

MEMORIA TÉCNICA JUSTIFICATIVA Y ECONOMICA RELATIVA AL PROYECTO DE MODIFICACIÓN DEL DECRETO 34/2024, DE 19 DE MARZO, POR EL QUE SE APRUEBAN LOS ESTATUTOS DE LA AGENCIA VASCA DE CIBERSEGURIDAD.

1. MEMORIA TÉCNICA JUSTIFICATIVA.

(i) Antecedentes y marco normativo.

El [Real Decreto 311/2022](#), de 3 de mayo, regula el Esquema Nacional de Seguridad (ENS), estableciendo los principios básicos y requisitos mínimos necesarios para la protección de los sistemas de información en el Sector Público. Asimismo, establece la necesidad de realizar auditorías para verificar el cumplimiento de dichos requisitos.

La [Guía CCN-CERT IC-01/19](#) establece los criterios generales para la Auditoría y Certificación de los sistemas de información en el ámbito del Esquema Nacional de Seguridad, especialmente dirigidos a los organismos de certificación.

Existen dos clases de Organismos de Certificación del ENS: Las Entidades de Certificación (EC) y los Órganos de Auditoría Técnica (OAT):

	Potestades	Sector	Foco de la actividad	Legitimación
OAT	Ambos organismos de certificación pueden certificar la Conformidad respecto al ENS	Pertenece al sector público	Audita al sector público en su ámbito de competencias	Reconocimiento directamente por el CCN
EC		Pertenece al sector privado	Audita a cualquier organización que así se lo solicite (sector público o sector privado)	Acreditación por ENAC y aceptación por el CCN

Por su parte, la [Guía CCN-STIC 122](#) regula los Órganos de Auditoría Técnica del Sector Público (OAT) y establece los requisitos para ser reconocidos como tales.

La [Ley 7/2023](#), de 29 de junio, de creación de la Agencia Vasca de Ciberseguridad en su Artículo 2 define que 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.

Así mismo, el artículo 7 del [Decreto 34/2024](#), de 19 de marzo, por el que se aprueban los estatutos de la Agencia Vasca de Ciberseguridad, atribuye a Cyberzaintza las siguientes funciones:

- a) Promover una estrategia de ciberseguridad para el conjunto de las administraciones públicas de la Comunidad Autónoma Vasca, y potenciar y coordinar el alineamiento en la ciberseguridad en dicho conjunto.
- b) Impulsar un marco de estándares, directrices y normas técnicas de seguridad recomendables para el sector público vasco.
- c) Informar, con carácter preceptivo, en los procedimientos de elaboración de disposiciones normativas tramitadas por la Administración de la Comunidad Autónoma Vasca en materia de ciberseguridad.
- d) Realizar evaluaciones anuales de las políticas públicas en materia de ciberseguridad desplegadas en el ámbito del sector público vasco.
- e) Prevenir y detectar incidentes de ciberseguridad en la Comunidad Autónoma Vasca y responder a ellos, estableciendo criterios y promoviendo el despliegue de las medidas de protección pertinentes ante las ciberamenazas y los riesgos inherentes sobre las infraestructuras tecnológicas, los sistemas de información, los servicios de las tecnologías de la información y la comunicación, y la información que estos tratan, todo ello con respeto del marco competencial aplicable.
- f) Recoger los datos pertinentes de las entidades que gestionan servicios públicos o esenciales en la Comunidad Autónoma Vasca en relación con el estado de la seguridad de la información, prestando especial atención a los sistemas considerados como críticos para el funcionamiento de los servicios públicos o la seguridad de las personas, con vistas a informar al Gobierno Vasco, así como a las Administraciones Públicas del territorio que intervengan en la prestación de dichos servicios críticos y esenciales, y proponer las medidas adecuadas llevando a cabo la gestión de riesgos en materia de ciberseguridad.
- g) Ejercer las funciones de equipo de respuesta a emergencias (CERT), competente en la Comunidad Autónoma Vasca. Al tratarse de un fenómeno transfronterizo, es necesaria la colaboración con administraciones y agencias de otros territorios con el objetivo de minimizar los daños y el tiempo de recuperación en caso de ciberataque.
- h) Coordinar los equipos de respuesta a incidentes de ciberseguridad (CSIRT) y equipos de respuesta a emergencias o entidades equivalentes que actúen en su ámbito de actuación y de acuerdo a la legislación vigente, estableciendo modelos de colaboración con otros CSIRT nacionales e internacionales. Asimismo, la Agencia ejercerá funciones de alerta temprana y de ayuda en la respuesta ante amenazas, vulnerabilidades, ataques e incidentes de seguridad, en el ámbito del sector público vasco.
- i) Trabajar en pro de una cooperación más estrecha con las universidades y los organismos de investigación con el fin de contribuir a un planteamiento estratégico para reducir la dependencia de productos y servicios de ciberseguridad de fuera de la Unión Europea y reforzar las cadenas de suministro de dentro de la Unión Europea.
- j) Investigar y analizar tecnológicamente los ciberincidentes y ciberataques sobre infraestructuras tecnológicas, sistemas de información, servicios de tecnologías de la información.
- k) Garantizar un nivel adecuado de ciberseguridad en el uso de los medios electrónicos.
- l) Organizar actividades de difusión, promoción, formación y concienciación en materia de ciberseguridad.

