Consejo General de Colegios
Administradores de Fincas
España

CIRCULAR 39/2017

ASUNTO.- CONVENIO MARCO DE COLABORACIÓN DE PRESTACIÓN DE SERVICIOS DE CIBERSEGURIDAD.

Nos complace acompañar el convenio marco de colaboración de prestación de servicios de ciberseguridad, firmado entre el Consejo General de Colegios de Administradores de Fincas de España y la empresa The Security Sentinel.

Rogamos difundir esta información entre sus colegiados.

Atentamente,

Madrid, 3 de noviembre de 2017

EL SECRETARIO

RAFAEL DEL OLMO GARRUDO

VºBº
EL PRESIDENTE

SALVADOR DIEZ LLORIS

Plaza del Marqués de Salamanca 10, 3º izda., 28006 Madrid
T +34 915 757 369 F +34 915 751 201 www.cgcafe.org

Consejo General de Colegios Administradores de Fincas España

THE SECURITY SENTINEL

CONVENIO MARCO DE COLABORACIÓN DE PRESTACIÓN DE SERVICIOS DE CIBERSEGURIDAD

En Madrid, a 26 de octubre de 2017

REUNIDOS

De una parte, Don **Salvador Díez Lloris** con D.N.I. número **12.365.780-Z** en nombre y representación del **CONSEJO GENERAL DE COLEGIOS DE ADMINISTRADORES DE FINCAS DE ESPAÑA**, con domicilio social y a efectos de notificaciones en 28006 Madrid, Plaza del Marqués de Salamanca nº 10 3º Izda. En adelante, **CGCAFE** o EL CONSEJO.

Y de otra parte, Don **Francisco Sanz Moya,** con DNI nº **05420756R,** actuando en nombre y representación de **ÁREAS SERVICIOS DE INFORMACIÓN,S.L.**, con C.I.F. nº **B84716919** y que actúa comercialmente con la denominación **THE SECURITY SENTINEL**, con domicilio social y a efectos de notificaciones en Madrid, C/ Santa Leonor, nº 65 Edificio A – 3ª Planta (28037 Madrid). Respecto de dicha sociedad se hace constar que figura inscrita en el Registro Mercantil de Madrid, Tomo 22.987, Folio 91, Hoja M-411.827. En adelante **TSS.**

ACTÚAN

El primero, Sr. Díez Lloris, debidamente facultado, para este acto, en su condición de Presidente del **CGCAFE**, cargo que manifiesta vigente, a todos los efectos legales.

Haciéndolo el Sr. Sanz Moya, como Director General y Representante Legal, conforme resulta de la escritura de Elevación a Público de Acuerdos Sociales autorizada por el Notario del Ilustre Colegio de Madrid D. Miguel Yuste Rojas, el día 5 de febrero de 2016, con número 324 de su protocolo. Cargo que manifiesta vigente, a todos los efectos legales.

Ambas partes se reconocen, en la calidad con que actúan, plena capacidad jurídica y de obrar, para suscribir y obligarse mediante el presente documento, y de sus libres y espontáneas voluntades.

MANIFIESTAN:

I. Que el **CGCAFE** es una Corporación de Derecho público con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines, que integra los diferentes Colegios Territoriales de la profesión, y, en su caso, los Consejos Autonómicos de Colegios y que, dentro de su ámbito de actuación territorial (España), tiene como fines – entre otros- establecer intercambios, acuerdos o cualquier clase de relaciones con otras organizaciones o entidades similares o afines españolas o extranjeras, tanto de ámbito nacional o supranacional; y en general, beneficiar los intereses generales de la profesión de Administradores de Fincas, o las que vengan establecidas o reconocidas por la legislación de Colegios Profesionales a los Colegios Territoriales, en cuanto tengan ámbito o repercusión estatal realizando aquellas funciones que redunden en beneficio de los intereses profesionales de los colegiados y se encaminen al cumplimiento de los fines colegiales.

II. Que el **CGCAFE**, en su función coordinadora de los Colegios de Administradores de Fincas y, con el ánimo de procurar el mejor servicio a dichos Colegios en general y a los Administradores de Fincas colegiados en particular, ha puesto en marcha la creación de una Red Privada de acceso a Datos, Servicios y Soluciones de Software (Cloud) que permitan al colectivo profesional colegiado, el uso de nuevas tecnologías en un entorno seguro.

