INFORME TÉCNICO DE VALORACIÓN TÉCNICA SUJETA A JUICIO DE VALOR
EXPEDIENTE S-00597-2024
"Soporte implantación SGSI y adecuación a ENS"

El presente informe tiene por objeto realizar la evaluación de los criterios que dependen de juicio de valor referido en la cláusula 11ª del Pliego de condiciones generales (PCG) de las ofertas presentadas en el procedimiento de licitación abierto para la adjudicación del contrato "Soporte implantación SGSI y adecuación a ENS".

EMPRESAS LICITADORAS

Se evalúan las ofertas técnicas de cuatro empresas, las cuales se detallan a continuación:

- NUNSYS
- S2 GRUPO
- SISTEMAS INFORMATICOS ABIERTOS, S.A.U., (S.I.A.)
- TELEFÓNICA EMPRESAS

VALORACIÓN DE LOS CRITERIOS

De acuerdo con la cláusula 10ª del PCG anexo II, con la finalidad de adjudicar el contrato valorando la idoneidad del soporte formado por los epígrafes del 1 al 4. Los criterios de valoración están vinculados al objeto del contrato, y a otros aspectos relevantes del servicio, que son de interés para RTVE y que tienen incidencia directa en la calidad en la prestación del servicio e influirán en gran medida en la correcta ejecución del proyecto.

Mediante esta valoración se pretende reflejar en qué medida la oferta presentada, será adecuada para cubrir las necesidades de RTVE.

Criterios de valoración sometidos a juicio de valor (sobre B)	Máximo 29 puntos
1. Memoria de implantación	15 puntos
2. Marco metodológico documental	8 puntos
3. Acuerdo nivel de servicios	3 puntos
4. Plan de formación.	3 puntos

RESULTADOS DE PUNTOS ASIGNADOS A OFERTAS TÉCNICAS CORRESPONDIENTES A CRITERIOS DE VALORACIÓN SUJETOS A JUICIO DE VALOR

De la revisión de las ofertas valoradas, estas obtienen la siguiente puntuación:

- NUNSYS 20,50 puntos.
- S2 GRUPO 25,73 puntos.
- SISTEMAS INFORMATICOS ABIERTOS (SIA) 26,00 puntos.
- TELEFÓNICA EMPRESAS 27,68 puntos.

En la documentación que se refleja a continuación (Anexos I y II) se pueden consultar el detalle de asignación de puntos y la justificación de las puntuaciones asignadas para cada uno de los diferentes apartados.

ANEXO I – TABLA DE ASIGNACIÓN DE PUNTOS DE LAS OFERTAS

		EMPRESAS			
Criterios de valoración sometidos a juicio de valor (sobre B)	**PLIEGO**	**NUNSYS**	**S2 GRUPO**	**SIA**	**TELEFÓNICA**
1. Memoria de implantación	**15 puntos**	11,00	13,00	14,00	15,00
2. Marco metodológico documental	**8 puntos**	5,00	8,00	6,00	8,00
3. Acuerdo nivel de servicios	**3 puntos**	3,00	2,73	3,00	2,18
4. Plan de formación.	**3 puntos**	1,50	2,00	3,00	2,50
TOTAL	**29 puntos**	**20,50**	**25,73**	**26,00**	**27,68**

ANEXO II - EVALUACIÓN DE APARTADOS DE LAS OFERTAS

11.1 MEMORIA DE PROPUESTA DE IMPLANTACIÓN

Incluirá una descripción detallada de la oferta, describiendo cada fase, tareas, responsables, necesidades, riesgos y herramientas que permitirán alcanzar los objetivos en fecha y forma.

El licitador especificará en este apartado la estimación de horas de dedicación al proyecto de los diferentes perfiles que va a emplear en cada fase.

Se valorará con la puntuación máxima de 15 puntos la presentación de la memoria de implantación del SGSI y de la adecuación al ENS que permita asegurar el cumplimiento de los compromisos de ejecución de las tareas que formar parte del objeto de la contratación.

Será tenida en cuenta la especificidad de las tareas, entendidas como propuesta propia del licitador y que desarrollen, a partir de las fases descritas en el punto 4.2 del Pliego de Especificaciones Técnicas (DETALLE DE LA EJECUCIÓN DE LOS TRABAJOS), o de su propia propuesta de implantación, las especificidades de los cometidos orientada al área de actividad específica de CRTVE, la metodología de coordinación de equipos de trabajo, así como la planificación y ejecución de los trabajos, y seguimiento de tareas hasta su cierre.

Para la obtención de puntuación en el presente apartado no será suficiente la mera reproducción de los contenidos descritos en el Pliego de Especificaciones Técnicas, sino que se espera de la propuesta el aporte de datos, procedimientos y compromisos que contribuyan a dotar de valor añadido a la misma.

Revisión de las propuestas

Basado en las fases que se indican en el Pliego de Especificaciones Técnicas, en la revisión de las ofertas de los licitadores se tendrá en cuenta la concreción de sus propuestas al objeto de poder determinar en qué medida implementan procedimientos formales que permitan determinar aspectos que garanticen una adecuada gestión del proyecto. Debemos destacar que la implantación del SGSI, con su especificidad en la adaptación el ENS, forma parte de una metodología, procedimientos y normativa fuertemente regulados conforme a la ISO 27001 y el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. Por dicho motivo, la revisión no se enfoca sobre el cumplimiento de dichos aspectos, que será obviado en sus propuestas por ser preceptivo en la implantación y de obligado cumplimiento, sino sobre "como" tienen previsto los licitantes realizar dichos trabajos.

En este apartado, se valora la profundidad y la amplitud de la propuesta, como demostración de la adaptabilidad a las necesidades o particularidades de RTVE mediante elementos diferenciales que permitan identificar la estrategia de aproximación y el aporte de valor que el licitador considera relevante en las necesidades a satisfacer en la ejecución del servicio.

Siendo las ofertas de los diferentes licitadores un documento abierto a las propuestas que consideran más adecuadas para el buen fin de la implantación, es inevitable la comparación entre las diferentes propuestas, debiendo asignar una mayor puntuación a las que consideran, dentro de su pertinencia, un alcance superior que denota un mayor conocimiento y especialización en los trabajos a desarrollar que puede redundar en garantías sobre el éxito de la implantación.

En base a dicha premisas, a continuación, se destacan las características diferenciales de cada una de las ofertas del presente apartado, así como la puntuación asignada a las mismas:

NUNSYS

Dispone de marcos metodológicos teóricos para gestión de proyectos.

Respecto de las fases iniciales del proyecto su propuesta es meramente enunciativa, pasando a la ejecución sin aporte de detalles en relación a los procedimientos y tareas a realizar en dichas fases.

La fase de planificación se aborda mediante la creación de un conjunto de planes de proyecto que establezcan una hoja de ruta, en la cual se desarrolla la planificación de detalle del proyecto describiendo los hitos a realizar, así como los entregables asociados, teniendo como resultado el Plan Operativo del proyecto.

Incide en el análisis del contexto interno y externo en la planificación de actividades a través del modelo DAFO, remitiéndose a las guías CCN-STIC para la definición de las políticas y roles a implantar, así como en la valoración de los activos del sistema de información.

En cuanto al análisis de riesgos, considera la necesidad de establecer los criterios de aceptación del riesgo y un inventario de activos de soporte como soporte de los activos esenciales a proteger. Para la identificación y valoración de los escenarios de riesgo dará uso de la herramienta PILAR para el análisis de riesgos poniendo a disposición de RTVE una plataforma propia (GConsulting Compliance), que permite importar y exportar a PILAR y agilizar la gestión en nube.

El plan de implementación considera la elaboración de la Política de Seguridad, 4 Normas y 12 Procedimientos, que cubren las necesidades estimadas por el licitador, proponiendo la implantación de controles para el Cuadro de Mando en base a la Guía 824 del CCN – Anexo C, sin información relevante adicional.

