



Eusko Jaurlaritzaren
Informatika Elkarte

Sociedad Informática
del Gobierno Vasco

Servicio de auditorías de seguridad de aplicaciones y sistemas para Cyberzaintza y suministro de herramientas asociadas

Pliego de Condiciones Técnicas

Julio de 2024

Este documento es propiedad de Eusko Jaurlaritzaren Informatika Elkartea – Sociedad Informática del Gobierno Vasco, S.A. (EJIE) y su contenido es CONFIDENCIAL. Este documento no puede ser reproducido, en su totalidad o parcialmente, ni mostrado a otras partes, ni utilizado para otros propósitos que los que han originado su entrega, sin el previo permiso escrito de EJIE. En el caso de ser entregado en virtud de un contrato, su utilización estará limitada a lo expresamente autorizado en dicho contrato. EJIE no podrá ser considerada responsable de eventuales errores u omisiones en la edición del documento.

Versión	Fecha	Resumen de cambios	Elaborado por	Aprobado por
1.0	12/07/2024	Versión inicial	Javier González Tavera	Josu Bagazgoitia

Índice

1	Introducción	4
1.1	Perfil de la compañía	4
2	Objeto del contrato.....	5
3	Servicios solicitados.....	6
3.1	Definición de una metodología de evaluación.....	6
3.2	Auditorías de seguridad.....	6
3.3	Mejora continua: diseño y operación de procesos y tecnologías de auditoría y evolución del modelo	8
4	Suministros solicitados	9
4.1	Herramienta de análisis web.....	9
4.2	Herramienta de análisis de aplicaciones.....	9
5	Planificación	10
5.1	Lanzamiento	10
5.2	Ejecución	10
5.2.1	Entregables.....	12
5.2.1.1	Informes de auditorías	12
5.3	Seguimiento.....	13
5.3.1	Entregables.....	13
5.4	Cierre	13
5.4.1	Entregables.....	13
5.4.1.1	Certificado acreditativo de borrado de información.....	14
6	Organización del servicio	15
6.1	Equipo de trabajo.....	15
6.2	Organigrama del servicio	15
6.3	Dimensionamiento y dedicación	16
6.4	Equipamiento y software para el equipo de trabajo dedicado	16
6.5	Lugar de trabajo	17
6.6	Horario.....	17

1 Introducción

1.1 Perfil de la compañía

EJIE, Eusko Jaurilaritzaren Informatika Elkarte – Sociedad Informática del Gobierno Vasco, es la Empresa pública de servicios de las tecnologías de la información y las comunicaciones (TIC), cuya razón de existir es contribuir a la consecución de un Sector Público Vasco, moderno y eficiente, en el Marco Legal establecido por el Gobierno, con la seguridad y calidad necesarias y con el debido respeto al medio ambiente.

EJIE tiene como meta final la consecución de la satisfacción de sus clientes, siendo el instrumento común de prestación de servicios TIC en el Sector Público Vasco, y comprometiéndose en:

- Construir y mantener con eficiencia y calidad la infraestructura de los Sistemas de Información, posibilitando su continuidad y seguridad.
- Garantizar la interoperabilidad entre las distintas administraciones.
- Servir de apoyo a las necesidades de planificación y realización de la función informática de los Departamentos y Organismos Autónomos del Gobierno, asegurando la cobertura de sus demandas con el compromiso y profesionalidad adecuados a las relaciones contractuales que se establezcan.

Por tanto, EJIE debe ser, un instrumento común de referencia para la prestación de servicios TIC en el Sector Público Vasco:

- Aportando valor añadido.
- Proporcionando soluciones competitivas.
- Transmitiendo confianza a sus clientes.
- Contando con personas cualificadas y comprometidas.

Se puede obtener información más detallada y extensa en nuestra dirección de Internet <https://www.ejie.eus>.

Cyberzaintza, la Agencia Vasca de Ciberseguridad, es un organismo público, con personalidad jurídica propia, creado para combatir, de una manera integral y transversal, las amenazas derivadas del uso de internet y las nuevas tecnologías en Euskadi y su creación se recoge en la Ley 7/2023, de 29 de junio, de creación de la Agencia Vasca de Ciberseguridad.

La Agencia tiene como objeto promover y coordinar la ciberseguridad en el sector público vasco delimitado en la Ley 3/2022, de 12 de mayo, del Sector Público Vasco, en el ámbito de la seguridad de los sistemas de información y de las redes electrónicas de competencia de dicho sector, y apoyar e impulsar la capacitación en ciberseguridad y el desarrollo digital seguro de la Comunidad Autónoma Vasca, de su Administración pública, de su ciudadanía y de su tejido empresarial.

Las funciones de la Agencia están recogidas en la propia Ley. Se puede obtener información más detallada y extensa en <https://www.ciberseguridad.eus>.