III. Que **CGCAFE** es consciente de la evidente y real existencia de amenazas externas, que van a intentar robar, destruir y/o secuestrar cualquier tipo de información que resida o transite por esta Red.

IV. Que **TSS.** Es una empresa altamente especializada en defensa y ataque de hacking ético y en prestar servicios de formación, prevención y corrección, en el campo de la CiberSeguridad.

V. Que **TSS** es la compañía líder en formación de hacking, muy reconocida por diversos estamentos del Estado y comprometida con la defensa de ciberseguridad de organismos, empresas y de la sociedad en general.

VI. Que **TSS** quiere y puede contribuir a la seguridad de la Red Privada del **CGCAFE**, con los derechos y obligaciones que se detallan en el presente documento y anexo.

VII. Y puestas de acuerdo, ambas partes, en virtud de lo anteriormente expuesto, acuerdan suscribir el presente CONVENIO MARCO DE COLABORACIÓN, que sujetan a las siguientes:

Por lo anteriormente expuesto, **Las Partes** deciden formalizar el presente **CONVENIO MARCO de Colaboración de Prestación de Servicios de Ciberseguridad,** que se regirá por las siguientes.

CLAUSULAS

PRIMERA.- OBJETO :

El objeto consiste en segurizar la mencionada Red Privada y todos los elementos que la componen (Servidores, Routers, Bases de Datos, Programas, etc.) a fin de proteger fundamentalmente los contenidos.
En consecuencia**, CGCAFE,** designa a **TSS**, para que se encargue de la seguridad de las transacciones y contenidos y aplique, por tanto, las medidas necesarias de segurización, a todos los elementos que componen la Red y a todos aquellos actores que se conecten y/o incidan o puedan incidir, en dichos contenidos.

SEGUNDA.- CONDICIONES DEL SERVICIO:

2.1 CGCAFE o en su caso, las personas y/o entidades por el designadas se encargarán de disponer de todos los elementos hardware y software que integran La Red, incluidas las personas que trabajen en esas infraestructuras (Administradores de Red, Sistemas, Programadores, Operadores, etc.)
2.2 Asimismo, **CGCAFE**, o las personas y/o entidades por el designadas, se encargarán de todas las infraestructuras necesarias, donde se ubiquen los Servidores y demás elementos de la Red, el control del acceso físico de las personas autorizadas a trabajar en esas instalaciones y las condiciones físicas de seguridad de las mismas.
2.3 Por su parte **TSS**, se encargará de auditar la seguridad en los volcados de datos y programas a los Servidores, informando de los resultados a la entidad, pero no entrará a valorar la naturaleza del contenido de los datos. Por lo que cada actor autorizado al volcado de programas y/o datos, será responsable de la naturaleza de los mismos.
2.4 En consecuencia, con el punto anterior **CGCAFE**, no permitirá ningún tipo de volcado de datos y/o programas ni conexión, que no haya pasado satisfactoriamente, una auditoria de pentesting de **TSS** en origen.
Estas auditorías, como mínimo se repetirán semestralmente para los Administradores durante el primer año, a partir del segundo año, será obligatoria al menos una anual. Y, cuatrimestralmente para Colegios y Proveedores de Software.
2.5 Las Auditorías consistirán en comprobar el nivel de protección de los equipos conectados a una red, desde la que se tenga acceso a la Red Privada de **CGCAFE**, ante un intento de intrusión, modificación o alteración de los datos, entre otros riesgos tecnológicos provocados por un ciberdelincuente.
Dichas pruebas se realizan en remoto, proporcionando la dirección o direcciones IPs que tenga operativas el usuario. No obstante, se especifican dichas pruebas en **el ANEXO I** del presente CONVENIO MARCO.
2.6 TSS remitirá el informe de las auditorías realizadas a la parte analizada en cada caso (Administrador, Colegio, Proveedor de Software), incluyendo por cada una de ellas su valoración y las posibles consecuencias de no atención de las mismas, así como una propuesta de vía de resolución o mitigación de las mismas en caso de existir, para que sea aplicada por la parte analizada. La presentación

de éste informe y recomendaciones concluye la misión de trabajo puntual de **TSS**, siendo responsabilidad de la parte analizada la atención y resolución de las vulnerabilidades informadas.
No obstante, **TSS** se ofrece a colaborar en las posibles soluciones a petición de la persona o entidad interesada.
2.7 Una vez, comprobada positivamente la seguridad, **TSS** emitirá el correspondiente Certificado de Auditoría de Ciberseguridad.
2.8 TSS monitorizará en tiempo real y en formato 24h/7 días todas las transacciones que se produzcan hacia y desde la Red Privada.
2.9 Además **TSS** recomienda la realización de copias de seguridad diarias, el cifrado de los datos, el control de passwords y la aplicación de medidas prevención de ingeniería social y concienciación.