Para las fases de seguimiento y revisión del SGSI, y conformidad con el ENS realiza una aproximación a los trabajos a realizar de nivel medio, acudiendo a lo dispuesto en las guías del CCN-CERT 808 de Verificación del cumplimiento del ENS y la 804 Guía de implantación del ENS, concluyendo con un Plan de Acción, orientadas a subsanar las no conformidades detectadas en el proceso de revisión, junto con un calendario propuesto de cumplimiento de dichas Recomendaciones, convenientemente priorizadas, incluyendo el acompañamiento y defensa en la auditoría de tercera parte o externa durante el proceso de auditoría de certificación.

Para la última fase de la implantación, propone realizar los cuadros de mando que permitan reflejar el cumplimiento y el seguimiento de la evolución del SGSI, así como la herramienta del CCN incluida en la Guía 824 del CCN – Anexo C, teniendo en cuenta KPi, actualización del Marco normativo, revisión del estado de controles y modelo de monitorización, entre otros.

Podemos concluir que NUNSYS aborda el proyecto de forma rigurosa en base a las normas y guías que regulan la implantación de los SGSI y ENS, demostrando conocimiento en el marco teórico de implantación. Si bien concreta las actividades de todas las fases conforme a un marco general de actuación, su punto más débil se deriva de una profundización media en la descripción de actividades y tareas a bajo nivel, en especial en lo referente a la interacción entre el equipo de NUNSYS y de RTVE en la realización de las diferentes tareas.

Puntos asignados a NUNSYS en el presente apartado: ***11 puntos***

S2 GRUPO

Para la fase de estructuración aporta aspectos organizativos y de coordinación del proyecto, desde una perspectiva amplia intentando aterrizar el proyecto sobre parámetros iniciales bien documentados.

S2 considera la fase de planificación, no solo como un modelo teórico, sino como un conjunto de actividades con un elevado nivel de concreción tanto en relación con la definición de las tareas como en la interacción entre equipos de trabajo, lo que puede permitir un desarrollo controlado de todo el proyecto a lo largo de su vida.

Su fase de implementación, habiendo realizado el grueso de actividades de campo en la fase anterior, manifiesta la importancia de generar y consolidar un sistema documental, aportando propuesta de desarrollo de diferentes documentos, normas y procedimientos a implantar.

Acude al cuadro de mandos, realizado en la fase anterior, y a un Plan de Auditoria Interna para la verificación del cumplimiento previo al trabajo de certificación por parte de auditor externo. Sin ser prolijo en esta fase, las tareas se estructuran de forma equilibrada y racional, coherente con la evolución esperable.

La Fase 5, adicionalmente a la elaboración y entrega del informe INES, considera todas las tareas de apoyo en relación a la subsanación de no conformidades, consolidación documental, evidencias y acompañamiento en entrevistas.

La última fase aborda los procesos de mejora continua con la metodología clásica PDCA, destacando la elaboración de informes mensuales de la evolución del Plan.

Podemos concluir que la oferta, en este apartado, responde de forma amplia y precisa a los diferentes hitos de desarrollo del proceso de implantación, abarcando todas las tareas y con capacidad de adaptación al desarrollo de la implantación.

Puntos asignados a S2 Grupo en el presente apartado: ***13 puntos***

SISTEMAS INFORMATICOS ABIERTOS (SIA)

SIA aporte dos modelos específicos en su plan mediante un Sistema Integrado de Gestión y un Modelo Unificado de Controles (MUC) que unifica diferentes controles de seguridad incluidos en los estándares objeto de la presente licitación.

Considera en la estructuración aspectos relevantes tanto organizativos a nivel documental como de distribución de tareas entre los diferentes actores que participarán en la implantación, coherentes y adecuados a la previsible necesidad.

Destaca, en la fase de planificación, el modelo adaptativo a con un marco de controles unificado que permitiría racionalizar las tareas para los diferentes estándares, así como los objetivos concretos de las tareas

En la implementación, SIA propone se solventen las deficiencias detectadas o las ausencias de cumplimiento en las fases anteriores, proponiendo y desarrollando un marco normativo en el que se enmarquen las principales normas y procedimientos.

Resulta adecuado el concepto de niveles de tratamiento (estratégico, táctico y operativo) por la nitidez en el desarrollo, creación, definición y distribución de tareas, así como asignación de las mismas entre los diferentes actores.

La fase de seguimiento y revisión del SGSI presenta un elevado nivel de detalle, de amplio espectro de actividades y concreción, lo que repercute en la capacidad de seguimiento supervisión de las tareas comprometidas. Si bien esta fase dependerá de la ejecución de tareas previas, se observa un elevado nivel de supervisión de dichas actividades lo que redunda en la calidad del trabajo final, lo cual se debe reflejar en las tareas de conformidad con el ENS donde SIA ejecutará las tareas necesarias para el alineamiento de CRTVE con los requisitos del ENS, priorizando aquellas actividades que requieran de atención inmediata y puedan ser resueltas de forma factible antes de la auditoría.

La fase final se considera de forma proactiva mediante la actualización permanente del cuadro de mandos y el seguimiento continuo del cumplimiento del marco normativo y la difusión de acciones orientadas a conseguir el compromiso con los procesos por parte de los involucrados en el mantenimiento del SGSI.

Podemos concluir que, la oferta de SIA es muy completa y va más allá de su forma de implementación, realizando una buena interrelación entre las actividades, con gran nivel de detalle en las mismas, y los entregables que se derivan de ellas.

Puntos asignados a SIA en el presente apartado: ***14 puntos***

TELEFÓNICA EMPRESAS

Presenta en la fase de estructuración un desglose de actividades con un alcance muy amplio y de alto nivel de detalle. Busca desde el inicio establecer una planificación consolidada con objetivos definidos y orientados a prestar un desarrollo del servicio con parámetros claros del marco de actuación del proyecto.

La planificación se realiza a través de un enfoque muy estructurado, con descripción de los diferente enfoques que regirán la implantación (corporativo, organizativo, negocio, aplicación, tecnología,...), presentando diferentes opciones a RTVE, permitiendo a RTVE flexibilizar la implantación en función del desarrollo de los trabajos, pero a su vez incidiendo en la responsabilidad de RTVE en las decisiones relativas a cumplimiento y compromisos y describiendo las diferentes interrelaciones entre objetivos y procedimientos.

La implantación se realiza a través de un plan de mejora y, posteriormente, en los procedimientos y normativas necesarias que sustentará las normas que deberán respetarse en la entidad para que el tratamiento de información se realice de forma segura. El detalle del plan incluye las acciones de implantación dentro de cada una de las tareas que considera, categorización, documentación, plazos de ejecución, presupuestos, etc. El detalle del plan proporciona una elevada capacidad de control de los parámetros de implementación que afectan a los controles que posteriormente darán lugar a la certificación del ENS.

La propuesta incide en la necesidad de disponer de un marco normativo adecuado, proporcionando un escenario mínimo de normas a desarrollar de una extensión que permitirá a RTVE disponer tanto de normas como de procedimientos en un elevado número de actividades, siendo de gran utilidad tanto en la desambiguación de responsabilidades como en la operación diaria en los diferentes ámbitos de actuación, incluyendo dentro de su Solución de Gestión Integral de Riesgos funcionalidades especializadas en el ámbito de la Administración Pública, específicamente en el cumplimiento del Esquema Nacional de Seguridad.

El seguimiento y revisión del SGSI se plantea como la confirmación de que todo lo anteriormente desarrollado es acorde con los niveles de seguridad exigidos por RTVE. Tras los procesos de revisión, planteado como preauditoría de los ejecutado, se concluye con un Procedimiento de Revisión por parte de la Dirección que incluye las decisiones relativas a las oportunidades de mejora continua y las necesidades de cambios del SGSI.

Tras el acompañamiento en la fase de auditoría externas se elaborarán los Planes de Acciones Correctivas centradas en la corrección inmediata de las no conformidades, pudiendo dejar las observaciones u oportunidades de mejora para el futuro.

Telefónica considera, de forma independiente a las fases mencionadas, el servicio de soporte con funciones de ejecución continua incluyendo, entre otros, asesoramiento legal y técnico, identificación de forma temprana de nuevos requisitos aplicables a la Seguridad de la Información, apoyo a nuevas iniciativas mediante labores de consultoría y apoyo técnico en los proyectos de RTVE así como asesoramiento sobre la gestión de incidencias y vulnerabilidades.