- m) Organizar actividades para promocionar el talento en la ciberseguridad, y participar en actividades de ciberseguridad, dando a conocer referentes, haciendo especial hincapié en las mujeres profesionales de la ciberseguridad.
- n) Proponer medidas técnicas de ciberseguridad en la utilización de los recursos informáticos y de las comunicaciones existentes, y proponer la formación en estas medidas del personal de la Administración de la Comunidad Autónoma Vasca y del propio personal de la Agencia.
- o) Actuar como apoyo, en materia de ciberseguridad, de cualquier autoridad competente para el ejercicio de sus funciones públicas y, en particular, en las tareas de lucha contra las conductas ilícitas, incluidas la intervención directa y la obtención de pruebas electrónicas.
- p) Coordinar al sector público vasco en la elaboración de sus respectivos planes de ciberseguridad, así como en la consecución de los objetivos establecidos en los mismos.
- q) Poner sus servicios materiales y técnicos de ciberseguridad a disposición del sector público vasco.
- r) Impulsar la coordinación del sector público vasco en todo lo que se considere necesario para la consecución de los objetivos especificados en los planes de ciberseguridad, estableciendo para ello las líneas de colaboración que se entiendan necesarias.
- s) Ostentar la representación oficial del sector público vasco ante organismos internacionales, estatales y regionales en materia de ciberseguridad.
- t) Apoyar e impulsar la capacitación en materia de ciberseguridad y el desarrollo digital seguro en el ámbito empresarial y en los sectores esenciales de la Comunidad Autónoma Vasca, como son el sector sanitario, el sector de emergencias y seguridad, el sector de servicios sociales y de intervención social, el sector educativo, el sector del transporte y el sector de la energía y las telecomunicaciones, o cualquier otro sector que pudiera considerarse sensible.
- u) Cualesquiera otras competencias que le sean conferidas por la legislación vigente o le sean expresamente delegadas o atribuidas.

(ii) Órganos de Auditoría Técnica del Sector Público.

El ENS es de aplicación a todo el sector público y, consecuentemente, la necesidad de realizar auditorías bienales de los sistemas de información comprendidos en el ámbito de aplicación del Real Decreto 311/2022 también lo es. Actualmente dichas auditoría se realizan en Euskadi exclusivamente a través de Entidades de Certificación privadas.