TERCERA.- COSTE DEL SERVICIO:

TSS ha tenido muy en cuenta la especial composición de los actores que van a ser los usuarios de esta Red Privada y que en su inmensa mayoría van a ser los Administradores de Fincas colegiados, los cuales habitualmente o son pequeñas PYMES o bien autónomos, con lo que sus infraestructuras informáticas suelen ser bastante reducidas (adecuadas por otro lado, a las necesidades de su propia actividad).
Por lo que la apuesta de **TSS** es ver el conjunto de los mismos y, por tanto, ha tratado de minimizar el coste para los usuarios con un nivel de seguridad válido para el objetivo marcado.
No obstante y como es lógico, **TSS** necesita cubrir un tiempo de duración del CONVENIO MARCO y unos mínimos para poder prestar el servicio.
La propuesta económica de Auditorías y la descripción técnica de los servicios, se adjunta como **ANEXO I**, al presente CONVENIO MARCO.
La propuesta económica referida a la monitorización en tiempo real, se adjuntará como **ANEXO II**, una vez que se inicien las auditorias, porque el coste vendrá determinado por lo que arrojen los primeros resultados de las mismas.
No obstante, **TSS**, anticipa que el coste por IP será extremadamente reducido y que el mismo no supondrá un hándicap, para ninguno de los usuarios que se conecten.

CUARTA.- DURACIÓN:

El presente CONVENIO MARCO, entrará en vigor a la fecha de su firma y tendrá una duración inicial de tres años, transcurridos los cuales se prorrogará automáticamente por años naturales, siempre que alguna de las partes no denuncie la rescisión del mismo con un preaviso fehaciente de dos meses de antelación.

QUINTA.- DIFUSIÓN Y COMUNICACIONES:

CGCAFE, se encargará de poner en conocimiento de los diferentes actores (Colegios y/o colectivos interesados), el contenido del presente CONVENIO MARCO que sea de interés para los mismos.
Así como, facilitar a **TSS** la tarea de concienciación, sobre la protección de la información, al Colectivo de Administradores de Fincas Colegiados.
A este fin**, CGCAFE**, invitará a asistir a **TSS**, a todos los actos en los que pueda difundir, participar o aportar información, en la consecución de una mejor y mayor seguridad de la información.

En compensación a este trabajo por parte de **CGCAFE**, la auditoría de ciberseguridad del mismo, se realizará sin coste económico.

SEXTA.- EXCLUSIVIDAD:

Durante el tiempo que permanezca vigente el presente convenio el **CGCAFE** se obliga a no suscribir directa o indirectamente, por sí mismo, ni a través de terceras personas, un convenio de colaboración de similares o idénticos términos al presente, con otra persona física o jurídica, empresa, despacho o profesional que desarrolle la misma actividad que **TSS**. Y en particular a no suscribir convenio, en idénticos o similares términos con otra persona física o jurídica que se dedique al campo de la seguridad informática o de la protección de datos que pudiera ser competencia de **TSS**.

SEPTIMA.- CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL:

Toda la información referente a cualquiera de los actores a la que **TSS** tenga acceso con motivo del cumplimiento de las gestiones encomendadas, será considerada confidencial, con expreso compromiso por su parte de no utilización para fines ajenos al presente CONVENIO MARCO, ni de divulgación en modo alguno a terceros.

Con independencia de la extinción del presente convenio, el compromiso de confidencialidad permanecerá indefinido desde la fecha de la firma del convenio y hasta que esa información, por otro medio, pase a ser de dominio público.

Por lo demás las partes se comprometen al cumplimiento de cuantas obligaciones les sean legalmente exigibles en cuanto al tratamiento de datos personales, por las disposiciones en materia de protección de datos de carácter personal, en particular por las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre (LOPD) y normativa posterior que la amplíe o la actualice.