La oferta de Telefónica cubre todas las necesidades planteadas en la implantación, asume la necesidad de RTVE de dotarse de un SGSI que considere tanto la amplitud de actividades como la penetración en todas las capas de la organización de cara a disponer de un método permanente de gestión de la seguridad de la información con controles efectivos sobre la misma.

Puntos asignados a Telefónica en el presente apartado: ***15 puntos***

11.2 MARCO METODOLÓGICO DOCUMENTAL

Descripción del marco metodológico a utilizar, ventajas del uso de este marco destacando aceleradores que permitan alcanzar los objetivos.

Se valorará la metodología y disponibilidad de herramientas que permitan el seguimiento de los avances de los trabajos, y de repositorio documental de documentos de trabajo sin coste alguno para RTVE.

Se valorará con la puntuación máxima de 8 puntos la presentación de la metodología seguida para asegurar la calidad de los entregables generados/solicitados por la Dirección de Seguridad Corporativa o por el CISO, así como la gestión de la documentación generada (actas, normas, procedimientos, circulares, formación, ...), control de versiones, y sistema de intercambio de archivos y/o documentación, acorde a los procedimientos para el tratamiento, en su caso, de información clasificada.

Revisión de las propuestas

La revisión de las ofertas de los licitadores, en el presente apartado, tienen en cuenta la concreción de sus propuestas al objeto de poder determinar en qué medida implementan procedimientos formales que permitan determinar aspectos que garanticen una adecuada gestión del proyecto.

A continuación, se destacan las características de cada una de ellas:

NUNSYS

Modelo de relación con RTVE considera la constitución de dos comités:

- Comité de Seguridad Estratégico (con una periodicidad de reuniones trimestral) con las funciones de:
  - Revisión del estado de avance de planes de tratamiento de Riesgos y mejoras.
  - Presentar el estado de madurez de controles de seguridad aplicables.
  - Revisión de los Indicadores de Seguridad.
  - Revisar las incidencias acaecidas en el periodo y proponer medidas correctivas.
  - Revisión de resultado de Análisis de riesgos realizados.
  - Aprobación formal del apetito al riesgo de RTVE, y los planes de tratamiento del riesgo.
  - Fijar nuevos objetivos de mejora de seguridad y seguimiento de las actividades y tareas.
  - Revisar el resultado de auditorías de seguridad periódicas y seguimiento de No conformidades y acciones de mejora registradas.
  - Resultados de la formación y concienciación realizada.
  - Resolución los conflictos de responsabilidad, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
- Comité táctico y Operativo (con una periodicidad de reuniones mensual), con las siguientes funciones:
  - Presentación de la información del estado real del proyecto (Plan de Servicio).
  - Informar acerca de la gestión de recursos.
  - Presentar y gestionar los riesgos, problemas e incidencias del servicio, y hacer un seguimiento hasta el cierre de estos
  - A nivel más operativo de la actividad propia de seguridad:

- Seguimiento del estado de madurez de controles de seguridad aplicables.
- Seguimiento de los Indicadores de Seguridad del periodo.
- Revisión de incidencias acaecidas en el periodo y realizar el aprendizaje de los mismos de cara a proponer Medidas que eviten que vuelvan a reproducirse en el futuro.
- Seguimiento de las actividades que se realizan en el ámbito de los planes de tratamiento del riesgo.
- Seguimiento de las actividades y tareas de objetivos de seguridad.
- Seguimiento de No conformidades y acciones de mejora registradas producto de las auditorias y mejoras detectadas de forma interna.
- Resultado y seguimiento de acciones de formación y concienciación.
- Protección de la seguridad de la información de carácter personal

Nunsys se ofrece a emplear las herramientas de gestión y reporting estándar de RTVE, si bien pone a disposición sin coste adicional, en caso de que el RTVE considere el uso de las mismas, las siguientes:

- Herramienta de comunicación y colaboración de equipos de trabajo Microsoft Teams
- Herramienta de gestión de servicios Service Desk Plus
- Herramienta de seguimiento del servicio, basada en Power BI

Propone un método simplificado de clasificación (en tres niveles) para facilitar el proceso de aceptación de la documentación a elaborar.

Asume la redacción de las correspondientes actas de reunión de los comités de seguimiento, quedando a disposición de RTVE en el repositorio documental propuesto (gestor colaborativo a través de MS Teams).

Define un Sistema de Gestión de Calidad (SGC) basado en la norma ISO 9001, disponiendo de una unidad específica (Oficina de Calidad de Proyectos y Servicios – OCPS) orientada a garantizar que los proyectos y servicios de la compañía se ofrezcan con la calidad definida, proponiendo una herramienta de control de la misma y articulando las actividades consideradas (objetivos, desviaciones, homogeneización, roles) así como la definición del Plan de Calidad a implementar en el proyecto, incluyendo auditorías periódicas, verificación de las entregas y validación del alcance enfocado a:

- Asegurar que todas las actividades relacionadas con la ejecución del proyecto se rigen en términos de calidad, según lo establecido en el Plan de Calidad.
- Asegurar que se respetan los acuerdos contraídos contractualmente con el cliente en aspectos relacionados con la calidad.
- Garantizar que las desviaciones que se produzcan entre la planificación efectuada y la realidad sean mínimas, y en caso de producirse, se controlen acotando sus efectos previstos en tiempo y en coste.
- Detectar y actuar sobre las deficiencias reales o potenciales que se puedan producir.
- Estandarizar y normalizar la metodología de trabajo y los productos a obtener.
- Homogeneizar la documentación asociada a los proyectos y disponer de la documentación mínima asociada a las aplicaciones que den soporte a la organización.
- Establecer roles y responsabilidades asociados a los entregables propuestos.
- Ser flexible y útil, estableciendo una metodología que sea flexible en función de las necesidades reales de los proyectos.
- Posibilitar la reutilización de software y documentación, minimizando tiempos de desarrollo.
- Adecuar el servicio a las expectativas y necesidades reales.
- Facilitar el acceso y la difusión de la información mediante un repositorio único de información de la metodología y de la documentación asociada a los proyectos que sea accesible por toda la organización.

Propone la recopilación de toda la información con el objetivo de elaborar un Plan de Calidad completo y realista. La información a recopilar será:

- Planes de Calidad que pudieran existir en el cliente.
- Plan de trabajo del proyecto revisado.
- Procedimientos y estándares de calidad del cliente.
- Plantillas de documentos y presentaciones, así como el formato establecido en el cliente.

- Obtener las lecciones aprendidas de proyectos relacionados con el objeto del servicio es clave a la hora de elaborar el Plan de Calidad porque permitirá poner el foco en aquellos aspectos más relevantes.
- Riesgos y problemas detectados relacionados con la calidad.
- Métricas e indicadores del cliente alineados con calidad de servicio

Puntos asignados a NUNSYS en el presente apartado: ***5 puntos***

S2 GRUPO

El Plan de gestión del servicio está soportado por los procesos del Sistema de Gestión Integrado de S2 Grupo, certificado de acuerdo con los estándares ISO 20000-1, ISO 22301, ISO 27001, ISO 9000, ISO 14001, ISO 166002, ENS con categoría ALTA. Considera procesos del sistema directamente aplicables al servicio (Gestión de incidencias, peticiones y problemas, Gestión de la capacidad y el rendimiento, Gestión de la seguridad, Gestión de riesgos, Gestión de la colaboración y Gestión de calidad).

La plataforma de gestión del servicio (denominada emas®) permite el seguimiento de los niveles de servicio comprometidos, siendo documentados en el sistema de gestión con los identificadores:

- PS7G.- Gestión de incidencias y peticiones de servicio
- PS7H.- Gestión de problemas

La gestión de incidencias y peticiones contempla la generación de documentación asociada, análisis y clasificación de cada incidencia que ocurra durante el desarrollo del proyecto, clasificándola en los distintos tipos de incidencias definidos y tratamiento específico incluyendo un estudio del impacto de la incidencia y una solución propuesta por S2 Grupo al cliente, para la valoración de RTVE.

