Junta de Andalucía
Consejería de la Presidencia, Administración Pública e Interior
SOCIEDAD ANDALUZA PARA EL DESARROLLO DE LAS TELECOMUNICACIONES S.A. (SANDETEL)

EVALUACIÓN DE LOS CRITERIOS DE JUICIO DE VALOR PARA LA CONTRATACIÓN DEL SERVICIO DE REVISIÓN TÉCNICA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN INFOLEX DE LA CONSEJERÍA DE LA PRESIDENCIA, ADMINISTRACIÓN PÚBLICA E INTERIOR

(EXPTE. 20-00171)

Departamento: Consultoría y Desarrollo Corporativo

Área: Seguridad y Confianza Digital

Tipo de documento: Análisis de ofertas

Código: N/A

Fecha: 22/01/2021

Elaborado	Revisado
Amalia Bote	
David Berni	

Firmado por BOTE ROSARIO AMALIA - 34779600N el día 22/01/2021 con un certificado emitido por AC FNMT Usuarios

Firmado por BERNI SANCHEZ DAVID - 44350343H el día 22/01/2021 con un certificado emitido por AC FNMT Usuarios

© 2017 Sociedad Andaluza para el Desarrollo de de las Telecomunicaciones S.A.
Este documento y, en su caso, cualquier documento anexo al mismo, contiene información de carácter confidencial exclusivamente dirigida a su destinatario o destinatarios. Queda prohibida su divulgación, copia o distribución a terceros sin la previa autorización escrita de "Sociedad Andaluza para el Desarrollo de la de las Telecomunicaciones S.A..". Si no es Ud. el destinatario del documento le ruego lo destruya sin hacer copia digital o física, comunicando a "Sociedad Andaluza para el Desarrollo de de las Telecomunicaciones S.A." vía e-mail o fax la recepción del presente documento. Toda declaración de voluntad contenida deberá ser tenida por no producida.

ÍNDICE

1 OBJETO 3

2 PROPUESTAS PRESENTADAS 3

3 DOCUMENTOS DE REFERENCIA 3

4 ANÁLISIS DE LAS PROPUESTAS 3

4.1 ANÁLISIS DE LOS CRITERIOS DE JUICIOS DE VALOR 4
4.1.1 Propuesta de AYESA. 4
4.1.2 Propuesta de BEONESEC. 6
4.1.3 Propuesta de CSA. 8
4.1.4 Propuesta de ICA. 10
4.1.5 Propuesta de INGENIA. 11
4.1.6 Propuesta de S2GRUPO. 13
4.1.7 Propuesta de SOTHIS. 14
4.1.8 Propuesta de TELEFÓNICA. 16

5 RESUMEN DE LAS PROPUESTAS Y CONCLUSIONES 18

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

1 OBJETO

El presente documento tiene por objeto realizar la evaluación de los criterios de Juicio de Valor de las ofertas presentadas por los licitadores al pliego de condiciones técnicas para la contratación por la Sociedad Andaluza para el Desarrollo de las Telecomunicaciones, SA (en adelante SANDETEL) del concurso con nº **EXPEDIENTE 20-00171** referente a la contratación del **SERVICIO DE REVISIÓN TÉCNICA DE SEGURIDAD DEL SISTEMA DE INFORMACIÓN INFOLEX DE LA CONSEJERÍA DE LA PRESIDENCIA, ADMINISTRACIÓN PÚBLICA E INTERIOR.**

2 PROPUESTAS PRESENTADAS

A continuación, se relacionan las propuestas presentadas:

1. AYESA
2. BEONESEC
3. CSA
4. ICA
5. INGENIA
6. S2GRUPO
7. SOTHIS
8. TELEFÓNICA

3 DOCUMENTOS DE REFERENCIA

[1] Expediente 20-00171: PPT y PCAP

4 ANÁLISIS DE LAS PROPUESTAS

Analizada la totalidad de la documentación presentada en el sobre 2 de las propuestas recibidas se obtienen las valoraciones de los criterios de Juicio de Valor.

Los criterios de valoración indicados en el PCAP ANEXO XI son los siguientes:

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

1º Especificación del proceso de auditoría: Valorándose el enfoque adecuado de los servicios (15%), completitud y detalle de la propuesta (30%), asignación de recursos (30%) y planificación de las tareas (25%) para la realización de los trabajos.