OCTAVA.- SEGUIMIENTO Y GESTIÓN:

A efectos del presente convenio, ambas partes designan como interlocutores para los temas a que se refiere el mismo a D. Carlos Domínguez García-Vidal, por parte de **CGCAFE** y a D. Manuel Torres Cruz, por parte de **TSS.**

Las comunicaciones vía correo electrónico se harán a:

CGCAFE sectecnica@cgcafe.org

TSS mtorres@thesecuritysentinel.es

NOVENA.- RESOLUCIÓN DEL CONVENIO:

Será causa de resolución del presente convenio, el incumplimiento fehaciente en el que incurran las partes en relación con las obligaciones asumidas en méritos del presente Convenio.

DECIMA.- LEGISLACION SUPLETORIA Y COMPETENCIA JURISDICCIONAL:

Este CONVENIO MARCO tiene carácter mercantil y se regirá por sus propias cláusulas y en lo que en ellas no estuviese previsto por el Código de Comercio Internacional, leyes especiales y usos mercantiles aplicables.
Las partes se comprometen a resolver amistosamente cualquier diferencia que pueda surgir en relación al presente Convenio.
Si esto no fuera posible, en caso de litigio, ambas partes, con expresa renuncia a cualquier otro fuero que pudiera corresponderle, y para cualquier controversia que pueda presentarse como consecuencia del contenido o interpretación del presente documento y su ejecución, ambas partes, se someten a la exclusiva competencia de los Juzgados y Tribunales de la Villa de Madrid.

Y leído y hallado conforme su contenido íntegro, lo firman por duplicado ejemplar, si bien a un solo tenor y efecto, en el lugar y la fecha indicados en el encabezamiento.

TSS **CGCAFE**

THE SECURITY SENTINEL

ANEXO I

Propuesta de
Seguridad Informática
Consejo Gral. Colegios Administradores Fincas

16-Marzo-2017

VERSIÓN	FECHA	ELABORADO	REVISADO	APROBADO
2.0	09/02/2017	Kamel Karabelli	Manuel Torres	

HOJA DE REVISIONES DE ACTUALIZACIONES

PUNTO	CAMBIOS RESPECTO A LA VERSIÓN ANTERIOR
6	Oferta Económica y Promociones

1 - ÍNDICE

2 - INTRODUCCIÓN

2.1 - PROPÓSITO DEL DOCUMENTO

El propósito de este documento es presentar una propuesta al Consejo General de Colegios de Administradores de Fincas en referencia a la evaluación y propuestas de mejora en la Estrategia de Ciberseguridad de sus transacciones y contenidos, así como en las condiciones de Seguridad Informática de los sistemas y comunicaciones del Consejo, los Colegios y Administradores, frente a las posibles acciones de ciberdelincuentes, o intentos de acceso a la información no autorizados.

En la presente propuesta, se plantea realizar un análisis continuado de los sistemas y red que prestan servicio para el CGCAF, y sus asociados, así como una segunda fase de monitorización de la actividad entrante y saliente de la red.

2.2 - CONTACTO Y RESOLUCIÓN DE DUDAS

Cualquier duda sobre el contenido de este documento, de la propuesta o cualquier otra cuestión, por favor dirijan su consulta a:

Manuel Torres

Director Cuentas Especiales

mtorres@thesecuritysentinel.es

+34 654 51 33 05

3 - OBJETO DE LA OFERTA

3.1 – OBJETIVO

El objetivo de este documento es colaborar con el Consejo General de Administradores de Fincas en el análisis y mejora de las Estrategias de Ciberseguridad implantadas actualmente en los sistemas y soluciones actuales de la entidad.

El Consejo como entidad, y sus Colegios y Asociados, se enmarcan en un sector donde la disponibilidad, privacidad e integridad de los datos es un elemento nuclear de su propuesta de valor de cara a sus clientes, y en el que la calidad de servicio, así como la seguridad del mismo, suponen un valor fundamental.

A lo largo del ejercicio 2016, se ha detectado un incremento en los riesgos tecnológicos y amenazas a la seguridad TI, privacidad de la información, y disponibilidad de servicio para entidades del mismo sector del Consejo, por lo que desde la perspectiva de The Security Sentinel, se aporta una propuesta de actuación específica, consistente en la evaluación del nivel de Ciberseguridad de sus sistemas y soluciones, así como la Red de comunicación entre el Consejo y sus asociados, con el fin de elevar a su dirección propuestas de mejora, aumentando de éste modo la resiliencia a posibles intentos de intrusión, modificación del servicio prestado, o accesos no autorizados a información específica de la compañía, de sus procesos de negocio, o de sus clientes.