Plantea la necesidad de realizar una clasificación/catálogo de peticiones e incidencias, cada uno de los cuales contará con las correspondientes definiciones y SLAs asociados.

Para la gestión de la capacidad dispone de un proceso específico (PS7E.-Gestión de la Capacidad) para planificar la provisión del servicio optimizando los recursos mediante el balanceo de carga entre diferentes servicios según las tendencias de la demanda, teniendo en cuenta:

- Demanda actual y prevista
- Dedicación actual de los recursos y capacidad disponible
- SLAs actuales y previstos
- Posibles cambios organizativos, así como inversiones en infraestructura y tecnología

Para la Gestión de la Capacidad de Recursos Personales, mensualmente la dirección de la unidad técnica elabora su plan de capacidad de personas que considera los proyectos y servicios en curso más la previsión de lo entrante, asignando las personas existentes a los proyectos y servicios e identificando posibles déficits o excesos de capacidad.

Incluye medidas para asegurar la baja rotación del equipo, ejecutando planes muy definidos de carácter correctivo y preventivo para la adaptación a la demanda en picos de trabajo, cobertura a las bajas y ausencias de personal, así como para promover la estabilidad del equipo de trabajo, evitando las rotaciones no deseadas, especialmente críticas en determinados niveles técnicos con elevado conocimiento de la problemática particular de los servicios.

Cuenta con un Plan de Continuidad del Servicio basado en la disponibilidad de personal en la plantilla, aparte del ofertado, que reúne la totalidad de requisitos de solvencia técnica requeridos para prestar el servicio propuesto por lo que, en caso de contingencia, garantizar el aseguramiento del servicio, incluyendo el mantenimiento de una base de datos de candidatos para las diferentes áreas de servicio, así como un proceso continuo de selección y formación de personal. Así mismo, contempla la documentación de todos los procesos y actividades que lo desarrollan, con el objetivo de facilitar la transferencia de conocimiento y minimizar el impacto de un reemplazo de personal.

Complementariamente prevé un plan de sustitución de personal que contempla la reserva de perfiles de respaldo, de manera que, en caso de alguna modificación en el equipo inicialmente previsto, realizará aviso con un mes de antelación, y tras la aceptación del nuevo perfil de respaldo, contempla un periodo de solapamiento entre ambos perfiles de 10 días laborables.

El proceso de gestión de seguridad (PE_5 Gestión de Seguridad de la Información) está certificado de acuerdo con ISO27001 y ENS nivel ALTO, en ambos casos con un alcance que cubre todos los servicios de ciberseguridad prestados y la infraestructura que los soporta, comprometiéndose al cumplimiento de la política de seguridad de la organización, así como la Ley de Protección de Infraestructuras Críticas.

Identifica de forma preliminar y de forma específica la gestión del riesgo del proyecto, dividiendo el mismo en etapas de una forma estructurada para poder identificar el alcance de cada entrega. Evalúa el riesgo de cada entrega, y se determina su impacto y su probabilidad, considerando riesgos externos impredecibles, riesgos internos no técnicos, riesgos técnicos y riesgos legales, en los siguientes ámbitos:

- Gobierno
- Recursos
- Planificación
- Alcance
- Contractuales

Tiene en cuenta la gestión de la colaboración, proponiendo un Plan de Proyecto que servirá como referencia al equipo de proyecto y a todos los involucrados en el mismo, en el cual identificar y documentar los requisitos y las normas de colaboración entre las diferentes entidades que son parte integrante del proyecto.

Respecto de la gestión de la calidad en el proyecto incluye medidas para conseguir que se cumpla la metodología fijando criterios de calidad de los entregables, antes que éstos se desarrollen, asegurando que se alcanzan los estándares de calidad, de acuerdo con lo especificado en el Plan de Calidad, detectando y corrigiendo los incumplimientos de metodología y calidad y controlando la utilización de los documentos de gestión del proyecto.

Propone la creación de un "Archivo de Calidad" para el archivo de:

- Actas de las reuniones de los comités de seguimiento y dirección.
- Plan de Proyecto.
- Informes de Incidencias.
- Peticiones de Cambio.
- Informes de seguimiento del proyecto.
- Cuestionarios de satisfacción del cliente

Como soporte al Jefe de Proyecto, integra su Oficina de Calidad y Mejora Continua (OCMC) como aporte de un enfoque externo e independiente a la Dirección del Servicio, con alcance sobre gestión de reclamaciones (resolución de incidencias durante la prestación del servicio), encuestas de satisfacción (medición sobre la satisfacción del servicio prestado, en base a los formularios), coordinación del diseño y revisión de procesos, así como mejora continua en todos los procesos que intervienen en el servicio.

El modelo de relación para la prestación de servicios, establece un modelo de relación a tres niveles, con comités que se reunirán con la periodicidad que se determine durante el establecimiento del contrato y en la fase inicial del proyecto de implantación del servicio, con independencia del compromiso de llevar a cabo tantas reuniones adicionales como se estime oportuno para garantizar la adecuada gestión del servicio.

Su propuesta considera la constitución de:

- Comité de Dirección. Para la definición de aspectos estratégicos del servicio, con frecuencia de reunión inicial semestral o anual.

- Comité de Seguimiento. Con propuesta de reunión mensual para revisar los informes de control, revisar incumplimientos, riesgos y acciones correctoras, así como verificar el progreso y la mejora continua del servicio.
- Comité Operativo. Con una función eminentemente técnica y práctica, asumirá la coordinación y gestión diaria del servicio y frecuencia de reuniones semanal, o siempre que el servicio lo requiera, para asegurar la resolución de conflictos, revisar las soluciones implantadas y evaluar riesgos y propuestas de mejora.

En lo que respecta a la gestión del conocimiento, esta incluye los informes del servicio, cuadros de mando, los materiales formativos y de concienciación que se desarrollen, así como documentación operativa como políticas, procedimientos, según el siguiente modelo:

- Gestión del cambio y ciclo de mejora continua para la elaboración y mantenimiento de la documentación del servicio
- Organización de la información
- Herramientas para gestionar el conocimiento

Se destaca en este sentido los procedimientos de revisión y aprobación, la clasificación de la información, y la oferta de uso de repositorios propios, así como herramientas de gestión de ticketing e implementación de mecanismos de Control de Accesos por roles otorgados según necesidad de conocer.

También considera el control de calidad de los entregables, destacando la gestión de versiones de los documentos (PSG-01.- Tratamiento y control de la documentación) para el tratamiento documental durante la ejecución del proyecto.

Puntos asignados a S2 Grupo en el presente apartado: ***8 puntos***

SISTEMAS INFORMATICOS ABIERTOS (SIA)

SIA pone a disposición del proyecto una metodología documental propia, tomando como base las Guías del CCN que proporcionan directrices para su elaboración, como pueden ser: CCN-STIC-805 Política de Seguridad de la Información, CCN-STIC-821 Normas de Seguridad en el ENS y CCN-STIC-822 Procedimientos de Seguridad.

Considera las funciones de cada uno de los comités (estratégico y táctico) propuestos en relación al modelo de gestión:

- Comité de Dirección
  Compuesto por:
  - Dirección RTVE
  - Jefe Proyecto RTVE
  - Dirección técnica SIA
  - Dirección Comercial SIA
  - Jefe Proyecto SIA
- Con las siguientes funciones:
  - Gestión y Dirección estratégica del proyecto
  - Aceptación del plan de proyecto actual y sus posibles modificaciones
  - Seguimiento y aceptación de los hitos principales y gestión de las desviaciones del mismo
  - Aprobación de cambios funcionales o de alcance del proyecto y sus posibles implicaciones en el plan y/o presupuesto del proyecto
  - Gestión de los recursos del proyecto (humano, máquinas, puestos de trabajo, ...)