6% Auditoría dinámica "caja negra"
6% Auditoría dinámica "caja blanca"
5% Control de acceso: gestión de roles y permisos

2º Entregables: Se valorará la relación y descripción de los entregables a presentar (3%), formato (3%) y contenido (6%): registro de evidencias, condiciones de hallazgo y reproducción, clasificación e impacto, medidas correctivas, planes de acción. **(12%)**

3º Formación: Metodología (3%), materiales, recursos (3%) y contenidos desarrollados de los temas (3%) "Tema 1: CICLO DE VIDA DEL DESARROLLO SEGURO DE SOFTWARE y Tema 3: SEGURIDAD EN LOS PROCESOS Y PROCEDIMIENTOS" **(9%)**

4º Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del ENS. Valorándose la metodología y herramientas empleadas en el proceso de análisis de riesgos (identificación de activos, revisión de controles, medidas de protección) (3%), planificación de tareas y asignación de recursos (2%) y el contenido y formato de los entregables generados (1%). **(6%)**

5º Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del RGPD. Valorándose la metodología y herramientas empleadas (2,5%), planificación de tareas y asignación de recursos (1,5%) y el contenido y formato de los entregables generados (1%). **(5%)**

4.1 ANÁLISIS DE LOS CRITERIOS DE JUICIOS DE VALOR

Se han presentado 8 propuestas para la contratación del servicio. A continuación, se muestra de manera resumida el resultado de su análisis y la valoración técnica realizada:

4.1.1 Propuesta de AYESA.

- **Criterio 1. Especificación del proceso de auditoría**

  Enfoque basado en la aplicación del ciclo de vida de desarrollo seguro de software. 10%

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

Tres fases: SAST, DAST, análisis de protocolos criptográficos (34 controles certifican integridad y confidencialidad de los datos que se intercambian). Top Ten de OWASP. Analiza el código, aunque no se pide. (Sonarqube, Checkmarx). 20%

Asigna analista de seguridad especializado en hacking ético, no detalla horas ni dedicación. 10%

Indica que se consensuarán los plazos de ejecución de cada una de las fases, poco detallado. 10%

- 1.1 Auditoría dinámica "caja negra". (6%)

  Batería de pruebas (aporta listado bastante detallado) basado en el modelo de amenazas de OWASP. Fases de reconocimiento, escaneo, explotación y documentación. Herramientas software libre. 1,75%

- 1.2 Auditoría dinámica "caja blanca". (6%)

  Misma metodología y tareas. Aplican mismos comentarios. 1,75%

- 1.3 Control de acceso: Gestión de roles y permisos. (5%)

  Propone consultoría de perfiles y áreas funcionales para comprobar la correcta asignación de los mismos. 1,38%

- **Criterio 2. Entregables (12%)**

  Dos informes, ejecutivo y técnico. 2%

  No especifica formatos. No hay herramienta de seguimiento. 0%

  Indica los contenidos de cada uno. Indica presentación de resultados. 5%

- **Criterio 3. Formación (9%)**

  Metodología e-learning, divide en varias fases: arranque, actualización (trimestral) y cierre. 2%

  Se entregarán manuales y guías rápidas. Equipo de formadores consultores expertos en cada materia. Emiten certificado. 2%

  Buen desarrollo de los temas. 3%

- **Criterio 4. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del ENS (6%)**

  Se llevará a cabo un plan de adecuación al ENS según la Guía CCN-STIC 806. Emplearán MAGERIT y PILAR para análisis de riesgos. 2,5%

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

Consultor especializado en el proceso de certificación del ENS. No hay estimación temporal/dedicación de horas. 1%

Entregables: Documento Política de Seguridad. Cuestionario de valoración de la información y del servicio para cada dimensión de seguridad, análisis del nivel de seguridad del sistema. Análisis de riesgos. Declaración de Aplicabilidad. Listado de insuficiencias basado en el análisis GAP. Plan de mejora de la seguridad con cronograma de actuaciones. 1%

- **Criterio 5. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del RGPD (5%)**

  Refiere la aplicación del ENS para el cumplimiento del RGPD por sus elementos en común, detallado según los aspectos de la ley. No hay especificación de recursos, planificación o entregables. 2% + 0,5% + 0,25%.