De ésta manera, se realizarán diversas pruebas técnicas con el objetivo de detectar, identificar y minimizar los vectores de entrada de un posible ciberdelincuente, que pudieran afectar al servicio de las redes y equipos del Consejo, tanto para su uso interno y gestión diaria, como a la hora de proteger adecuadamente la información referente a sus clientes y procesos, salvaguardando de éste modo la reputación del Consejo ante ellos.

Asímismo, se propone un servicio de monitorización permanente en las comunicaciones de la Red Interna del Consejo, con el fin de detectar las comunicaciones de Red que puedas ser sospechosas de actividad ilegítima o no autorizada, de manera que se pueda contemplar la Ciberseguridad de manera integral en el marco de la operación diaria y diseño de redes y equipos de la entidad.

4 - RESUMEN DE SERVICIO Y ENTREGABLES

El servicio que The Security Sentinel ofrece al Consejo se divide en dos hitos:

El **Primer Hito**, consiste en la realización de una **Auditoría de Seguridad** en la red y sistemas del Consejo, de los Colegios y de los Administradores designados, con el fin de conocer el estado actual de Ciberseguridad de cada uno de los elementos y actores que desempeñan su actividad en interrelación con la entidad.

La periodicidad recomendada de éstas auditorías es variable según la entidad a auditar, y según el conocimiento experto de The Security Sentinel, se propone la siguiente división:

- **Auditorías externas:** (comprobación de seguridad en conexión externa y seguridad de las comunicaciones)
    - Administradores de Fincas: Durante el Primer año, dos auditorías una por semestre. A partir del segundo año, una Auditoría anual como mínimo.
    - Colegios:Una Auditoría anual. Para los Colegios que aporten al Proyecto el diez por ciento de sus afiliados o bien, cincuenta o más Administradores de Fincas colegiados, estas auditorías se realizarán sin coste..

-

- **Auditorías internas:** Será necesario evaluar cada caso de manera particularizada, en función de su parque informático, y dispositivos y plataformas a securizar.

Tras la realización de cada una de las auditorías, se elaborará, en un periodo de 15 días desde la fecha de inicio de la auditoría, la siguiente documentación a modo de **entregable**:

- **Informe de resultados:** Reporte específico de los trabajos realizados, que incluye:
  - Riesgos Identificados.
  - Calificación.
  - Recomendaciones y propuestas de resolución / mitigación.
  - Detalle Técnico del/los análisis realizado(s).
  - Prioridad de atención al riesgo.
  - Vulnerabilidades, amenazas y consecuencias de no cumplir con las recomendaciones.

En cuanto a la **calificación** de los incidentes, se utilizará la fórmula (Prioridad = Urgencia + Impacto) a la hora de catalogarlos según el nivel de atención que debe tener, a propuesta de The Security Sentinel.

Segundo Hito: Monitorización

Consiste en la inspección y análisis en tiempo real y continuado (servicio 24/7) del tráfico de red entrante y saliente en cada uno de los dispositivos de comunicación identificados (router, wifi, etc), mediante el análisis de su tráfico de red y la detección de las conductas y situaciones calificadas como "de riesgo", para la entidad o para la integridad, seguridad y confiabilidad de sus datos.

El servicio de Monitorización será propuesto individualizadamente una vez realizada la primera serie de auditorías de seguridad contenidas en el primer hito, según los niveles detectados de seguridad informática y necesidades de protección o mejora en cada caso particular.

Mediante éste servicio de monitorización se intervendrá de manera directa en los incidentes de seguridad definidos como prioritarios, y se elaborará a modo de **entregable**, con carácter mensual, un informe de los incidentes detectados, así como las medidas emprendidas en cada caso, con el fin de evaluar conjuntamente entre la entidad y el Consejo las actuaciones necesarias y posibles mejoras en la securización de la red y sistemas.

- **Éste informe de resultados contendrá**:
  - Riesgos Identificados.
  - Calificación.
  - Actuaciones realizadas.
  - Propuesta de mejora, en su caso.

En cuanto a la **calificación** de los incidentes, se utilizará la fórmula (Prioridad = Urgencia + Impacto) a la hora de catalogarlos según el nivel de atención que debe tener, a propuesta de The Security Sentinel.