  Con reuniones de periodicidad trimestral
- Comité técnico
  - Jefe Proyecto RTVE
  - Jefe Proyecto SIA
  - Interlocutores clave RTVE

- Equipo técnico SIA

Con las siguientes funciones:

- Seguimiento del cumplimiento del plan de proyecto
- Aprobación de actividades y documentos principales del equipo técnico
- Identificación y gestión de riesgos
- Coordinación de las actividades e información de los distintos equipos
- Obtención y filtrado de la información pertinente para la presentación al comité directivo
- Ejecución de las decisiones tomadas en dicho comité
- Con reuniones de periodicidad mensual

Los criterios del modelo documental consideran:

- Criterios para el Contenido, en relación a los formatos de comunicación, incluyendo los datos referidos a necesidad, objetivo y alcance, aplicabilidad y vigencia.
- Criterios para la Estructura:
  - Personal a quien va dirigido (todos los usuarios, personal externo, personal interno, directivos, personal TIC, personal de Seguridad Lógica, personal de Seguridad Física).
  - Dominios, objetivos o ámbito. Por ejemplo:
    - Identificación y Organización (organización de la seguridad en el negocio y análisis y gestión del riesgo).
    - Protección (gestión de activos e inventario, políticas y normativas, control de acceso lógico y físico, seguridad en explotación y operación, seguridad Sistemas y comunicaciones, seguridad en adquisición y desarrollo de nuevos componentes, formación y concienciación del personal, seguridad física y del entorno, procesos de comunicación).
    - Detección (monitorización continua, procesos de detección de eventos y anomalías, gestión del cumplimiento).
    - Respuesta (comunicación y gestión de incidencias, gestión de vulnerabilidades)
    - Recuperación, continuidad de TI o del Negocio).
- Criterios para Información de Control de los Documentos. SIA propone el desarrollo de normas según la plantilla para documentación de uso en RTVE, recomendando incluir determinados campos. A saber: Título, Fecha, Versión, Área responsable, Responsable y fecha de revisión, Responsable y fecha de aprobación, Tabla para el control de cambios y Lista de distribución)

SIA compromete la generación de un Modelo de Gobierno y un Marco Normativo donde los documentos generados cumplan con los requerimientos de alineación con la estructura, necesidades y particularidades de la Organización, incluyendo todos los requerimientos (en normas) o pasos (en procedimientos) necesarios e incorporando las responsabilidades claras para los implicados y relaciones entre ellos, así como que estén estructurados para conocer cuando unos documentos derivan de otros.

Aporta diagramas de flujo del procedimiento de generación, revisión y aprobación de la documentación generada en el proyecto.

Dentro de marco metodológico contempla tareas que permitan garantizar la continuidad, calidad y fiabilidad del servicio:

- Organización y gestión del servicio: Roles y responsabilidades de los recursos asignados al servicio.
- Comunicación: Canales de interlocución.
- Parámetros de Medida: Determinación de los factores a controlar de cara a obtener la medida del nivel de servicio alcanzado.
- Asignación de recursos: Disponibilidad y utilización de los recursos tanto humanos como técnicos involucrados en la prestación del servicio.
- Control: Calendario de reuniones de supervisión.
- Dado uso a indicadores de medición de la calidad:
  - Satisfacción: Grado de éxito de las actuaciones realizadas para cubrir los requisitos establecidos.

- Uso: Utilización de la documentación para la prestación del servicio de acuerdo con los procedimientos predefinidos, y velando en todo momento por su aplicabilidad.
- Normativa: Regulación procedimental de acuerdo con las normas existentes o que se desarrollen.
- Confidencialidad: Todo el personal de SIA guardará la más absoluta discreción sobre todos los elementos relacionados con el presente servicio mediante la declaración de confidencialidad firmada por cada uno de los integrantes del equipo.
- Personal: Grado de capacitación técnica de los distintos recursos de SIA encargados de la prestación del servicio.
- Documentación:
  - Formato: Presentación de toda la documentación relacionada con la prestación del servicio en un formato predefinido con SIA.
  - Comprensibilidad: La documentación se desarrollará con un enfoque en el que prime la claridad de los contenidos y la facilidad de uso.

Puntos asignados a SIA en el presente apartado: 6 puntos

TELEFÓNICA EMPRESAS

Telefónica propone un Modelo de Servicio, Relación y Comunicación desde un punto de vista Estratégico, Táctico y Operativo basado en tres capas interconectadas que faciliten una comunicación transparente entre las áreas implicadas:

- Nivel Estratégico: Comité de Dirección, con las siguientes funciones:
  - Máximo responsable de decisiones del servicio.
  - Estrategia, directrices y principios del servicio.
  - Supervisión y seguimiento del cumplimiento de los objetivos, los hitos y plazos del servicio.
  - Establecer estrategias y líneas generales de acción, cuando estos afectan a elementos establecidos en los objetivos del servicio.
  - Evaluación global de la prestación del servicio y revisión del nivel de cumplimiento trimestral de los objetivos establecidos en el contrato.
  - Aprobar cualquier incorporación y/o cambio de personal.
  - Propone una periodicidad trimestral.
- Nivel Táctico: Comité de Servicio o de Seguimiento, como órgano de relación de seguimiento permanente entre RTVE y Telefónica, con las siguientes funciones:
  - Controlar, monitorizar y regir el servicio.
  - Ratificar las directivas aprobadas por el Comité de Dirección.
  - Supervisar el cumplimiento con las responsabilidades asumidas por las diferentes partes.
  - Organizar la distribución de responsabilidad y objetivos entre los grupos de trabajo del servicio.
  - Proveer cualquier requisito necesario para el servicio.
  - Predecir posibles desviaciones.
  - Evaluar riesgos y determinar posibles mitigaciones.
  - Informar al Comité de Dirección del progreso del servicio y del nivel de cumplimiento con las metas de calidad establecidas.
  - Solicitar la aprobación del Comité de Dirección si algún cambio cercano lo requiere. Los cambios cercanos dirigidos al Comité serán aquellos que modifican significativamente los objetivos del servicio (ámbito, periodo, coste y estándares).
  - Todos los acuerdos adoptados por el Comité de Seguimiento serán comunicados al Comité de Dirección.
  - Los miembros de Comité de Servicio o Seguimiento serán responsables de comunicar a sus respectivos equipos de trabajo los acuerdos alcanzados.
  - Propone una periodicidad mensual.
- Nivel Operativo: Comité Técnico - Equipo de Trabajo, velando porque el servicio se desarrolle según la planificación establecida para garantizar el cumplimiento del servicio contratado, y solventar las problemáticas específicas que afecten a los trabajos diarios, con las siguientes funciones:

- Seguimiento de la planificación del servicio.
- Seguimiento de las actividades operativas diarias del servicio.
- Seguimiento de los proyectos a corto y medio plazo.
- Velar por la correcta ejecución de los procesos, procedimientos y protocolos.
- Gestión de incidencias vinculadas al servicio.
- Identificación de aspectos de mejora.
- Periodicidad de Reunión Semanal o Quincenal

El modelo organizativo es complementario con las metodologías de gestión de proyectos más reconocidas, como PMI, PMBOK, NIST, ISO 20000 o similares, ya que encaja roles, responsabilidades y tareas.

Propone un Enfoque Metodológico Documental para lograr la Escalabilidad del Servicio estará basado en los siguientes procesos que constituyen los "aceleradores" para permitir cumplir los objetivos y la calidad del proyecto:

- Gestión Integral de la Calidad, Innovación y Mejora Continua.
- Gestión de la Demanda.
- Gestión de la Comunicación.
- Gestión de Incidencias.
- Gestión de los Riesgos del Servicio.
- Gestión del Conocimiento.
- Gestión de Riesgos del Talento: Plan de Retención y Formación del Talento

El modelo de la estructura prevista para este Plan Documentado de Calidad y Procedimientos, Innovación y Mejora Continua del Servicio de Soporte a la Implantación del Sistema de Gestión de Seguridad de la Información (SGSI) y Adecuación al Esquema Nacional de Seguridad (ENS) considera la disponibilidad de Servicio de Oficina de Seguridad de Telefónica para la gestión de la demanda de las actividades y tareas del proyecto, peticiones, consultas, seguimiento e incidencias integrantes del mismo, con su correspondiente capacidad de medición, aseguramiento de la calidad y el cumplimiento de los Acuerdos de Nivel de Servicios (SLA´s) acordados.