TOTAL AYESA (sobre 49%) = 26,13%

4.1.2 Propuesta de BEONESEC.

- **Criterio 1. Especificación del proceso de auditoría**

  Buena descripción de activos, objetivos y resultados a proporcionar. Técnicas de movimiento lateral para testar la propagación por la red. Segunda revisión para comprobar la implementación de las recomendaciones. 15%

  Principalmente se utilizarán métodos de análisis manual (con el apoyo de herramientas. Seguimiento mediante herramienta de registro y gestión de vulnerabilidades. Auditoría estática o de análisis de código sobre los módulos desarrollados a medida de INFOLEX si se proporciona acceso al código fuente. 30%

  Actividades y tiempos muy detallados, diagrama de Gantt, sólo a falta de los hitos destacados. 25%

  Descripción de recursos (4 personas + JP) pero sin distribución de cargas/esfuerzo de trabajo (horas/hombre) para cada una de las auditorías. 20%

  - 1.1 Auditoría dinámica "caja negra". (6%)

    Buena descripción áreas de diagnóstico. Metodologías de trabajo OWASP y OSSTMM.
    Listado exhaustivo de herramientas de auditoría disponibles (Anexo III)
    Valor añadido movimiento lateral y segunda auditoría al cabo del tiempo para verificar cumplimientos. 4,5%

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

- 1.2 Auditoría dinámica "caja blanca". (6%)

  Misma metodología y tareas. Aplican mismos comentarios. 4,5%

- 1.3 Control de acceso: Gestión de roles y permisos. (5%)

  Metodología concreta guía de pentesting de la OWASP (secciones 4.5, 4.6 y 4.7, Authentication Testing, Authorization Testing y Session Managdement Testing) sumado al análisis realizado en caja blanca. Herramientas como Padbuster o CyberChief para analizar las cookies. Aspecto técnico y organizativo: análisis de lógica de negocio, consistencia de roles asignados, generación de mapa de visibilidades. Muy completo. 4,05%

- **Criterio 2. Entregables (12%)**

  Un informe técnico y uno ejecutivo por cada tipo de auditoría (dinámica, estática y roles). Segundo informe de revisión para comprobar la implementación de las recomendaciones. 3%

  Los dos formatos indicados en el pliego, en digital y papel. Además, subidos a la herramienta. Habrá además presentación de resultados con demostraciones y pruebas de concepto. 3%

  Información técnica completa para cada vulnerabilidad (nombre, código, valor CVSS, dificultad de descubrimiento y explotación, recomendaciones de resolución, etc). 5%

- **Criterio 3. Formación (9%)**

  Metodología "learning by doing" bien expuesta y desarrollada. 30 horas distribuidas en sesiones de 2-3 horas eminentemente prácticas. 3%

  A elegir presencial (15-20 personas) disponible aula de formación u online. Materiales digitalizados disponibles en la plataforma edX, accesibles para 40 usuarios durante 2 años. Equipo docente especificado. 3%

  Realiza una propuesta de contenidos, algunos temas correspondientes a los indicados en pliego y otros de aporte propio. 3%

- **Criterio 4. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del ENS (6%)**

  Plantea su ejecución de manera conjunta con los trabajos para el cumplimiento del RGPD, en un plazo de 18 semanas. Listado de tareas a acometer y temporalidad muy detalladas mediante Gannt y listado del apartado 9.2. Análisis original (documental y reuniones) para establecer el GAP con los objetivos a alcanzar. Guía en el Decálogo del CCN, uso de sus herramientas y de la que aportan ellos para el seguimiento y medición de grado de cumplimiento y madurez.

  Listado de entregables en cada una de las fases claro y detallado en apartado 12.3 de la oferta.

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

Fase de la auditoría desarrollada por un consultor jurídico especializado Derecho Digital.

Incluye una última fase de acompañamiento a la certificación en caso de que la Consejería se encontrase interesada en ello.

3% + 2% + 0,75%.

- **Criterio 5. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del RGPD (5%)**

  Metodología y descripción similar y conjunta a ENS, aplican mismos comentarios. 2,25% + 1,5% +0,75%

TOTAL BEONESEC (sobre 49%) = 43,30%

4.1.3 Propuesta de CSA.

- **Criterio 1. Especificación del proceso de auditoría**

  Gestión del proyecto basada en PMBOK. Mejora continua: Planificación, aseguramiento y control de Calidad. Auditorías basadas en metodologías como la OSSTMM, ISSAF y OWASP. 15%

  Realización de mapa de arquitectura inicial. Especificación de la dotación de infraestructura necesaria e información a disponer, bien enfocado. Herramientas: Burp Pro, Nessus, OpenVAS y desarrollos propios, no agresivas con los servicios. Herramienta Defect Dojo para seguimiento. 25%