En este contexto, para poder cumplir con su mandato, es necesario que **Cyberzaintza se establezca como Órgano de Auditoría Técnica del Sector Público**. Esto permitiría realizar auditorías desde una posición de proximidad, garantizando la imparcialidad y objetividad propias de los organismos públicos. Además, la familiaridad de Cyberzaintza con el funcionamiento diario del sector público vasco facilitaría auditorías más alineadas con las particularidades de las entidades públicas de Euskadi. Adicionalmente, al concentrar la contratación, se generaría una economía de costes y el proceso de auditoría sería más homogéneo que si fuese realizada por una o varias Entidades de Certificación privadas.

El establecimiento de Cyberzaintza como Órgano de Auditoría Técnica del Sector Público fomentaría el desarrollo de las funciones que le confiere la Ley, en especial aquellas relacionadas con la coordinación y el alineamiento en materia de ciberseguridad.

(iii) Requisitos para el reconocimiento como Órgano de Auditoría Técnica.

Pueden erigirse como Órganos de Auditoría Técnica del Sector Público aquellas entidades, órganos, organismos o unidades vinculadas o dependientes de las Administraciones Públicas **cuyas competencias incluyan el**

desarrollo de auditorías de sistemas de información, así conste en su normativa de creación o decretos de estructura y quede garantizada la debida imparcialidad.

A continuación, se detallan los dos requisitos fundamentales para el reconocimiento como Órgano de Auditoría Técnica del Sector Público:

- Capacidad técnica y organizativa para la realización de Auditorías de Seguridad, evaluando los requisitos que dispone el ENS para los sistemas de información auditados.
- Imparcialidad y ausencia de conflicto de intereses entre el OAT y la entidad titular, responsable o usuaria del sistema de información en cuestión.

Si bien la agencia ostenta actualmente la función de realizar evaluaciones anuales de las políticas públicas en materia de ciberseguridad en el sector público vasco, es necesario distinguir dicha labor del desarrollo completo de auditorías de sistemas de información. Las evaluaciones se centran principalmente en el análisis de la eficacia y el alcance de las estrategias y políticas implementadas, aportando una visión global y orientada a la mejora continua de la gobernanza en ciberseguridad. Sin embargo, la función de auditoría implica un examen técnico, sistemático y detallado de la conformidad de los sistemas de información respecto a los requisitos normativos, especialmente los definidos por el Esquema Nacional de Seguridad (ENS).

Por ello, se propone **incorporar en el Artículo 7 del Decreto 34/2024**, de 19 de marzo, por el que se aprueban los estatutos de la Agencia Vasca de Ciberseguridad, **la función de realizar auditorías de los sistemas de información**.

Este cambio permitirá cerrar la brecha funcional, posibilitando que la Agencia Vasca de Ciberseguridad pueda ser conocida Órgano de Auditoría Técnica. De esta manera, se dotará al sector público vasco de una capacidad especializada para llevar a cabo Auditorías de Certificación de la Conformidad con el ENS, cumpliendo con el rigor y la objetividad exigidos.

2. MEMORIA ECONÓMICA.

Los Órganos de Auditoría Técnica del Sector Público deben mantener actualizada la información relacionada con su estructura interna, incluyendo su organización, equipos constituidos y listado nominal del personal habilitado para llevar a cabo Auditorías de Certificación de la Conformidad con el ENS.

En un OAT, además del personal que participa en las evaluaciones formando el Equipo de Auditoría, que podría incorporarse bajo la modalidad de prestación de servicios, es fundamental contar con otras figuras relevantes para la organización; se trata de la persona responsable técnica, la persona que lidera el equipo auditor y la persona revisora de expedientes.