Telefónica propone para a RTVE sin coste alguno, el uso de la Solución SANDAS GRC® de Gestión Integral de Riesgos GRC para la Gestión Documental y la Gestión del Servicio de Soporte, con las siguientes características:

- Software de Gestión Integrada del Riesgo (Integrated Risk Management – IRM) que facilita una visión global del riesgo incluyendo los riesgos asociados al cumplimiento normativo.
- Dispone de funcionalidades especializadas en el ámbito de la Administración Pública tanto para el Cumplimiento del Esquema Nacional de Seguridad (soportando todas las guías de la sería CCN-STIC-8xx, la emisión automatizada del Informe de Estado de la Seguridad, incluyendo las modificaciones del E.N.S. y el soporte a Infraestructuras Críticas, como para el cumplimiento y certificación de estándares ISO (ISO 31000, ISO 27001, ISO 20000/ITIL, ISO 22301 o ISO 9001 entre otros) y marcos de referencia en Gobierno TI de forma integrada.
- Dispone de módulos comunes a los diferentes marcos normativos (en este caso SGSI 27001, ENS y RGPD/LOPDGDD), de manera que actividades que deben realizarse en sendos marcos normativos se unifican, creando sinergias entre ambos marcos, uniendo criterios y reduciendo sensiblemente el tiempo de ejecución de un proyecto. Los módulos que generan sinergias entre las funcionalidades de los sistemas de cumplimiento: SGSI 27001, ENS y RGPD/LOPDGDD son los siguientes:
- Módulo de gestión documental integrado (Gestión del Riesgo, Cumplimiento, Continuidad de Negocio y el Gobierno TI), para definición y documentación de Alcances, Políticas, Instrucciones Técnicas, Procedimientos Operativos, entre otros. Dicho Gestor gestiona y reconoce automáticamente cualquier tipo de documento, realizar un control de versiones automático de los mismos, permite definir flujos de aprobación por una persona o grupo, así como la posibilidad de integrarse en gestor documental del cliente (SharePoint – Office 365), enlazando a las ubicaciones correspondientes.
- Módulo de Gestión de Proyectos, que habilita un entorno común donde poder planificar, documentar y dar soporte a todos procesos de una forma centralizada y visual utilizando la metodología Kanban, para gestión de proyectos genéricos, tratamientos del Riesgo y programas de Auditoría, con seguimiento de actividades

ya que permite asociar a las tareas los responsables de ejecutarlas, equipos de trabajo, prioridad, fechas de ejecución, estado y costes.

Respecto de la documentación generada asegura la conformidad a la normativa interna y procedimientos de RTVE, así como normativa legal aplicable a la seguridad de la información (ENS, RGPD, LOPDGDD, Infraestructuras Críticas, ISO 27001...), incluida información clasificada, confidencial, sensible y secreta (actas, informes, normas, procedimientos, circulares, formación...), mediante:

- Procedimientos de Clasificación de la Información y Procedimiento de Distribución y/o Transporte Seguro de Documentación Confidencial, procedimientos que entregará Telefónica al inicio del Servicio a RTVE, el cual establecerá diversas medidas para garantizar la seguridad de la información automatizada y soporte papel generada y gestionada del Proyecto (clasificación de la información, control y versionado de documentación, medidas de seguridad, autorizaciones, custodia segura, almacenamiento seguro, registros de acceso logs, valija interna, correspondencia, embalaje seguro, registros de trazabilidad documentación papel, entre otros).
- Correo electrónico con funcionalidades adicionales, con la finalidad de distribuir de forma segura la información del servicio:
    - Activación de configuración de clasificación de etiquetas de seguridad "Sensible o Confidencial" de correos electrónicos y ficheros adjuntos, para garantizar la confidencialidad y protección de los datos distribuidos, independientemente de dónde estén almacenados o con quién son compartidos.
    - Activación de permisos de seguridad para determinar y controlar quien tiene acceso a los datos remitidos y que pueden hacer con ellos (ej. permisos de visualización, edición, etc.).
    - Activación de visibilidad y control del correo y datos distribuidos, a través de un seguimiento de actividad y revocación de acceso, en caso de que sea necesario.
    - Cifrado de la información gestionada, entre otras medidas.

Incluye el compromiso de implementar las siguientes medidas de acuerdo con la normativa legal y procedimientos internos de RTVE para garantizar la distribución segura de la información:

- La prohibición o restricción del uso de dispositivos externos de almacenamiento (USB, Discos Duros, etc.)
- La prohibición o restricción de Sistemas de Intercambio de Ficheros No Autorizados (ej. FTP para el envío y obtención de archivos).
- La prohibición de envío de ficheros en claro sin cifrar a través de correo electrónico, entre otros.

Considera necesario establecer un sistema de Control de Incidencias/Peticiones que permita la puesta en común entre ambas partes de todas las incidencias que se han producido durante la prestación del Servicio. Para ello, el Responsable del Servicio de Telefónica recibirá por parte de los afectados cualquier tipo de incidencia o problema detectado durante el Servicio, llevando un control automatizado de las mismas, para ponerse periódicamente en conocimiento de RTVE en las reuniones de seguimiento establecidas al efecto. Establece canales de comunicación para resolución de incidencias o la adaptación de la operativa de Control de Incidencias/Peticiones o integración de herramientas o sistemas propios de monitorización y gestión de las mismas, una vez analizada y aprobada su viabilidad por ambas partes.

Ofrece la presentación a RTVE de un Plan de Adecuación y Transformación diseñado a la medida del Servicio, permitiendo acometer una adquisición o transición sin riesgos para afrontar la gestión del servicio:

- Gestión del conocimiento de cara a mantener el Know-How actual del Servicio.
- Documentación intensiva en base al Plan de Calidad y Procedimientos de todo el ámbito del Servicio.
- Plan de Formación Ad-Hoc para la adecuación a los niveles de experiencia necesitados en los casos que se estime conveniente.

Telefónica se presta a utilizar las herramientas corporativas de RTVE para gobierno, gestión proyectos, incidencias y ticketing, así como la identificación de aspectos de mejora de la herramienta corporativas de RTVE, en caso de ser necesario para la optimización del Servicio, incluyendo toda la formación necesaria para la consecución de un manejo a un nivel avanzado de las mismas para los profesionales asignados por Telefónica.

Ofrece el diseño, de forma proactiva informes periódicos de seguimiento, fijando también sus correspondientes indicadores, lo que permitirá proporcionar un mayor control del Servicio a la RTVE. El objetivo es que dichos informes contengan toda la información relevante para el adecuado control y seguimiento del Servicio (indicadores, cuadros de mando, incidencias, riesgos, mejoras, seguimientos, volumetrías, línea base, etc.). Estos informes serán la herramienta y el marco de referencia para realizar el seguimiento del grado de cumplimiento del Servicio, adaptados a los nuevos indicadores y englobando toda la información referente al Servicio.

Puntos asignados a Telefónica en el presente apartado: ***8 puntos***

11.3 ACUERDO NIVEL DE SERVICIOS

Se otorgará hasta un máximo de 3 puntos las propuestas que mejoren el Acuerdo de Nivel de Servicio recogido en el pliego técnico (a mayor mejora mayor puntuación).

Revisión de las propuestas

El Pliego de especificaciones técnicas prescribe un Acuerdo de Nivel de Servicios (ANS), con un tiempo de respuesta de máximo de 24 horas.

Todas las empresas ofrecen una mejora en los tiempos máximos de respuesta. Se considera la asignación del 100% de la puntuación del apartado a la oferta con el mayor tiempo de reducción y el 0% a la inexistencia de mejora en este aspecto. Al resto de ofertas se le aplica un criterio de proporcionalidad entre ambos márgenes en función del tiempo de reducción.

A continuación, se destacan las características diferenciales y puntuación asignada a cada una de las ofertas:

NUNSYS

La oferta ofrece un tiempo medio de respuesta ante incidencia/petición urgente < 2 horas.