  Propuesta temporal basada en un Gantt, 7 meses para auditoría, 2 meses para ENS y RGPD, con una duración total de entre 9 y 11 meses desde el inicio, detalle de tareas e hitos de entrega de informes y aprobación. Especifica la implantación de la herramienta, carga de datos, etc. Muy completo. 30%

  Equipo: 1 jefe de proyecto + 1 consultor senior + 1 técnico de apoyo + Pool de apoyo (de CSA y de fabricante). Especialistas para ENS y RGPD. Detalle de asignación de esfuerzos/cargas de trabajo en nº de horas x perfil para cada una de las auditorías. 25%

  - 1.1 Auditoría dinámica "caja negra". (6%)

    Esquema de herramientas a emplear en cada fase de las auditorías. Proceso manual, búsqueda de vulnerabilidades y validación de las encontradas por las herramientas. Ciclo de escaneo-validación alternando automático y manual. 4,75%

  - 1.2 Auditoría dinámica "caja blanca". (6%)

    Idem "caja negra", aplica misma metodología y tareas. Aplican mismos comentarios. 4,75%

  - 1.3 Control de acceso: Gestión de roles y permisos. (5%)

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

Listado de actividades correcto, análisis en base a la información proporcionada por el cliente en ficheros y entrevistas más los resultados de caja blanca. 3,80%

- **Criterio 2. Entregables (12%)**

Para auditoría dinámica y estática: 2 informes (ejecutivo y técnico) + Excel con vulnerabilidades + PowerPoint con resumen/presentación de resultados de la auditoría. Para auditoría de roles y permisos: 2 informes (ejecutivo y técnico) + PowerPoint con resumen/presentación de resultados de la auditoría. 3%

Los dos formatos indicados en el pliego, digital y papel si se solicita. Plantilla de Consejería o propia. Carga y seguimiento de resultados en Defect Dojo (en CSA o en cliente), formación para usarla. 3%

En los anexos entregan informes de ejemplo. Muy completo. 6%

- **Criterio 3. Formación (9%)**

Metodología a escoger presencial o telemática. Formato teórico práctico, proporciona un sistema vulnerable para estudiar, realización de ejercicios y evaluación. 2,5%

40 horas en 8 jornadas de 5 horas c/u presenciales para 15-20 personas. Entrega de documentación escrita. Personal docente con amplia experiencia. 2,5%

Presenta los 7 temas, y desarrollo del T1 y T3. Adicionalmente ofrece 6 horas (temas 8 y 9) para formación ENS y RGPD. 3%

- **Criterio 4. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del ENS (6%)**

Planificación del GAP, entrevistas con responsables, análisis de riesgos y entrega de resultados. Metodología basada en CCN-CERT. 2,75%

Recursos específicos especialistas en la materia. Detalle de asignación de recursos/horas de dedicación. 2%

Entregables: informe GAP, plan de actuación, declaración de aplicabilidad. 0,75%

- **Criterio 5. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del RGPD (5%)**

También propone un informe GAP de cumplimiento de RGPD, entrevistas con responsables y análisis con MAGERIT. 2%

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

Recursos específicos especialistas en la materia. Detalle de asignación de recursos/horas de dedicación. 1,5%

Entregables: informe GAP, análisis de riesgos sobre protección de datos con conexiones con nueva LOPD y plan de actuación. 0,75%

TOTAL CSA (sobre 49%) = 43,05%

4.1.4 Propuesta de ICA.

- **Criterio 1. Especificación del proceso de auditoría**

  Describe unas fases de realización del proyecto que incluye, en la inicial, el establecimiento de la metodología a seguir. 5%

  Descripción de las tareas a realizar a muy alto nivel. Enfoque pobre. 10%

  No aporta planificación ni asignación de recursos propia. 10%

  Indica que en las reuniones de lanzamiento se determinarán los alcances de las actividades, planificación de tareas y asignación de recursos. 7,5%

  - 1.1 Auditoría dinámica "caja negra". (6%)

    Descripción de actividades de pentesting a alto nivel, no detalla metodologías ni herramientas. 0,98%

  - 1.2 Auditoría dinámica "caja blanca". (6%)

    Idem caja negra, aplican mismos comentarios. 0,98%

  - 1.3 Control de acceso: Gestión de roles y permisos. (5%)