2 Objeto del contrato

El objeto del expediente es la contratación bajo demanda de servicios de auditorías de seguridad de diversos tipos (se detallan en el punto 3 del presente PCT) para Cyberzaintza y las entidades que tiene definidas como estratégicas, con el objetivo de identificar sus vulnerabilidades ante ataques externos o internos, y disponer las medidas adecuadas para mitigar o reducir los riesgos de las mismas, así como la suscripción de licencias de herramientas involucradas en la realización de estas actividades.

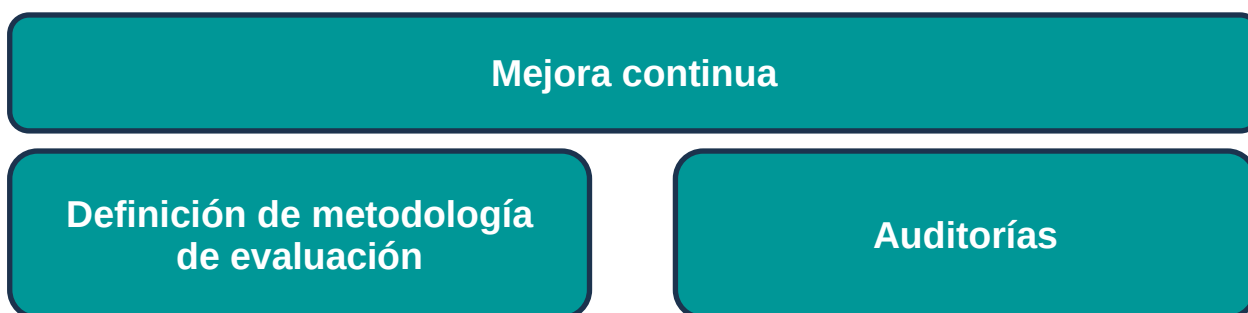
Las entidades objeto de estos servicios de auditoría no forman parte del conjunto de entidades a las que EJIE ofrece este tipo de servicios en la actualidad.

Las metodologías deberán ser acotadas por los auditores para cada servicio de acuerdo con los escenarios que se encuentren en cada momento con el fin de realizar las pruebas más oportunas optimizando los recursos disponibles, siempre con el visto bueno por parte de la entidad contratante.

El objeto de contratación del presente pliego se encuadra dentro de la prestación de servicios a contratar mediante encargo, por parte de las entidades integrantes del sector público de la Comunidad Autónoma de Euskadi, a través de sociedades que tengan la condición de medio propio de acuerdo con la legislación vigente. EJIE, como sociedad pública, órgano gestor tecnológico y medio propio, tiene encomendada la gestión centralizada de contratación, de conformidad con el Decreto 36/2020, de 10 de marzo, por el que se regula el Modelo de Gestión de las Tecnologías de la Información y la Comunicación en el Sector Público de la Comunidad Autónoma de Euskadi.

3 Servicios solicitados

En este apartado se describe el alcance de los servicios solicitados a través de este expediente, no siendo el listado que aparece a continuación una relación exhaustiva de las características del servicio contratado, sino las actividades generales demandadas por Cyberzaintza, cubriendo los aspectos de tareas a realizar y los resultados esperados.



3.1 Definición de una metodología de evaluación

Los licitadores deberán proponer una metodología que permita evaluar de manera común y objetiva a las entidades a las que se realicen las auditorías.

Dicha metodología, que deberá ir alineada con los estándares de ciberseguridad existentes en la prestación de este tipo de servicio, deberá así mismo detallar diferentes ámbitos de evaluación, ponderando cada uno de ellos, de modo que finalmente se obtenga tanto una puntuación general, así como individual por cada uno de los apartados, y recomendaciones concretas que permitan a las entidades participantes la mejora de su nivel de resiliencia.

De igual modo, deberán realizar un planteamiento de entregables que incluya formularios y documentación adicional para la recogida de evidencias de las entidades participantes, para la presentación de resultados, incluyendo métricas, etc.

3.2 Auditorías de seguridad

El objetivo es la revisión y evaluación de la seguridad desde todos los ámbitos técnicos, tecnológicos y organizativos de la seguridad, y se describen características y requisitos mínimos que la empresa adjudicataria deberá prestar, pudiendo ésta ampliarlos y mejorarlos, y no siendo el listado que aparece a continuación una relación exhaustiva de las características de los servicios contratados, sino las líneas generales demandadas por la entidad contratante.

La empresa adjudicataria deberá aportar los conocimientos, metodologías y apoyarse en las herramientas necesarias para asegurar el resultado óptimo del proyecto, teniendo la indicación expresa de no ser admitidos los trabajos que sean realizados únicamente mediante el empleo de técnicas automáticas.