5 - DETALLE TÉCNICO DE PRUEBAS A REALIZAR

A continuación, se detallan las principales pruebas, que se realizarán en función de la auditoría. The Security Sentinel destaca que se trata de un resumen informativo, y no limitativo ni exhaustivo, acerca de la batería de pruebas en que está especializado, y que se realizarán según se acuerde con la entidad, tanto en profundidad como en alcance

Existe un punto en común en todos los tipos de auditoria:

5.1 EXTERNAL FOOTPRINTING

Esta parte es la inicial a la hora de realizar una auditoría de seguridad.

Básicamente, se trata de recopilar toda la información posible en Internet, sobre el cliente. El objetivo de esta fase es conocer mejor al cliente, y ver que recursos tiene publicados, cuentas de correo visibles, etcétera.

Algunos de las pruebas que se realizan en esta fase son:

- Descubrimiento de DNS
- Identificación de CMS (si lo tiene)
- Banner Grabbing (Versiones de servicios)
- Descubrimiento SMTP
- Protocolo SNMP
- Detección de IDS/IPS
- Extraer información del dominio
- Análisis de SMB
- Google Dorking
- Shodan Hacking
- Emails visibles en Internet para realización de ataques en un futuro.
- Recopilar información extra para la realización de ataques de Ingeniería Social

5.2 ANÁLISIS WEB

Una vez realizada la primera fase, ya se tiene suficiente información para empezar a realizar pruebas específicas.

En esta fase, varia un poco en función de que se esté auditando. Si se trata de una página web, los ataques serán completamente diferentes a si se está auditando una red de servidores externamente.

En el primer caso, si la auditoría está enfocada a una aplicación web, se realizarían ataques específicos como:

- SQL Injection
- XSS (Cross-site scripting)
- LFI (Inclusión de ficheros locales)
- RFI (Inclusión de ficheros remotos
- CSRF
- Métodos soportados por el servidor (head, trace, get, post, put, options, etcétera) - BlindSQL Injection
- Bypass a sistema de autenticación (formulario)
- Solicitudes falsificadas en sitios cruzados
- Validación de variables recibidas por el servidor
- Listados de directorio
- RCE (Ejecución de comandos en el servidor)
- LDAP Injection
- Descubrimiento de directorios ocultos
- Fuerza bruta a directorios
- Ataques XML
- Subida de ficheros
- Comprobación de certificados SSL (ruptura)
- Etcétera

Difícilmente se pueden detallar todas las pruebas que se realizarán, dado que The Security Sentinel, no sabemos qué nos vamos a encontrar hasta el momento que empiece la auditoria. Pero tratándose de una aplicación web, estos son los tipos de ataque más comunes (hay mucho más).

Propuesta técnica

5.3 ANÁLISIS DE SERVIDORES, FIREWALL Y PC'S

Si se trata de un listado de ip's, las cuales proporcionan servicios que no sean aplicativos web, se realizarían pruebas como:

- Escaners automatizados
- Pruebas manuales
- Detección de tipos de servicios con sus respectivas versiones
- Límites de intento de sesión a un servicio
- Fuzzing
- Análisis de métodos de autenticación
- Ruptura de cifrados (si los hay)
- Pivoting a la red interna
- Búsqueda de hashes de usuarios
- Análisis de reglas de firewall
- Bypass al firewall
- Ataques de diccionario
- Búsqueda de vulnerabilidades públicas en versiones detectadas
- Explotación de las mismas
- En caso de acceso a la red interna, escalada de privilegios
- Comprobación de efectividad de antivirus
- Bypass Antivirus
- Análisis de IDS y generación de alertas
- Comprobación de certificados SSL (ruptura)
- Descubrimiento de equipos en la red
- Etcetera

En este apartado, difícilmente se podrían detallar los ataques empleados, dado que en función de los que sirvan los servidores, se lanzarían unos u otros no mencionados.

5.4 ANÁLISIS WIRELESS

En este apartado, se analizarían los puntos de acceso del cliente, con el fin de averiguar que podría llegar a provocar una persona que reciba la señal del cliente.