    Entrevistas con los implicados, estudio de procedimientos, identificación de controles implementados. Evaluación de la coherencia entre políticas definidas y su implementación. Entregable plan de acción para corrección de brechas. 1,30%

- **Criterio 2. Entregables (12%)**

  Especifica cada entregable en su apartado correspondiente: plan de trabajo inicial, detalle de vulnerabilidades, resultados de las herramientas, auditoría estática con ejecutivo, técnico y plan de acción. Roles: informe de debilidades, plan de acción. 3%

  Los dos formatos indicados en el pliego, digital y papel. No hay herramienta. 2,5%

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

Detalle de las pruebas realizadas, aplicaciones auditadas, vulnerabilidades con clasificación, quickwins para subsanación, propuesta de calendario de implantación... 5%

- **Criterio 3. Formación (9%)**

  Metodología a escoger presencial (en instalaciones del cliente) u on line. Entrega de documentación formato digital. 2,5%

  25 horas en jornadas de 8:00-15:00 para 15-20 personas. No detalla equipo docente. 2,5%

  No desarrolla los temas. 0%

- **Criterio 4. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del ENS (6%)**

  Realizarán análisis de riesgos basado en MAGERIT. Detectarán las salvaguardas de ENS y RGPD. Entregan el análisis de riesgos, informe de riegos y plan de mejora. Poco detallado. 1,5% + 1% + 0,75%

- **Criterio 5. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del RGPD (5%)**

  Conjuntamente con ENS. 1,25% + 0,75% + 0,5%

TOTAL ICA (sobre 49%) = 24,50%

4.1.5 Propuesta de INGENIA.

- **Criterio 1. Especificación del proceso de auditoría**

  Metodologías OSSTMM y OWASP. Evaluarán los SSOO, aplicaciones (comerciales y propietarias), web y apss móviles y las infraestructuras de comunicaciones. Propone como opcional acciones de ingeniería social (phising). 15%

  Proceso estructurado en fases. Certficación de acciones correctoras (6 meses de plazo) con nueva ejecución de pruebas. 30%

  Divide el proyecto en paquetes de trabajo: auditoría, control de roles, formación, ENS/RGPD y un paquete de gestión integral que contempla mecanismos de gestión de riesgos para posibles desviaciones. 25%

  Cronograma detallando actividades por semanas contemplando los 12 meses previstos. Detalla a los integrantes del equipo de trabajo y la asignación a cada tarea de los paquetes. Muy correcto. 25%

  - 1.1 Auditoría dinámica “caja negra”. (6%)

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

Fases estándar de reconocimiento, análisis (escaneo), acceso (explotación) y presentación de resultados. Listado detallado de las herramientas a emplear. 5,23%

- 1.2 Auditoría dinámica "caja blanca". (6%)

  Misma metodología y herramientas pero con credenciales, intento de escalada de privilegios, etc. Bien especificado. 5,23%

- 1.3 Control de acceso: Gestión de roles y permisos. (5%)

  Se tienen en cuenta los controles de ENS que aplican y otros estándares de buenas prácticas (NIST, ISO 27001). Estructurado en el proceso AS-IS -> GAP-> TO-BE. Analiza los procedimientos existentes para la asignación. Entrevistas con los responsables. Resultados de Caja Blanca. Herramienta CLARA del CCN. Muy completo. 4,75%

- **Criterio 2. Entregables (12%)**

  Relación de entregables por cada uno de los paquetes de trabajo. En caja negra y caja blanca informe ejecutivo y técnico. En control de roles y ENS/RGPD Plan de mejora. Mecanismo para control de calidad hasta versiones definitivas aceptadas por el cliente. 3%

  Formatos: Los dos indicados en el pliego, tanto digital como en papel. 2,5%

  Contenido: especificación de los metadatos. Bien detallados los apartados de cada informe. Siempre hay presentación ejecutiva. 6%

- **Criterio 3. Formación (9%)**

  Enfoque metodológico estructurado en 5 fases. Contenidos específicos según perfil de los asistentes (desarrolladores, administradores, etc). Acción 1 Desarrollo software: 30 horas de duración. 15-20 personas, perfiles TIC. Acción 2 Seguridad de procesos para administradores y auditores. 15 horas. Acción 3 Buenas prácticas. 2 horas. Sesiones presenciales (talleres) y webinars. Pruebas de suficiencia y mecanismos de evaluación. 3% + 3% +2%

- **Criterio 4. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del ENS (6%)**

  Abordan ENS y RGPD de forma conjunta dadas las sinergias. Enfoque AS-IS -> GAP -> TO-BE. Misma metodología que gestión de roles, alineada en cuanto a las medidas de seguridad del ENS para control de acceso. Análisis de riesgos con MAGERIT y herramienta PILAR. Descripción detallada de actividades. Los entregables y planificación están en los apartados comunes. Muy completo. 2,75% + 1,75% + 1%.