Cyberzaintza, solicitará bajo demanda, la auditoría de una infraestructura/aplicación/servicio. El alcance de la auditoría puede comprender una o varias de las siguientes tipologías de servicio:

1. **Auditoría de seguridad de aplicaciones software (nueva o en ejecución):** análisis de aplicaciones software para identificar posibles vulnerabilidades de seguridad de las mismas. Se deberán emplear diferentes técnicas de detección y explotación, herramientas de hacking, etc. Las pruebas y análisis de seguridad a realizar deberán incluir, donde proceda, como mínimo los siguientes: descubrimiento de aplicaciones, identificación de puntos de entrada a la aplicación, posibilidades de inyección de código, gestión de sesiones y análisis del esquema de autenticación, escalada de privilegios, pruebas de autorización y autorización entre aplicaciones, análisis de códigos de error, propagación de vulnerabilidades, ingeniería inversa de protocolos y/o posibles

exploits que se pudieran usar, pruebas de denegación de servicio, sistemas de autenticación, posibles suplantaciones, de entrada de datos y de tráfico y comunicaciones.

2. **Auditoría de seguridad de aplicaciones móviles (nueva o en ejecución):** análisis de aplicaciones destinadas a terminales móviles para identificar posibles vulnerabilidades de seguridad de las mismas mediante análisis estáticos y dinámicos, pruebas de intrusión, suplantación de identidades, etc. Se deberán emplear diferentes técnicas de detección y explotación, herramientas de hacking, etc.
Las pruebas y análisis de seguridad a realizar deberán incluir, donde proceda, como mínimo los siguientes: descubrimiento de aplicaciones, identificación de puntos de entrada a la aplicación, posibilidades de inyección de código, gestión de sesiones y análisis del esquema de autenticación, escalada de privilegios, pruebas de autorización y autorización entre aplicaciones, análisis de códigos de error, propagación de vulnerabilidades, ingeniería inversa de protocolos y/o posibles exploits que se pudieran usar, pruebas de denegación de servicio, sistemas de autenticación, posibles suplantaciones, de entrada de datos y de tráfico y comunicaciones.
3. **Test de intrusión en la red desde Internet:** el objetivo del test de intrusión es evaluar el estado de los sistemas identificando las vulnerabilidades que puedan existir: obteniendo las probabilidades de éxito de un ataque y comprobar la eficacia de las medidas de defensa perimetrales implementadas. El objetivo será cualquier sistema que pudiera estar accesible: routers, IPS/IDS, firewalls, WAF, VPN, servicios web, correo, fichero, etc. En definitiva, cualquier otro servicio accesible desde el exterior
4. **Auditoría de seguridad de red interna:** el objetivo es evaluar la seguridad de la red interna: desde DMZ, desde cualquier otra red o plataforma a la que un atacante pudiera obtener acceso. Se deberá determinar si la inseguridad en esas redes y plataformas puede llegar a repercutir en la red interna de la empresa.
5. **Auditoría de seguridad de redes WIFI:** evaluación de seguridad de las redes WIFI.
6. **Auditoría de seguridad de información accesible desde Internet:** el objetivo es identificar toda la información que pudiera estar accesible desde internet y que, de algún modo, sirviera a un atacante para sus objetivos: desde pliegos con información técnica, sus redes, sistemas, organización, u otros. Del mismo modo, se deberán obtener una serie de recomendaciones para eliminar o reducir dicha exposición.
7. **Auditoría de ingeniería social:** con el objeto de obtener información confidencial a través de la manipulación de usuarios legítimos. Es un ataque dirigido a la confianza del usuario con fin de ver qué información sensible puede obtenerse siguiendo una metodología propia desarrollada en base a técnicas de Ingeniería Social, y realizar planes para reducir el riesgo.
8. **Auditorías de dispositivos IoT (Internet of Things):** análisis de dispositivos IoT con el objetivo de descubrir cualquier vulnerabilidad que pueda provocar un acceso no autorizado a los sistemas e infraestructuras.
9. **Simulación APT Ransomware:** ejercicio para mostrar el grado de exposición de la organización y el impacto que tendría en caso de materializarse una amenaza de cifrado masivo que permitirían a un atacante potencial bloquear el funcionamiento y/o acceso a una parte o a todos los equipos de la compañía.
10. **Auditoría de directorio activo:** el objetivo es identificar si el directorio activo está debidamente bastionado o no y en el caso de que no sea así, proponer mejoras para un nivel de securización óptimo.
11. **Auditoría de configuración de dispositivos de protección (firewall, EDR, etc.):** el objetivo es evaluar el nivel de bastionado de diferentes tipos de dispositivos de protección para lo cual se seguirán guías existentes de entidades de referencia y fabricantes.
12. **Otros tipos de auditoría y consultoría técnica de ciberseguridad:** cualquier otro tipo de auditoría de ciberseguridad que no esté contemplada en los tipos indicados previamente. Adicionalmente, Cyberzaintza podrá consultar al contratista aspectos relacionados con la seguridad en sus sistemas de información, con el fin de garantizar una comprensión de los riesgos, identificación de debilidades o mejoras de seguridad en sus sistemas y prevenir vulnerabilidades que puedan surgir en las correspondientes auditorías.