Las distintas pruebas que se realizarían serían:

- Análisis de los nombres de los puntos de acceso
- Alcance de los puntos de acceso
- Análisis de repetidores (si los hay)
- Ruptura de cifrado WEP
- Ruptura de cifrado WPA
- Ruptura de cifrado WPA2-PSK
- Ruptura de cifrado WPA2-MGMT (Servidor Radius)
- Levantamiento de RogueAP

- Comprobación de IDS/AntiRogueAP
- Denegación de servicio a las redes inalámbricas (confirmación con el cliente)
- Análisis de la segmentación de la red+
- Análisis de contraseñas Wireless
- Análisis de alcance de las señales Wireless
- Ataques de Ingeniera Social a los usuarios
- Análisis de filtrado MAC (Si lo hay)
- Análisis de WiteList (si lo hay)
- Análisis de BlackList (si lo hay)
- Análisis y ruptura de WPS (si está activado)
- Etcetera

5.5 ANÁLISIS SISTEMAS DE CONTROL INDUSTRIAL (SCI)

En el apartado de los Sistemas de Control Industrial, se realizará, entre otras, la siguiente serie de pruebas:

- Análisis de la arquitectura de red de los SCI:
  - Seguridad de red
  - Cifrado
  - Autenticación
  - Acceso remoto
  - Disponibilidad
- Análisis de los protocolos de comunicación SCI
  - Protocolos
  - Analisis de posibles CIP,Profinet, Modbus,Powerlink E., OPC, EtherCat...

- Recomendaciones de seguridad

- Recomendaciones de seguridad específicas:
  - Cortafuegos
  - Servicios

6 - DETALLES PRESUPUESTO

A continuación se desglosa presupuesto por servicios:

HITO 1: AUDITORÍAS EXTERNAS			
Concepto	**Contenido**	**Periodicidad (Recomendada)**	**Importe Por IP y Auditoría**
Auditoría Externa Administradores	**Análisis de la seguridad de las comunicaciones y conexión externa.** (IP facilitada por el auditado). **Promoción: Para los primeros 75 Administradores colegiados adheridos al Proyecto, se les aplicará un descuento lineal por IP y Auditoría de 70 €**	**Semestral (Primer año)**	**270€**
Auditoría Externa Colegios	Análisis de la seguridad de las comunicaciones y conexión externa. (IP facilitada por el auditado). Para los Colegios que aporten un mínimo de 50 colegiados o bien que el diez por ciento (10 %) de sus colegiados se sumen al proyecto. La Auditoría externa se realizará sin coste. **Auditoría del consejo (Gratuita)**	Anual	**270 €**

HITO 2: MONITORIZACIÓN			
Concepto	**Contenido**	**Periodicidad**	**Importe**
Monitorización Comunicaciones de Red Administradores	Monitorización 24/7 de las comunicaciones de red entrantes/salientes de Administradores de Fincas Colegiados.	24/7	**25€/mes por ip con el supuesto de 1000 ip's** **17,5 €/mes por ip con el supuesto de 2000 ip's**
Monitorización Comunicaciones de Red Colegios	Monitorización 24/7 de las comunicaciones de red entrantes/salientes de Colegios de Administradores de Fincas. **Para los Colegios que aporten un mínimo de 50 colegiados o bien que el diez por ciento (10 %) de sus colegiados se sumen al proyecto, la monitorización será gratuita.**	24/7	**25€/mes por ip . con el supuesto de 1000 ip' s(*)** **17,5/mes € por ip .con el supuesto de 2000 ip's (*)**
Monitorización Comunicaciones de Red Administradores	Monitorización 24/7 de las comunicaciones de red entrantes/salientes de Administradores de Fincas Colegiados.	8/5	**14€/mes por ip con el supuesto de 1000 ip's** **10 €/mes por ip con el supuesto de 2000 ip's**
Monitorización Comunicaciones de Red Colegios	**Monitorización 24/7 de las comunicaciones de red entrantes/salientes de Colegios de Administradores de Fincas.** **Para los Colegios que aporten un mínimo de 50 colegiados o bien que el diez por ciento (10 %) de sus colegiados se sumen al proyecto**, la monitorización será gratuita.	**8/5**	**14/mes por ip con el supuesto de 1000 ip's(*)** **10 €/mes por ip con el supuesto de 2000 ip's(*)**

(*) NOTA IMPORTANTE. Es evidente, que la suma de los ip's de los Colegios, nunca o de forma muy improbable,van a alcanzar la cifra de 1000, 2000 ip's. El cálculo, para esta cifra, lo estamos contemplando a nivel nacional, es decir a la suma de Todas las conexiones Ip´s del conjunto total de Administradores, Colegios, etc.

Lo habitual es que la monitorización de los Colegios sea gratuita porque todos alcancen el objetivo del 10% o de 50 colegiados adscritos, pero para el caso de que el Colegio no cumpliera este requisito, les facturaríamos las cantidades que figuran en la presente oferta.