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

- **Criterio 5. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del RGPD (5%)**

  Abordan ENS y RGPD de forma conjunta. Aplican mismos comentarios. 2,25% + 1,25% + 1%.

TOTAL INGENIA (sobre 49%) = 44,70%

4.1.6 Propuesta de S2GRUPO.

- **Criterio 1. Especificación del proceso de auditoría**

  Metodología OSSTMM, OWASP y GIAC del SANS Institute. Amplio listado de herramientas detallado en anexos por categorías, muy completo. 15%

  Fases de la auditoría dinámica (caja negra y blanca) bien estructuradas, definidas y explicadas, emplean las técnicas de test de intrusión avanzado y movimiento lateral si llega a comprometerse el sistema. 25%

  RRHH: 1 Jefe de Proyecto + 1 Consultor senior + 1 Consultor junior. Estimación de carga de trabajo (horas x perfil) para cada auditoría. 30%

  Presentan planificación temporal con porcentaje de dedicación/horas necesarias para cada servicio. 12 meses. Faltaría Gantt con desglose de actividades e hitos con más nivel de detalle. 20%

  - 1.1 Auditoría dinámica "caja negra". (6%)

    Muy detallado, con metodología, desglose de actividades, detección de vulnerabilidades, control, acuerdo para explotación con el cliente, movimiento lateral. Descripción de las técnicas de descubrimiento. No hace referencia a la validación posterior de la corrección de errores. 4,5%

  - 1.2 Auditoría dinámica "caja blanca". (6%)

    Idem "caja negra", aplica misma metodología y tareas. Aplican mismos comentarios. 4,5%

  - 1.3 Control de acceso: Gestión de roles y permisos. (5%)

    Tareas a alto nivel: verificación mecanismos de autorización, poco detalle. 2,70%

- **Criterio 2. Entregables (12%)**

  Para auditorías estática, dinámica y roles: documento de activos, Informe técnico de auditoría (con contenido y epígrafes suficientes: resumen ejecutivo, resultado técnico, pruebas de concepto, mitigación de vulnerabilidades, ...), presentación, informes de alertas (vulnerabilidades

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

críticas/urgentes encontradas sin esperar a informe técnico). Ejemplo de Análisis de riesgos para ENS. 2%+2%+5%

- **Criterio 3. Formación (9%)**

  30 horas para 15-20 personas. Plataforma ZOOM webinar. Docente analista senior experto. Se abordan los 2 temas propuestos en PPT. 2%+1%+3%

- **Criterio 4. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del ENS (6%)**

  Propone realizar las actividades comunes a ENS y RGPD de forma conjunta. Análisis de Riesgos según MAGERIT con herramienta PILAR. 2%

  La planificación de tareas y el detalle de entregables en apartados comunes de la oferta y especificados aquí en tabla de hitos y entregables: informe de situación y plan de iniciativas. 1,5% + 0,75%

- **Criterio 5. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del RGPD (5%)**

  Conjuntamente con ENS. 1,75%+1%+0,75%

TOTAL S2GRUPO (sobre 49%) = 33,55%

4.1.7 Propuesta de SOTHIS.

- **Criterio 1. Especificación del proceso de auditoría**

  Gestiona el proyecto basándose en fases de puesta en marcha (6 semanas), prestación y devolución (8 semanas), aporta planificación y matrices RACI. Herramienta colaborativa para gestión TEAMS. 12%

  Para auditorías: Metodología integral contempla aplicaciones e infraestructura. Centro experto de operaciones de seguridad ERIS-CERT y Read Team -> priorizando pruebas manuales frente al uso de herramientas. 25%

  Aporta planificación global de gestión del proyecto con porcentajes de dedicación a cada tarea de los componentes del equipo (JP, jefe Red Team, Consultor SOC y consultor técnico). Para la ejecución oficina de auditorías con pool de recursos. 25% + 15%.