Cyberzaintza podrá solicitar al adjudicatario la realización de cualquiera de los tipos de servicios expuestos en cualquier momento durante la vigencia del contrato, siempre y cuando no se haya alcanzado el límite presupuestario.

Ante la importancia del ámbito de uso de las aplicaciones e infraestructura crítica asociada, no se impactará sobre los servicios en producción derivados de posibles pruebas de impacto de la auditoría, que en ningún caso deberán afectar al funcionamiento normal. Se deberán definir previamente los impactos y acordar las horas de actuación sobre plataformas y aplicaciones junto con la entidad contratante.

3.3 Mejora continua: diseño y operación de procesos y tecnologías de auditoría y evolución del modelo

El servicio incluirá una capa transversal a todas las tareas solicitadas que contribuya a la industrialización de las capacidades y al seguimiento y a la mejora continua de las mismas.

Para ello, el equipo de trabajo de auditores asignado a la tarea trabajará así mismo en todas las tareas relacionadas con el desarrollo del modelo de auditoría técnica de Cyberzaintza, entre las que se incluyen:

- Se identificará, describirá y documentará toda la operativa, lo que incluye todos los procesos y procedimientos de gobierno y operativos del área de auditoría técnica, definiendo los flujos de trabajo, los roles y responsabilidades, el alcance, las entradas y salidas con su correspondiente estructura, procesos asociados, etc.
- Se definirán las arquitecturas de las diferentes soluciones para los servicios demandados y se implantarán, adaptarán y evolucionarán los servicios y las herramientas soporte correspondientes.
- Se definirá un catálogo de productos y servicios en este ámbito, identificando para cada uno de ellos catálogo de peticiones, niveles de servicio, planes de calidad, modelo de escalado, etc. a ofrecer desde el área de inteligencia, de acuerdo con las necesidades de los clientes.
 - Se establecerá un modelo de seguimiento de la eficiencia y calidad de la prestación de los servicios ofrecidos por el área de auditoría técnica, con el objetivo de contribuir a mejorar el nivel de satisfacción de los clientes.
 - Se identificarán indicadores KPIs y métricas, y se propondrán cuadros de mando.
- Se definirá un modelo de gestión del conocimiento.

4 Suministros solicitados

Relacionado con las actividades involucradas en este expediente se requiere el suministro de licencias de suscripción que cumplan los requisitos técnicos especificados en ese apartado.

La empresa adjudicataria deberá suministrar las licencias de suscripción indicadas, junto con la garantía y el soporte de fabricante asociado. Estas licencias deberán ser oficiales y estar garantizadas por el fabricante.

El soporte de fabricante debe incluir, sin coste adicional, el acceso a las actualizaciones de parches, alertas de seguridad y nuevas versiones de software durante el periodo de garantía. El suministro de la actualización incluirá tanto las licencias y software como los manuales y la documentación técnica del fabricante asociado.

Dentro del marco de servicios incluidos en este expediente, las herramientas deberán instalarse en equipos pertenecientes a Cyberzaintza que se indicarán al inicio del contrato.

4.1 Herramienta de análisis web

Se requiere el suministro de una licencia de suscripción por un periodo de 3 años correspondiente a una herramienta de análisis web que cumpla, como mínimo, los siguientes requisitos:

- Escaneos ilimitados.
- Número ilimitado de FQDNs a escanear.
- Posibilidad de programar escaneos.
- Descubrimiento de activos.
- Descubrimiento de vulnerabilidades.
- Análisis contra el TOP 10 de OWASP.
- Un escaneo simultáneo con posibilidad de ampliación.
- Integración con herramientas de ticketing.
- Dashboards para visualizar los resultados.
- Propuesta de remediaciones.
- Exportación de informes en diferentes formatos.
- Posibilidad de crear usuarios ilimitados con diferentes roles y acceso SSO.
- Posibilidad de despliegue on premise y en cloud.
- Posibilidad de integración con API.
- Compliance.

4.2 Herramienta de análisis de aplicaciones

Se requiere el suministro de una licencia de suscripción por un periodo de 3 años correspondiente a una herramienta de análisis de aplicaciones que cumpla, como mínimo, los siguientes requisitos:

- Escaneos ilimitados
- Número ilimitado de direcciones IP a escanear.
- Análisis de aplicaciones
- Descubrimiento de activos.
- Escaneo de direccionamiento IPv4 e IPv6.
- Descubrimiento de vulnerabilidades.
- Exportación de informes en diferentes formatos.
- Posibilidad de integración con API.
- Compliance.
- Posibilidad de instalación on premise.