EL INICIO DEL SERVICIO DE MONITORIZACIÓN, COMENZARÁ A PARTIR DE 1000 IP' s ADSCRITAS AL CLOUD.

La monitorización se encargará de tectectar tráfico sospecho, análisis de posibles archivos infectados , descubrimiento de ip's atacantes (tanto si es desde el exterior, como si es desde interior de las redes), así como cualquier evento que haya sido programado para saltar como alerta y el bloqueo de las ip's atacantes.

Condiciones de la oferta:

Los precios propuestos se han ajustado atendiendo a las particularidades del servicio previsto para el Consejo General de Administradores de Fincas.

Validez del presupuesto: 45 días.

Los precios indicados NO incluyen IVA / Impuestos.

Desplazamiento / Dietas:

En caso de desplazamientos fuera de la comunidad de Madrid, se repercutirán los gastos de desplazamiento y dietas correspondientes a cada caso.

Forma de pago

Transferencia a la presentación de factura al inicio de la Auditoría

Fechas de realización de las auditorías:

Las fechas de realización de las auditorías serán pactadas de manera individualizada entre The Security Sentinel y la entidad, con el fin de garantizar la óptima calidad del servicio.

7 - ANEXO – DATOS DE LA EMPRESA

7.1 ¿QUIÉNES SOMOS?

The Security Sentinel está compuesta mayoritariamente por profesionales expertos en hacking ético y una red de colaboradores con una sólida formación y una experiencia mínima de 5 años en el campo de la seguridad.

Nuestros colaboradores han desempeñado labores tales como:

- Profesores de Universidad.
- Profesores de centros donde se imparten certificaciones de seguridad informática.
- Fundadores de conferencias de Seguridad Informática. - Responsables de seguridad de entidades bancarias.
- Responsable de seguridad de las Fuerzas armadas.
- Consejeros de seguridad informática de gobiernos.
- Responsables de seguridad informática de multinacionales

7.2 - PLAN DE TRABAJO

Protegemos la información y los sistemas ante amenazas internas y externas.

- Identificamos los fallos y problemas de seguridad mediante test avanzados, que permiten realizar simulaciones controladas como si fueran ataques reales producidos por hackers.
- Presentamos informes exhaustivos de las pruebas realizadas y de cómo hemos conseguido acceder que permitan una lectura entendible para la dirección y para el personal técnico.

Ponemos el mejor talento al servicio de las compañías, priorizamos las necesidades reales del cliente, presentando un plan de acción que marque claramente los servicios a evaluar y/o servidores, zonas de actuación, tiempo de la auditoría y los riesgos que ésta pudiera ocasionar.

Nuestro equipo solamente actuará mediante un acuerdo contractual firmado entre The Security Sentinel y el cliente que especifique claramente todos los puntos anteriores.

7.3 SERVICIOS

Entre los servicios que podemos ofrecer a nuestros clientes podemos destacar:

- Coordinación de proyectos de seguridad
- Detección de fugas de información de clientes
- Formación.
- Seguridad en código de aplicativos
- Auditoría de los aplicativos móviles y servicios con los que conectan e interactúan.
- Desarrollo de aplicaciones de seguridad.
- Servicio de Seguridad del ciclo de vida del software
- Pentesting web aplicaciones internas y externas a la compañía
- Test de intrusión a plataformas de Telefonía IP

7.4 CLIENTES

Los clientes que confían en nosotros pertenecen a diferentes sectores:

- **Financieras y aseguradoras**: Son la principal motivación para la gran parte de delincuentes en Internet. Necesitan unos grandes sistemas de seguridad y contar con el personal más cualificado.
- **Tecnológicas y online**: La cantidad de ataques a redes sociales, portales de búsqueda y los ataques contra el correo electrónico están creciendo considerablemente y necesitan de las técnicas más innovadoras para subsanar sus agujeros de seguridad.
- **Multinacionales y PYMES**: Cada vez más compañías sufren ataques de diferente gravedad que les hacen sufrir grandes pérdidas de tiempo y dinero. Necesitan contar con unos sistemas fiables que les permitan ser competitivos, eficientes y fiables de cara a sus clientes.
- **Organismos Públicos**: Necesitan de la máxima seguridad para salvaguardar todos los datos confidenciales que mueven. Es primordial y prioritario realizar constantes test de seguridad.