Puntos asignados a NUNSYS en el presente apartado: ***3,00 puntos***

S2 GRUPO

S2 Grupo mejora el nivel de servicio requerido para el caso de incidencias concretas o solicitudes urgentes comunicadas por RTVE, teniendo un tiempo de respuesta máximo de 4 horas

Puntos asignados a S2 Grupo en el presente apartado: ***2,73 puntos***

SISTEMAS INFORMATICOS ABIERTOS (SIA)

SIA, en caso de resultar adjudicataria del presente expediente, se compromete a un tiempo de respuesta no superior a 2 horas para aquellas incidencias urgentes comunicadas por RTVE.

Puntos asignados a SIA en el presente apartado: ***3,00 puntos***

TELEFÓNICA EMPRESAS

En caso de incidencias concretas o solicitudes urgentes comunicadas por RTVE, Telefónica Empresas ofrece un tiempo de respuesta de máximo 8 horas.

Puntos asignados a Telefónica en el presente apartado: ***2,18 puntos***

11.4 PLAN DE FORMACIÓN

Se otorgará hasta un máximo de 3 puntos el contenido de las propuestas que desarrollen en su oferta el plan de formación, incluyendo estructura de planificación, detalle de entregables, duración, metodología (presencial, on-line…) y alcance de las sesiones formativas (materiales, documentación, acciones de promoción propuestas, cartelería, videos, etc.) y métodos de evaluación del resultado.

Se valorará el plan corporativo de comunicación, formación y concienciación, teniendo en cuenta la especificidad de contenidos dirigidos a los diferentes colectivos que forman parte del personal de RTVE en materia de Seguridad de la Información, en especial al personal y responsables de las estructuras de gobierno, supervisión y operación establecidas en la estructura de seguridad de RTVE.

El objetivo será informar y formar (mediante campañas periódicas) a los distintos colectivos de los cambios introducidos por el Esquema Nacional de Seguridad y la legislación vigente en la materia, sus principales contenidos, y su impacto en RTVE.

Revisión de las propuestas

Las ofertas del conjunto de licitadores contienen un elemento común, con ligeras variaciones, que pueden considerarse homologables a todas ellas. A saber:

- Boletines de Actualidad o Newsletter
- Infografías
- "Píldoras" formativas o informativas
- Videos monográficos

Siendo el objeto del contrato la implantación de implantación en RTVE de un SGSI y la adecuación al ENS, se valora especialmente las acciones formativas y de concienciación a la estructura directiva y mandos intermedios relacionada con el gobierno y generación de normativa asociada directamente a la implementación del Esquema Nacional de Seguridad.

En este sentido, también se tiene en cuenta la concreción de la propuesta que, aunque su detalle se posponga al inicio de la ejecución del contrato, permita disponer de un marco de desarrollo determinado y con la entidad suficiente que permita comprender el esfuerzo por parte del licitador para apoyar la implementación del SGSI, tanto en recursos propios aportados como en la comprensión de las necesidades de RTVE en la concienciación y necesaria capacitación de los diferentes actores implicados en su puesta en marcha.

A continuación, se destacan las características diferenciales y puntuación asignada a cada una de las ofertas:

NUNSYS

Nunsys pone a disposición de RTVE un entorno colaborativo que permite seguir la sesión de forma on–line, a través de la herramienta Microsoft TEAMS, postergando una propuesta concreta a una revisión previa de las necesidades formativas y el público objetivo, de cara a establecer el contenido y el diseño de la formación.

En base a dicho análisis, ofrece el uso del portal público de formación ÁNGELES (https://angeles.ccn-cert.cni.es/es/) del Centro Criptológico Nacional para visualizar webinars online sobre diferentes temáticas en torno a la ciberseguridad, sobre el ENS, normativa de uso de medio electrónicos o cursos online para que los técnicos puedan mejorar su nivel de conocimiento en diferentes ámbitos de la ciberseguridad.

Incluye en su propuesta campañas mensuales de elaboración propia con recordatorios en materia de seguridad y protección de datos en forma de "píldoras" formativas.

Ofrece material divulgativo (infografías) puesto a disposición público por parte del Centro Criptológico Nacional (CCN) sobre aspectos clave de seguridad de la información

Se compromete a aportar informes de asistencia, cuestionarios de satisfacción y cuadros de mando.

Se ofrecen ilimitadas sesiones para los cursos online disponibles de:
- Concienciación a los empleados
- Formación avanzada sobre RGPD y LOPDGDD
- Formación sobre Esquema Nacional de Seguridad

Se ofrecen dos plazas en el curso de formación on-line específico para CISOs de preparación para la obtención de certificación del ISMS Forum.

Puntos asignados a NUNSYS en el presente apartado: ***1,50 puntos***

S2 GRUPO

S2 Grupo propone al inicio del servicio una evaluación teórica del grado de madurez de la cultura de ciberseguridad de la organización mediante:
- Entrevistas de información sobre políticas de seguridad no identificadas en la fase AS-IS del PDSyCN
- Identificación de grupos y colectivos con diferentes necesidades de formación por la información que manejan
- Generación de una encuesta con preguntas (en la intranet corporativa o mediante email para identificar el estado actual de la cultura.
- Análisis de los resultados de la encuesta para determinar las necesidades de concienciación, formación y entrenamiento de los diferentes colectivos para incrementar el nivel de madurez.

El Plan de Concienciación se diseñará a partir de los resultados de la evaluación teórica sobre la cultura de ciberseguridad. En dicho Plan se determinará el Plan de comunicación para los colectivos identificados, con contenidos específicos dirigidos a Directivos, Responsables de la Información, Responsables del Servicio, Responsables de Sistemas, Administradores de Seguridad y Empleados en general.

Las diferentes acciones de concienciación que se desarrollarán, especificando:
- Duración
- El calendario anual de acciones

Incluyen sesiones presenciales, impartidas por dos miembros del equipo de S2 Grupo en los roles de encargado de impartir la charla y encargado de ejecución de las prácticas, con presentación de los riesgos generales en el uso de las tecnologías tanto en el ámbito personal como el profesional. Sesiones de concienciación con orientación práctica donde se exponen y analizan en el uso de las TI y sus consecuencias, en un entorno muy cercano para el empleado, en el ámbito personal para después trasladarlo al ámbito corporativo. Análisis de casos reales con sensibilización del empleado hacia la seguridad de la información corporativa con el siguiente programa:
- Exposición del caso
- Ejemplo práctico
- Análisis de las consecuencias
- Recomendaciones prácticas para evitarlo

Las acciones formativas se desarrollarán en función del colectivo afectado teniendo en cuenta:
- Audiencia o colectivo
- Formato: webinar, sesión presencial, SCORM, infografía, boletín
- Canales de comunicación: intranet, plataforma e-learning, email, Teams
- Contenidos o píldoras a tratar: ingeniería social, contraseñas, WiFi, backups,

Los mensajes se distribuirán en dos posibles formatos:

- Infografías que, mediante una colección de imágenes, datos y gráficos, resume un mensaje fácil de entender. La infografía básica será una composición de iconos y texto, y además respetará el look & feel corporativo.
- Boletines de noticias acerca de la actualidad en el panorama de la seguridad entradas en una temática. En ellas, el empleado descubre qué amenazas están sufriendo las organizaciones y qué consecuencias producen a nivel económico y reputacional.

Respecto de la evaluación de la formación, propone la elaboración de un informe de riesgos profundizando en el componente humano del riesgo, detallando los aspectos de seguridad que han sido cubiertos por cada una de las acciones de formación: mensajes, comportamientos y riesgos:

- Informe del riesgo derivado de las conductas sabiendo cómo de cerca o lejos se está del comportamiento esperado.
- Salvaguardas interrelacionadas a planificar que permitan una mitigación real del riesgo.
- Análisis de causa raíz por la que se produce el comportamiento de riesgo.
- Precisar alcances concretos (Ej.: colectivos concretos, riesgos esperados a planificar) proporcionando una mayor efectividad a las salvaguardas propuestas.
- Priorizar los comportamientos y/o amenazas a abordar, así como la inversión a realizar en base a criterios de riesgo.