5 Planificación

5.1 Lanzamiento

Se realizará en un plazo máximo de 15 días posteriores a la formalización del contrato. Se realizará una reunión para validar cualquier aspecto relacionado con la prestación del servicio:

- Objeto, alcance y otros aspectos del contrato.
- Identificación de responsables, puntos de contacto y mecanismos de comunicación.
- Metodología y herramientas a utilizar.
- Etc.

5.2 Ejecución

Se deben presentar las fases de trabajo, aunque a nivel general, se solicitan las siguientes:

FASE 1: Solicitud de auditoría

Cyberzaintza designará a un interlocutor el cual podrá solicitar al adjudicatario la realización de auditorías tanto para sí misma, como para alguna entidad que haya designado como estratégica.

Esta solicitud se realizará mediante correo electrónico a una dirección establecida. Cyberzaintza pondrá a disposición de la entidad adjudicataria un buzón para realizar la gestión del servicio.

Una vez activada la demanda de servicio, el adjudicatario deberá solicitar todo lo necesario para la correcta realización de la auditoría, para lo cual elaborará una plantilla de solicitud de requisitos que incluirá, así mismo, información detallada de todo el proceso.

Tras recibir la información y analizarla, se llevará a cabo una reunión de lanzamiento de auditoría entre el adjudicatario y Cyberzaintza, incluyendo a terceras partes si fuera necesario. Dicha reunión deberá llevarse a cabo en un plazo inferior a 7 días laborales desde la entrega de la solicitud de requisitos cumplimentada, salvo que Cyberzaintza por el motivo que fuera decidiese posponerla.

De forma previa a la ejecución de las tareas indicadas, se deberá proceder con:

- Obtención de consentimiento de la entidad sobre la que se realizará la auditoría, por parte del adjudicatario.
- Firma de aceptación de las cláusulas de confidencialidad por parte de las personas que van a participar en la auditoría (modelo que enviará Cyberzaintza).

FASE 2: Planificación: definición e identificación de los sistemas a auditar.

Se establecerá el alcance detallado, junto con Cyberzaintza y un responsable de la entidad estratégica del servicio auditado si corresponde. El adjudicatario presentará una planificación, con hitos y sus plazos, para ejecutar dichos trabajos y presentar los informes correspondientes. Cyberzaintza valorará dicha planificación y solicitará las correcciones o aclaraciones que considere oportunas.

FASE 3: Definición de la tipología de las pruebas en base al tipo de auditoría

El objetivo es diseñar los ataques, para por una parte conocer si el servicio o la infraestructura es vulnerable (análisis de intrusión) y por otra el detectar posibles vulnerabilidades (análisis exhaustivo de vulnerabilidades).

No se admitirán únicamente ataques a realizar con herramientas automáticas.

HITO fases 1-3: Todas las tareas comprendidas entre la fase 1 y fase 3 descritas previamente deberán realizarse en un plazo igual o inferior a tres (3) semanas.

FASE 4: Preparación de la auditoría

El adjudicatario del servicio será el responsable de realizar las tareas previas pertinentes para la debida preparación de la auditoría, lo que incluirá entre otras cosas:

- Las interacciones con Cyberzaintza y entidades designadas como estratégicas, en caso necesario.
- Acordar el direccionamiento desde el que se ejecutarán los trabajos, en caso necesario.
- Acordar la ventana de tiempo para ejecutar los trabajos.
- Concretar e informar del potencial impacto de los trabajos.
- Las notificaciones de inicio, seguimiento y finalización de los trabajos realizados.

FASE 5: Ejecución de la auditoría

El adjudicatario realizará la auditoría (en una 1ª iteración) según su propia metodología, que tendrá que ser descrita en la oferta a este pliego y que deberá ir alineada con los estándares existentes. Como referencia:

- Identificación de vectores de ataque: detección de vulnerabilidades y debilidades de seguridad en los sistemas y aplicaciones que puedan ser utilizadas como vector de ataque por parte de un usuario malintencionado.
 - Técnicas manuales.
 - Técnicas automáticas.
 - Evasión de controles de seguridad (pruebas sobre un entorno real y con los controles de seguridad desplegados).
- Diseño de ataques: desarrollar vías de explotación específicas sobre los sistemas en alcance como prueba de concepto utilizando uno o varios de los vectores de ataque detectados en la fase anterior.
 - Combinación de vectores de ataque.
 - Ataques de ingeniería social.
 - Diseño de ataques reales (no basados en pruebas de concepto incompletas).
- Ejecución o Explotación: ejecutar los ataques diseñados sobre los sistemas en alcance, de manera que se puedan descartar falsos positivos y evaluar el impacto de los vectores de ataque.
 - Valor de criticidad
 - Post-explotación (diseño de nuevos ataques en base a los avances tras la explotación).

