicionado a la organización tras el incidente.

Se han acometido medidas técnicas que no han supuesto costes adicionales, como aumentar la complejidad de las contraseñas o restringir reglas en los cortafuegos exterior y de perímetro, pero otras, sí suponen un coste adicional.

Se propone:

- **Servicio especializado de monitorización y alerta temprana 24x7.** El 3 de noviembre finaliza el servicio de monitorización y alerta temprana 24x7 asociado a los agentes EDRs desplegados que estaba incluido en el servicio de análisis forense y recuperación ante incidentes. La idea es contar con ese servicio, pero además de recolectar eventos y disparar alertas de los agentes XDR, lo haga también de la protección que vamos a desplegar en los 50 móviles de personal directivo y determinados responsables de área, de la solución de antivirus actual Kaspersky y de los cortafuegos Fortinet.

ICA en el marco del servicio actual ya recolecta eventos en su plataforma LogICA de parte de la infraestructura de seguridad de RTVM. Ese paso ya está adelantado. Complementando LogICA con la solución MonICA que correla estos eventos con patrones de ataque conocidos el servicio de SOC 24x7 se tarda menos en implantar que con cualquier otro proveedor. Todos los SOC se basan en recolectar eventos y por ese lado ya hay acciones realizadas que va a permitir que el servicio esté operativo antes.

- Desplegar en 50 móviles (asignado a personal directivo y ciertos responsables de área) un agente CheckPoint Harmony **solución para la defensa contra las amenazas móviles**. Mantiene la información corporativa a salvo protegiendo los dispositivos móviles en todos los vectores de ataque: aplicaciones, red y sistema operativo. Se adapta perfectamente al entorno móvil existente, se despliega y escala rápidamente, y protege los dispositivos sin afectar a la experiencia del usuario ni a la privacidad.

En términos generales es una buena práctica diversificar fabricantes en lo que a arquitectura de seguridad se refiere. CheckPoint es un fabricante de referencia desde hace años y pionero en protecciones de equipos móviles. ICA por su parte soporta y mantiene nuestros puntos de acceso WIFI.

III.- Términos de la modificación contractual

El artículo 205 de la Ley de contratos del Sector Público “Modificaciones no previstas en el pliego de cláusulas administrativas particulares: prestaciones adicionales, circunstancias imprevisibles y modificaciones no sustanciales”, en su punto 2.b), en su literal dice:

b) Cuando la necesidad de modificar un contrato vigente se derive de circunstancias sobrevenidas y que fueran imprevisibles en el momento en que tuvo lugar la licitación del contrato, siempre y cuando se cumplan las tres condiciones siguientes:

- 1º. Que la necesidad de la modificación se derive de circunstancias que una Administración diligente no hubiera podido prever.
- 2º. Que la modificación no altere la naturaleza global del contrato.
- 3º. Que la modificación del contrato implique una alteración en su cuantía que no exceda, aislada o conjuntamente con otras modificaciones acordadas conforme a este artículo, del 50 por ciento de su precio inicial, IVA excluido.

En esta ocasión se reúnen los tres requisitos acumulativamente, ya que:

- 1º. Como se ha expuesto, RTVM no pudo prever ser el objetivo de un ciberataque,
- 2º. Ya que se trata de un contrato mixto de suministros y servicios profesionales de instalación y puesta en marcha por un lado y mantenimiento y soporte, por otro, y la modificación da cobertura al servicio especializado de alerta temprana recolectando eventos de la infraestructura de seguridad desplegada y al suministro de las licencias del agente que se quiere desplegar en 50 móviles asignados a personal directivo y determinados responsables de área, para aumentar el nivel de seguridad en esos dispositivos.
- 3º. La modificación, como se indica a continuación, no excede del 50 por ciento del precio inicial, representa, un 46,2 por ciento del importe máximo del contrato.

A la vista de lo expuesto anteriormente, se solicita la modificación del contrato, en referencia a:

- **Servicio especializado de monitorización y alerta temprana 24x7.**
- **Solución para la defensa contra las amenazas en 50 móviles.**

CÓDIGO	DESCRIPCIÓN	UNITARIO	UD.	TOTAL
Suministro				
	Soporte y mantenimiento 2 Agentes de monitorización	1.008,00 €	1 Ud.	1.008,00 €
	Harmony Mobile , per-user single device subscription 50 licencias. Enterprise SW Subscription and Standard Support.	7.010,16 €	1 Ud.	7.010,16 €
		9.737,44 €	1 Ud.	9.737,44 €
Implantación ICA SYS				
	Servicio de instalación y migración de LOGICA a MONICA NGSIM. Parametrización, integración con 7 fuentes y puesta en producción.	25.600,00 €	1 Ud.	25.600,00 €
Servicio CiberSOC ICA SYS				
	Servicio CiberSOC 24x7 gestión de alertas de seguridad - monitorización, operación, administración de MONICA NGSIM y notificación de incidentes de seguridad asociados a los 7 monitores, a prestar en horario 24x7.	25.600,00 €	1 Ud.	25.600,00 €
	Servicio CiberSOC 24x7 gestión de alertas de seguridad - Contención y respuesta complementaria a la monitorización y notificación, a prestar en horario 24x7	25.600,00 €	1 Ud.	25.600,00 €
TOTAL:				68.955,60 €

El suministro de los 50 agentes para móviles está previsto durante el mes de noviembre 2023.
La implantación del SOC se llevará a cabo a partir del día después a la formalización de esta modificación y hasta la finalización del contrato.
El pago de las correspondientes facturas se realizará a la finalización del contrato.

El importe de la modificación, es de SESENTA Y OCHO MIL NOVECIENTOS CINCUENTA Y CINCO CON SESENTA EUROS (68.955,60 €), y representa, un 46,2% del importe máximo del contrato que es CIENTO CUARENTA Y NUEVE MIL CIENTO SETENTA Y CINCO EUROS (149.175,00 €).

Y para que surta los efectos oportunos, firmo en Pozuelo de Alarcón, a 27 de octubre de 2023



Ana Ferrero López
Responsable del Área



Jose María Casaos Patrón
Director del Área

Carta de conformidad a la modificación del Contrato Servicio Gestionado de Mantenimiento y Soporte de Seguridad Perimetral

Muy señores míos:

En el trámite que nos ha sido conferido en relación con la propuesta de modificación del **Contrato Servicio Gestionado de Mantenimiento y Soporte de Seguridad Perimetral**, en adelante el “Contrato”, en vigor desde el 15 de enero de 2021 entre ICA INFORMATICA Y COMUNICACIONES AVANZADAS S.L., (en adelante ICA), y Radio Televisión Madrid, S.A.U, (en adelante RTVM), que nos vincula hasta la finalización del mismo, por medio de la presente mostramos nuestra conformidad al contenido del informe de modificación que nos ha sido remitido por RTVM el día 30 de octubre de 2023, aceptando todos los términos contenidos en el mismo, y más concretamente la aceptación de los puntos indicados en el apartado II del citado informe donde se describe la necesidad de la modificación contractual.

En Madrid, a 30 de octubre de 2023

13756473N JUAN LUIS RIVERO (R:
B28893139)

Firmado digitalmente por
13756473N JUAN LUIS
RIVERO (R: B28893139)
Fecha: 2023.10.30 13:27:56
+01'00'

Fdo. Juan Rivero

Apoderado