Puntos asignados a S2 Grupo en el presente apartado: ***2,00 puntos***

SISTEMAS INFORMATICOS ABIERTOS (SIA)

SIA define una estrategia de concienciación teniendo en cuenta el contexto de la organización, las funciones, responsabilidades y misión de los actores, para establecer un proceso continuo, que permita concienciar a los diferentes destinatarios de la importancia de la ciberseguridad.

El análisis, alcance y objetivos se lleva a cabo partiendo de la información obtenida de, al menos, las siguientes fuentes:

- Marco normativo existente identificando la Política de Seguridad de los SSII y corporativa del cliente.
- Misión de la organización y directrices generales del Plan Director de Seguridad (si existe).
- Información práctica de los sistemas de información críticos (si es posible disponer de esa información).
- Incidentes de seguridad ocurridos, que hayan tenido impacto en el cliente o en otras organizaciones similares.
- Marco normativo y legal aplicable (básicamente ENS, LOPDGDD, NIS2, LPIC, etc.).
- Revisión de posibles cursos, materiales y/o posibles planes de concienciación que con anterioridad en su caso hayan sido realizados por la organización.

SIA dispone de un curso específicamente desarrollado para directivos. Son sesiones de una hora a hora y media de duración, impartidas por expertos con formación, experiencia y know how en ciberseguridad, gestión de riesgos tecnológicos, cumplimiento legal y continuidad, adaptadas a las necesidades de la organización tanto en contenido como en forma. El índice de contenidos aportado incluye:

- Importancia de la ciberseguridad
- Ámbito legal y normativo
- La gestión de riesgos en la estrategia de la seguridad
- Importancia de la formación y concienciación en la organización
- Notificación de incidentes de seguridad
- Roles en ciberseguridad (CISO, CIO, CSO, CTO, CDO, DPD)
- Tendencias ciberseguridad 2024
- Buenas prácticas

El plan de formación propuesto que incluye, a modo de referencia, aporta un ejemplo de temas a tratar en las actividades formación incluidas en el alcance de su propuesta:

- Política y normativa de seguridad
- Presentación ENS e ISO 27001. Auditorías de cumplimiento.
- Objetivos y Plan Director de Seguridad
- Análisis y gestión de riesgos
- Control de acceso
- Criptografía, firma, cifrado
- Protección de servicios y servidores
- Protección de la información
- Seguridad en redes y SO
- Seguridad en desarrollo
- Gestión de incidentes de seguridad, análisis de vulnerabilidades y test de penetración
- Gestión de rastros y auditorías de seguridad
- Protección de Datos y Privacidad (resumido en impacto en GISS)
- Plan de Continuidad de Negocio
- Seguridad en teletrabajo
- Tendencias y desafíos: Seguridad en la nube y virtualización, IA, nuevas amenazas y mitigación de riesgos, vigilancia digital

El material sobre el que se basará las acciones de formación contempladas en el alcance de la presente propuesta, será en formato digital, para su divulgación a través de la intranet de RTVE y/o correo electrónico.

Destaca en el plan de formación la importancia de la formación a los responsables de la implementación del ENS, estando especialmente dirigido a los distintos colectivos de trabajadores y directivos de RTVE, siendo uno de los objetivos de dicho plan el de informar de los distintos cambios introducidos por el Esquema Nacional de Seguridad y la legislación vigente en cuanto a protección de información se refiere y el impacto de los mismos en RTVE a:

- Directivos.
- Responsables de la Información
- Responsables del Servicio
- Responsables de Sistemas
- Administradores de Seguridad.
- Empleados en general.

Puntos asignados a SIA en el presente apartado: ***3,00 puntos***

TELEFÓNICA EMPRESAS

Telefónica plantea, en primer lugar, identificar las competencias y necesidades en materia de seguridad de la información y privacidad que se consideren precisas, para la prestación de un servicio de calidad, conforme a las expectativas definidas.

Ofrece ayudar a RTVE a planificar la formación de forma general y periódica, dejando constancia en el Plan de Formación Anual todas las acciones que se prevén, y en donde incorporar las acciones específicas concernientes a la seguridad de la información y privacidad señaladas. En este documento deberá dejarse constancia de todos los aspectos concernientes a todo lo que afecte a la planificación formativa correspondiente.

Plantea la necesidad de la organización de adquirir los conocimientos necesarios para desempeñar los roles asignados a cada uno de los puestos de trabajo, conforme a una correcta categorización de los puestos de trabajo y teniendo en cuenta el acceso al tratamiento de información que se realiza por cada usuario.

Para definir las necesidades formativas en cada caso tendrá en cuenta:

- Estándares ISO 9001 Sistemas de Calidad e ISO 27001 Seguridad de la Información.
- Procedimientos específicos: Describen las funciones que se realizan en cada puesto de trabajo en materia de seguridad.
- Procedimientos generales en materia de seguridad: Acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

Respecto de métodos de formación y criterios de selección, refleja la intencionalidad de enumerar los métodos potenciales de formación que cumplan con las necesidades concretadas, haciéndolo dependiente, de forma genérica, de los recursos, las limitaciones y los objetivos enumerados, pudiendo incluir:

- Cursos
- Enseñanza a distancia
- Otros métodos que la entidad pueda incluir de su parte

Emplaza a definir y documentar en un futuro los criterios para la selección de los métodos apropiados, o una combinación de éstos. Pueden incluir:

- Fecha y lugar
- Instalaciones
- Costes
- Objetivos de la formación
- Público al que se dirige la acción formativa
- Duración de la formación y secuencia de implementación
- Formas de valoración, evaluación y certificación

Se deberá fijar un Plan de Formación en el que figuren los objetivos de la formación, es decir, que defina lo que los destinatarios serán capaces de lograr como resultado de la misma.

El objetivo de la formación en materia de seguridad de la información incluye: comprensión de los conceptos básicos de esta materia, novedades de los diferentes marcos normativos o estándares que la regulan, así como las medidas de seguridad, procedimientos y políticas de seguridad aplicables al tratamiento de la información a la que el destinatario accede en el desempeño de su puesto de trabajo. También considera un objetivo de la formación la comprensión de las consecuencias de un potencial incumplimiento.

Establece el procedimiento de comunicación a los asistentes de convocatoria de cursos, naturaleza de la formación y la carencia de competencia que se desea disminuir con la ejecución del mismo, solicitando la interlocución directa entre el formador y los destinatarios, para informar sobre el carácter obligatorio o no de la formación, el mínimo de sesiones al que en su caso haya que asistir obtener la correspondiente certificación, y cualquier información relevante adicional.

Recomienda la creación de un Plan de Formación y Concienciación que incluya la confección, adaptación, actualización, preparación, realización, y seguimiento de acciones concretas y contenidos sobre seguridad de la información, de forma eficiente y adaptadas a las necesidades detectadas, con la finalidad de mejorar y reforzar el desempeño y la línea de actuación de las personas en este ámbito.

Dentro de las acciones mínimas que considera este Plan se encuentran:

- Charlas informativas para Directivos, Técnicos y usuarios en general. Dentro del primer grupo estarían la Alta Dirección y Altos Mandos de la entidad; En el segundo encajarían figuras como los Responsables de la Información, Servicios, Seguridad y Sistemas, así como los Administradores de Seguridad; y en el tercero estaría el resto de las personas que utilicen información en sus funciones laborales.
- Cursos de formación para personal general y técnico: Sesiones de formación presencial u online, con la finalidad de repasar las principales cuestiones que implican a las personas en su día a día corporativo y

personal en materia de seguridad de la información con la finalidad de que los asistentes cuenten con una visión global de todo aquello que deben tener en cuenta en sus relaciones con el mundo online.

- Infografías y/o vídeos, u otro material de concienciación contemplando como posibles temas: autentificación en dos pasos, dispositivos móviles, ingeniería social, navegación segura, seguridad en el puesto de trabajo, seguridad Redes Wifi, teletrabajo seguro, inteligencia artificial (IA), entre otros.

Puntos asignados a Telefónica en el presente apartado: ***2,50 puntos***