El adjudicatario podrá apoyarse en el uso de herramientas de seguridad para la realización de las auditorías. Sin embargo, siempre que sea posible, las vulnerabilidades explotables serán reportadas indicando los pasos que se han seguido para su explotación mediante técnicas de hacking, con suficientes evidencias para poder acometer la remediación. Se propondrán las medidas de remediación que se consideren adecuadas, con una estimación del esfuerzo de implementación necesario.

FASE 6: Documentación e informes de resultados

Una vez finalizada la/s auditoría/s, el adjudicatario enviará un informe completo al contacto establecido en Cyberzaintza, quien facilitará las plantillas necesarias a la entidad adjudicatario del servicio.

Se deberán presentar los correspondientes entregables. En los casos en los que para una misma aplicación se requieran auditorías de diferente tipología especificadas en el apartado 3.2, los resultados de ambas auditorías deberán ser cruzados (relación de las vulnerabilidades detectadas en ambas auditorías) y se elaborará un único informe de resultados por aplicación.

Los informes de auditoría serán revisados por Cyberzaintza y se fijará una reunión para la explicación de los mismos.

No se admitirá un informe basado únicamente en la salida de las herramientas que se usen.

Cyberzaintza procederá a dar el visto bueno a la auditoría o propondrá los cambios pertinentes que tendrán que ser revisados y realizados por el adjudicatario.

En caso de que Cyberzaintza considere que el informe no tiene la calidad necesaria (de acuerdo a lo establecido en el presente pliego) se lo notificará a la adjudicataria y ésta deberá devolverle el informe corregido. En el caso de que el informe no cumpla con los requerimientos mínimos de acuerdo al presente

pliego, no se considerará realizado y, por lo tanto, no será facturable. Si esta situación se repite en tres ocasiones (sean o no consecutivas), Cyberzaintza podrá rescindir el contrato.

FASE 7: Informes de confirmación de remediación (retest)

Una vez aceptado el informe por Cyberzaintza, se decidirán las acciones a llevar a cabo para la corrección de las vulnerabilidades encontradas, en la medida de lo posible y en función de las criticidades.

Como fase posterior a la realización de la auditoría, y después de que Cyberzaintza o la entidad estratégica afectada ejecute las acciones de remediación que considere oportuno, será necesario confirmar que efectivamente se han remediado con éxito las vulnerabilidades.

El adjudicatario verificará que las correcciones han sido realizadas, y redactará un Informe de Confirmación de Remediación. Si la solución aplicada por Cyberzaintza o la entidad afectada no cumple con los requisitos para remediar la vulnerabilidad especificada, el adjudicatario, realizará nuevas recomendaciones para la solución correcta de las vulnerabilidades detectadas.

FASE 8: Borrado de información

Al finalizar cada servicio, el adjudicatario deberá borrar de sus sistemas o archivos los códigos fuente, certificados o cualquier otra información propiedad de Cyberzaintza que haya recibido para la realización de su trabajo.

5.2.1 Entregables

5.2.1.1 Informes de auditorías

El adjudicatario deberá proporcionar a Cyberzaintza informes de auditoría por servicio auditado.

El objetivo es informar de forma detallada de las vulnerabilidades y vectores de explotación detectados sobre los sistemas auditados, así como de las acciones correctivas que se han de llevar a cabo y aspectos de mejora.

Los informes de auditoría incluirán, como mínimo, los siguientes apartados:

- Elaboración de un informe con un resumen ejecutivo a alto nivel, identificando los principales problemas y procesos afectados, así como las áreas de mejora globales.
 - Objeto y alcance.
 - Resumen ejecutivo.
 - Metodología empleada.
 - Herramientas empleadas.
 - Pruebas realizadas.
 - Hallazgos y debilidades.
 - Vías de explotación exitosas.
 - Riesgos principales e impacto (criticidad, evidencias...).
 - Recomendaciones principales de mejora a alto nivel.
- Informe ligero de cada una de las pruebas:
 - Detalle pruebas realizadas especificando su objetivo.
 - Resultados obtenidos, incluyendo el nivel de vulnerabilidades detectadas.
- Elaboración de un informe técnico en detalle, analizando cada una de las vulnerabilidades y hallazgos detectados a bajo nivel, así como las acciones correctivas concretas:
 - Detalle de cada una de las vulnerabilidades.
 - Valoración del impacto.
 - Descripción y evidencias.
 - Descripción del impacto asociado.
 - Recomendaciones detalladas para su resolución.
- Elaboración de un informe de vulnerabilidad crítica detectada con el detalle técnico:
 - Descripción de la vulnerabilidad.
 - Impacto asociado.
 - Detalle de explotación y prueba de concepto.