  - 1.1 Auditoría dinámica "caja negra". (6%)

    Aplica Guía de Seguridad CCN STIC-812 y OWASP (aquí aparecen ya pruebas de gestión de roles). OWASP, OSSTMM, NIST, OWISAM (redes inalámbricas). Listado de herramientas (Burpsuite, Gobuster, Goca...). Fases estándar (escaneo, explotación...) incluye técnicas de movimiento lateral y persistencia. 3,08%

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

- 1.2 Auditoría dinámica "caja blanca". (6%)

  Idem "caja negra", aplica misma metodología y tareas. Aplican mismos comentarios. 3,08%

- 1.3 Control de acceso: Gestión de roles y permisos. (5%)

  Metodología OWASP mencionada en auditoría dinámica, especialmente los controles de 3.0.1: verificación de autenticación y verificación de control de acceso. 2,31%

- **Criterio 2. Entregables (12%)**

  Para cada trabajo un informe ejecutivo y uno técnico. Entrega en papel y digital en los dos formatos del pliego. Paneles de visualización Tenable SecurityCenter de su ERIS CERT. Detalle de contenido de cada informe y aporta ejemplos. Ofrecerán varias alternativas de mitigación. 3% + 3% + 6%.

- **Criterio 3. Formación (9%)**

  Consensuado con Consejería, presencial u online y número de sesiones. 15-20 personas, no más de 30 horas, según pliego. Entorno colaborativo TEAMs para seguimiento on line de las sesiones. 3%

  Metodología que emplea la gamificación como estrategia de motivación con herramienta KAHOOT. Seguimiento a través de cuestionarios de satisfacción y evaluación final. 3%

  Desarrollo muy completo de los contenidos de los dos temas. 3%

- **Criterio 4. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del ENS (6%)**

  Revisión en base a la Guía CCN STIC-808, empleando metodología MAGERIT para análisis de riesgos con herramienta PILAR. Recopilación de documentación y análisis: inventario de activos, identificación de amenazas y salvaguardas, etc hasta obtener el GAP y el posterior plan de tratamiento del riesgo. 2,75%

  Especifica planificación con porcentajes de dedicación de los recursos. 2%

  Entregables: GAP inicial, valoración ENS, actualización GAP. Plan de tratamiento. 0,75%

- **Criterio 5. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del RGPD (5%)**

  Empleará la revisión de ENS anterior que es aplicable y además revisarán puntos de cumplimiento de normativa legal: información de derechos y consentimiento de interesados, uso de cookies, avisos y cláusulas, finalidad de los tratamientos,... adicionalmente revisión técnica según OWASP de los controles que afectan a disponibilidad, integridad y confidencialidad de la información. 2%

  Especifica planificación con porcentajes de dedicación de los recursos. 1,5%

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

Entregables: esquema de riesgos RGPD y plan de acción. 0,75%

TOTAL SOTHIS (sobre 49%) = 39,22%

4.1.8 Propuesta de TELEFÓNICA.

- **Criterio 1. Especificación del proceso de auditoría**

  Metodologías OSSTM y OWASP, 4 fases estándar: descubirmiento, activos, explotación, recomendaciones y evaluación de la aplicación de las mismas. Clasificación según CVSS (miembro del FIRST). 15%

  Herramientas especializadas: nessuss, acunetix, metasploit, nexpose... y técnicas manuales. Una vez entregado el informe se certificará la corrección de las vulnerabilidades. Seguimiento mediante portal web de gestión de vulnerabilidades. Se auditará la red, aplicaciones y servidores. 25%

  Planificación de roles y permisos en 3 actividades y 3 semanas. Nada más del resto de trabajos. 10%

  No hay ningún detalle de recursos asignados. 7,5%

  - 1.1 Auditoría dinámica "caja negra". (6%)

    Basado en el enfoque general. Propone test de intrusión interno y externo (aunque sin conocimientos de infraestructura o credenciales.) Alto nivel. 2,01%

  - 1.2 Auditoría dinámica "caja blanca". (6%)

    Idem "caja negra", pero con credenciales. Aplican mismos comentarios. 2,01%

  - 1.3 Control de acceso: Gestión de roles y permisos. (5%)

    Propone un enfoque metodológico de evaluación de 5 dominios para identificar el nivel de madurez de la gestión actual y plan de proyecto con fases que incluyen entrevistas, recopilación de información en cuestionarios, etc para revisar políticas y procedimientos. Entrega informe de situación AS-IS y listado de recomendaciones. 2,01%