A continuación, se especifican las figuras mínimas requeridas y los criterios que deben cumplir para la realización de Auditorías de Certificación de Conformidad con el ENS:

Figura	Funciones	Requisitos
Responsable Técnica	Coordinación técnica del personal que participa en las evaluaciones, así como de la elaboración, adecuación o supervisión de las normas internas y procedimientos relacionados con su función evaluadora	
Responsable del Equipo Auditor	Supervisión de todo el proceso de auditoría, y la exactitud de los hallazgos observados y el dictamen final, así como preservar las evidencias de la auditoría	- Formación en auditorías de sistemas de información. - Experiencia verificable de, al menos, cuatro (4) años, en la realización regular de auditorías, evaluaciones o inspecciones de seguridad en tecnologías de la información. - Conocimientos demostrables de seguridad de la información y gestión de riesgos de seguridad, al menos, cuatro (4) años en estas competencias. - Conocimiento demostrable de los requisitos del ENS, que comprendan un mínimo de veinte (20) horas de formación. - Conocimientos de la legislación aplicable cuando la auditoría pueda requerir la evaluación de la conformidad de medidas derivadas del cumplimiento de otras normativas, tales como las de protección de datos o el Esquema Nacional de Interoperabilidad, entre otras.
Revisora de los expedientes de auditoría	Verificación de los diferentes expedientes de auditoría que tramite el OAT antes de la adopción de la decisión final de certificar, o no, el sistema de información auditado.	Al menos, las exigidas para la persona Responsable del Equipo Auditor de cara a posibilitar una ejecución de la evaluación eficaz. Todo ello de acuerdo con el epígrafe 7.5 de la norma ISO/IEC 17065:2012.
Un número suficiente de personas auditoras para la correcta realización de las auditorías aceptadas contractualmente.		

Actualmente, en la Agencia Vasca de Ciberseguridad están creadas las plazas que cubren las dos primeras figuras, mientras que aún no se ha creado la plaza específica para la persona que desempeñaría la figura de Revisora de los expedientes de auditoría. Esta plaza (nivel retributivo 27) ya está planificada y recogida entre las necesidades que se venido han trasladando desde finales de 2024 a la Dirección de Empleo Público, si bien su inclusión en la RPT de Cyberzaintza todavía no ha sido aprobada.

A continuación, se detallan los costes anuales asociados a la creación de dicha plaza:

LANPOSTUAREN ZENBATEKOA / IMPORTE PLAZA	GIZARTE SEGURANTZAREN ZENBATEKOA / IMPORTE SS	GUZTIRA / TOTAL
68.006,77€	18.115,39€	86.122,16€

Además, resulta imprescindible estimar el coste asociado a la contratación de un servicio externo para la ejecución de las auditorías, con el fin de garantizar que el número de personas que integran el Equipo Auditor pueda adaptarse de manera ágil y eficiente a picos de demanda que superen la capacidad cubierta por las plazas existentes. La previsión de estas necesidades permite responder a posibles escenarios de alta carga de trabajo, asegurando la calidad y los plazos de las evaluaciones comprometidas, sin que las limitaciones estructurales de personal supongan un obstáculo para el cumplimiento de los objetivos establecidos.

A continuación, se detalla el coste anual asociado a dicha contratación de servicios externos:

COSTE (SIN IVA)	IVA (21%)	COSTE TOTAL CON IVA)
100.000,00€	21.000,00€	121.000,00€

14604241T
FRANCISCO
JAVIER
DIEGUEZ (R-
Q0100620D)

14604241T FRANCISCO JAVIER DIEGUEZ (R-
Q0100620D)
Description=BOLETIN OFICIAL PAIS VASCO,
OID 2.5.4.97=VATES-Q0100620D, OU=Ordezkaritza zuzendaritza
- Certificado de representante, O=AGENCIA VASCA DE
CIBERSEGURIDAD, SERIALNUMBER=14604241T, SN=
DIEGUEZ BARRIOCANAL, G=FRANCISCO JAVIER, CN=
14604241T FRANCISCO JAVIER DIEGUEZ (R-
Q0100620D), C=ES
Estoy aprobando este documento
2025.09.01 23:14:32+02'00'