En caso de que se encuentren durante las auditorías vulnerabilidades críticas o que impliquen un alto riesgo de fuga de información se emitirá una alerta (al responsable del servicio auditado) acompañada de un informe ligero con la información más importante (descripción de la vulnerabilidad, descripción del tipo de impacto y solución o workaround temporal para mitigar la misma en caso de que no hubiese una solución eficiente disponible en el momento).

En todos los tipos de informes indicados, deberá aparecer un apartado final con:

- Plan de acción para mitigar el riesgo.
- En caso de aplicar, se adjuntará un video explicativo de la explotación.
- Propuestas de tratamiento, incluyendo estimación de esfuerzo y priorización.
- Conclusiones: resumen de las principales vulnerabilidades detectadas y recomendaciones de mejora.

5.3 Seguimiento

A raíz de la reunión de lanzamiento y con periodicidad mensual el contratista se reunirá con la dirección técnica del proyecto de Cyberzaintza, si esta lo considera necesario para la adecuada prestación del servicio, con la finalidad de realizar un seguimiento periódico de las tareas asociadas al contrato.

Cyberzaintza podrá convocar cuantas reuniones de seguimiento del proyecto considere oportunas para asegurar el cumplimiento y la correcta ejecución del objeto del contrato. El contratista será responsable de la redacción y distribución de las correspondientes actas de reunión.

En dicha reunión se revisarán al menos los siguientes puntos:

- Auditorías realizadas en el periodo anterior.
- Auditorías planificadas para el siguiente periodo.
- Seguimiento económico del contrato.
- Incidencias surgidas y áreas de mejora.

5.3.1 Entregables

- Presentación de trabajos realizados.
- Actas de reuniones de seguimiento.
- Memoria anual: Anualmente, el adjudicatario deberá presentar una memoria como informe justificativo del alcance efectivo de los trabajos realizados, que debe incluir todos los entregables anteriormente realizados. Asimismo, la memoria incluirá un capítulo adicional con contenido detallado especificando las herramientas y tácticas empleadas, referencias utilizadas, propuestas de remediación, etc.

5.4 Cierre

La fase de cierre concluirá con la celebración de la reunión de cierre del proyecto, donde se tratarán al menos los siguientes puntos:

- Revisión de los entregables de esta fase.
- Revisión de lecciones aprendidas y mejoras incluidas en la memoria final del contrato. Esta información podrá ser solicitada como adelanto en cualquier momento durante la ejecución del contrato.
- Cierre del contrato.

5.4.1 Entregables

- Presentación de trabajos realizados
- Actas de reuniones de seguimiento

- Memoria final: al alcanzar la finalización del proyecto, el adjudicatario deberá presentar una Memoria Final, como informe justificativo del alcance efectivo de los trabajos realizados, que debe incluir todos los entregables anteriormente realizados. Asimismo, la memoria incluirá un capítulo adicional con contenido detallado especificando las herramientas y tácticas empleadas, referencias utilizadas, propuestas de remediación, etc.

5.4.1.1 Certificado acreditativo de borrado de información

Asimismo, a la finalización del proyecto el adjudicatario deberá entregar un documento firmado en el que garantiza que todo el código fuente u otra información propietaria de Cyberzaintza han sido eliminados de sus sistemas y archivos.

6 Organización del servicio

6.1 Equipo de trabajo

El contratista deberá disponer de los medios materiales y personales necesarios para el correcto, adecuado y satisfactorio desarrollo de la actividad contratada. En relación con los medios personales y materiales deberá tenerse en cuenta lo previsto en el presente pliego.

Para la adecuada ejecución del proyecto el contratista debe tener capacidad suficiente para aportar, como mínimo, los siguientes perfiles con la dedicación correspondiente y la solvencia requerida en el Pliego de Condiciones Particulares:

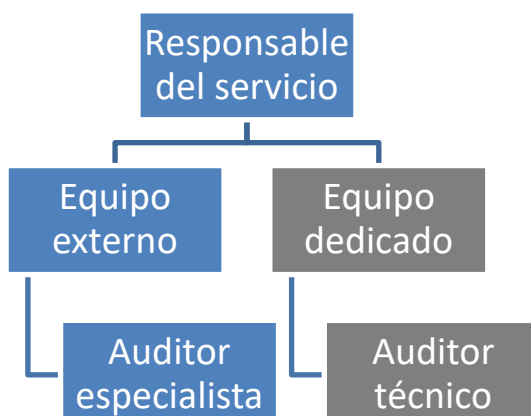
- **Responsable del servicio:** el contratista adscribirá al contrato a un responsable del servicio, quien se encargará de gestionar el contrato y las actividades de los auditores que participen en el proyecto. Así mismo, tendrá que comunicarse con la persona que designe Cyberzaintza como interlocutor, o con quien este último considere, para las labores de gestión del contrato y la coordinación de los trabajos de auditoría y retest de seguridad a realizar. Será el responsable de que el servicio se preste con la calidad exigida por Cyberzaintza.
- **Auditores especialistas:** el contratista adscribirá al contrato un equipo con la experiencia y conocimientos necesarios para la correcta prestación del servicio. Se encargarán de definir la metodología de evaluación, de la mejora continua, de realizar todas las auditorías de seguridad y de prestar apoyo al perfil auditor.
- **Auditor técnico:** el contratista adscribirá al contrato un recurso con la experiencia y conocimientos necesarios para la correcta prestación del servicio. Se encargará principalmente de la integración de las capacidades de auditoría en el modelo de Cyberzaintza y de la ejecución de tareas en el ámbito del objeto de la licitación. En el caso de que necesitara formación específica para acometer las tareas objeto del presente contrato, la empresa adjudicataria pondrá los medios para proporcionarle la formación necesaria.