- **Criterio 2. Entregables (12%)**

  Auditorías informe ejecutivo + técnico + análisis de código. Roles en su apartado. ENS y RGPD. 2%

  Formatos digital y papel encuadernado en los dos exigidos en pliego. Además, todos subidos al portal de gestión. Ilustra con un ejemplo. 3%

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

Aporta las pruebas realizadas, vulnerabilidades, método de explotación, recomendaciones de corrección. Correcto. 5%

- **Criterio 3. Formación (9%)**

  15-20 personas en instalaciones de Consejería o según pandemia online. Acceso a plataforma Cyberacademy+ durante 3 meses. 3%

  7 temas, personal docente especializado, listado detallado, calendario tentativo (30 horas), descripción de metodología, contenidos prácticos, seguimiento y evaluación. 3%

  Poco detallados los contenidos. 1%

- **Criterio 4. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del ENS (6%)**

  Visión integral ENS+RGPD. Análisis de riesgos con MAGERIT, detalle de insuficiencias y plan de mejora con categorías de las tareas. 2%

  Plazos estimados de implementación y prioridad. Correcto. 1,25%

  Entregables en apartado común: análisis de riesgos, GAP, declaración de aplicabilidad, plan de mejora integrado. 1%

- **Criterio 5. Especificación del proceso de identificación de cambios de configuración en INFOLEX que ayuden al cumplimiento del RGPD (5%)**

  Integrado en anterior, plan de mejora continua ciclo de Deming. 1,75% + 1% + 0,75%

TOTAL TELEFÓNICA (sobre 49%) = 30,79%

© 2017 Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A.

5 RESUMEN DE LAS PROPUESTAS Y CONCLUSIONES

Se muestran los resultados anteriores de forma agregada:

Nº	CRITERIO	VALOR	AYESA	BeOneSec	CSA	ICA	INGENIA	S2GRUPO	SOTHIS	TELEFÓNICA
1	**Especificación del proceso de auditoría**		50,00%	90,00%	95,00%	32,50%	95,00%	90,00%	77,00%	57,50%
	1.1Auditoría dinámica "caja negra"	**6%**	1,75%	4,50%	4,75%	0,98%	5,23%	4,05%	3,08%	2,01%
	1.2Auditoría dinámica "caja blanca"	**6%**	1,75%	4,50%	4,75%	0,98%	5,23%	4,05%	3,08%	2,01%
	1.3 Control de acceso: gestión de roles y permisos	**5%**	1,38%	4,05%	3,80%	1,30%	4,75%	2,70%	2,31%	2,01%
2	**Entregables**	**12%**	7,00%	11,00%	12,00%	10,50%	11,50%	9,00%	12,00%	10,00%
3	**Formación**	**9%**	7,00%	9,00%	8,00%	5,00%	8,00%	6,00%	9,00%	7,00%
4	**Especificación del proceso de identificación de cambios de configuración en GEA que ayuden al cumplimiento del ENS**	**6%**	4,50%	5,75%	5,50%	3,25%	5,50%	4,25%	5,50%	4,25%
5	**Especificación del proceso de identificación de cambios de configuración en GEA que ayuden al cumplimiento del RGPD**	**5%**	2,75%	4,50%	4,25%	2,50%	4,50%	3,50%	4,25%	3,50%
TOTAL		**49%**	**26,13%**	**43,30%**	**43,05%**	**24,50%**	**44,70%**	**33,55%**	**39,22%**	**30,79%**

A la vista de los resultados obtenidos se pospone la proposición de adjudicatario a la valoración de los criterios que se evalúan aplicando formulas.

© 2017 Sociedad Andaluza para el Desarrollo de de las Telecomunicaciones S.A.
Este documento y, en su caso, cualquier documento anexo al mismo, contiene información de carácter confidencial exclusivamente dirigida a su destinatario o destinatarios. Queda prohibida su divulgación, copia o distribución a terceros sin la previa autorización escrita de "Sociedad Andaluza para el Desarrollo de la de las Telecomunicaciones S.A..". Si no es Ud. el destinatario del documento le ruego lo destruya sin hacer copia digital o física, comunicando a "Sociedad Andaluza para el Desarrollo de de las Telecomunicaciones S.A." vía e-mail o fax la recepción del presente documento. Toda declaración de voluntad contenida deberá ser tenida por no producida.