Los gastos correspondientes al proceso de formación y los derivados del mismo correrán a cargo del contratista, teniendo lugar dicha formación fuera de la jornada del tiempo estimado de dedicación al servicio.

Asimismo, el auditor técnico será el encargado de instalar, configurar y operar las herramientas que se suministrarán en el marco de este contrato.

6.2 Organigrama del servicio

El equipo de trabajo encargado de ejecutar las tareas especificadas en el ámbito de este contrato deberá respetar el siguiente organigrama:



6.3 Dimensionamiento y dedicación

Los recursos con los que se dimensione el servicio dependerán de las ofertas presentadas, pero se considera, y por tanto es un requisito mínimo, que para cubrir los roles planteados al menos es necesario que el equipo tenga la capacidad establecida en la siguiente tabla para cada uno de los roles, cumpliendo para ello con la dedicación indicada durante la ejecución del contrato:

	% Dedicación	Contrato (12 meses)	Prórroga 1ª (12 meses)	Prórroga 2ª (12 meses)	Formato
Responsable del servicio	La necesaria para realizar el seguimiento del servicio	Seguimiento del servicio	Seguimiento del servicio	Seguimiento del servicio	Recurso nominal
Auditor especialista	La necesaria para ejecutar los servicios a demanda solicitados	Bajo demanda. Estimación máxima 2.200 horas anuales.	Bajo demanda. Estimación máxima 2.200 horas anuales	Bajo demanda. Estimación máxima 2.200 horas anuales	Pool de auditores (equipo externo)
Auditor técnico	100%	1.700 horas	1.700 horas	1.700 horas	Recurso nominal (equipo dedicado)

6.4 Equipamiento y software para el equipo de trabajo dedicado

El adjudicatario del servicio proveerá al auditor técnico dedicado todo el equipamiento necesario para la prestación del servicio, lo que incluye:

- Portátil con las características suficientes para la prestación del servicio. Cyberzaintza requerirá la instalación de diferentes agentes de ciberseguridad. Así mismo, requerirá una cuenta de administración sobre el mismo.
- Teléfono móvil.
- Licencia de Office 365 de tipo E3.

6.5 Lugar de trabajo

Debido a la naturaleza sensible de la información que se va a gestionar dentro del alcance del contrato, el acceso a los sistemas y la necesidad de coordinación con otras áreas de Cyberzaintza, se hace necesario que el equipo realice la actividad en los siguientes términos:

- Las reuniones de seguimiento mensuales se realizarán de manera específica de forma presencial en las oficinas de Cyberzaintza y requerirán de la participación del perfil Responsable del servicio.
- En el caso de los perfiles Auditores especialistas será necesario, si así se solicita por parte de Cyberzaintza, que realicen su actividad de manera presencial en las dependencias de Cyberzaintza o en otras ubicaciones (alcance geográfico de País Vasco) pertenecientes a las entidades designadas por Cyberzaintza como estratégicas. En aquellos casos en los que no sea necesaria la presencialidad se realizará en las instalaciones del adjudicatario.
- En el caso del perfil Auditor técnico será necesario que realice su actividad de manera presencial en las dependencias de Cyberzaintza. No obstante, la persona responsable de Cyberzaintza podrá establecer para este perfil que, hasta 3 días por semana, pueda realizar su actividad en modalidad de teletrabajo.

El adjudicatario asumirá en su propuesta los gastos derivados de los desplazamientos, dietas etc., que tengan lugar, así como aquellos derivados de la disposición de los medios correspondientes para los mismos y, en general, para la ejecución del proyecto en las condiciones de presencialidad indicadas, y en todo caso, además todos los conceptos establecidos en el anexo I del pliego de condiciones particulares.

6.6 Horario

El desarrollo de los servicios se realizará en el siguiente horario:

- Lunes a jueves: 8h a 17h.
- Viernes todo el año y lunes a viernes de 1 de junio a 30 de septiembre: 8h a 15h.