CONVENIO DE COOPERACIÓN HORIZONTAL ENTRE LA SINDICATURA DE CUENTAS DE CATALUÑA Y LA AGENCIA DE CIBERSEGURIDAD DE CATALUÑA PARA LA ASISTENCIA TÉCNICA Y LA IMPLEMENTACIÓN DE MEDIDAS DE CIBERSEGURIDAD PARA LA CONSECUCIÓN CONJUNTA DE LAS FUNCIONES PÚBLICAS QUE TIENEN ATRIBUIDAS

En Barcelona, a fecha de firma electrónica.

REUNIDOS

Por un lado, la **Sindicatura de Cuentas de Cataluña**, representada por el Ilustre señor Miquel Salazar Canalda, síndico mayor de la Sindicatura de Cuentas de Cataluña, en virtud de las facultades que le confiere el artículo 29 de la Ley 18/2010, de 7 de junio, de la Sindicatura de Cuentas de Cataluña, con NIF S5800001I (en adelante, "la **Sindicatura**").

Por otro lado, la Sra. Laura Caballero Nadales, directora general **de la Agencia de Ciberseguridad de Cataluña**, designada por acuerdo del Gobierno de la Generalidad de Cataluña Acuerdo GOV/1/2025, de 7 de enero, con las competencias que le son atribuidas en virtud de la letra *l*) del artículo 12.3 de los Estatutos de la Agencia, aprobados por Decreto 223/2019, de 29 de octubre, con NIF Q0802270I (en adelante "**la Agencia**").

La Agencia y la Sindicatura podrán ser denominadas conjuntamente como las "**Partes**" e individual e indistintamente, cuando corresponda, como la "**Parte**".

Ambas Partes se reconocen recíprocamente competencia para suscribir el presente "**Convenio**" y, de común acuerdo y reconociéndose plena capacidad para este acto, a tal efecto

EXPONEN

I. La Sindicatura ejerce la función de fiscalización de las cuentas de la Generalidad, los entes locales y el resto del sector público de Cataluña, conforme a los artículos 80 y 81 del Estatuto de autonomía de Cataluña. Entre las funciones establecidas en el artículo 2 de la Ley 18/2010, de 7 de junio, de la Sindicatura de Cuentas ("**Ley 18/2010**"), destaca la revisión de la legalidad, la eficacia y la eficiencia de la gestión económica de los entes públicos, así como la propuesta de innovaciones para mejorar la gestión pública.

A través de estas funciones, la Sindicatura realiza un control exhaustivo sobre las actividades económicas y financieras del sector público catalán. Además, desde la Sindicatura se ha promovido la suscripción de convenios con la Administración de la Generalidad, el Tribunal de Cuentas y otras administraciones para unificar la rendición de cuentas y datos que las diferentes normas imponen. Este proceso se realiza mediante herramientas electrónicas que permiten una interconexión de datos entre las entidades y la Sindicatura, con acceso recurrente a los datos para hacer el volcado de manera continua.

II. Para llevar a cabo estas funciones, la Sindicatura necesita acceder de manera constante a una gran cantidad de información de elevada sensibilidad e importancia institucional. Esta información incluye datos económicos y financieros, informes de auditoría, documentos vinculados a la gestión pública, datos personales de responsables de entidades fiscalizadas y otras informaciones que, por su naturaleza, deben ser tratadas de manera confidencial.

El artículo 4.3 de la Ley 18/2010 establece la obligación de colaboración de las entidades fiscalizadas con la Sindicatura y el deber de facilitar toda la información y documentación requerida para el ejercicio de sus funciones. Esta potestad se refuerza con el reconocimiento de la condición de autoridad al personal de la Sindicatura en el ejercicio de sus funciones de fiscalización, según el artículo 49 de la propia ley, así como en las actuaciones de inspección previstas en el artículo 51.

El acceso a estos datos, así como su custodia y preservación, es fundamental para cumplir con las funciones legales de la Sindicatura y para garantizar la transparencia y la buena gestión de los fondos públicos.

III. La gestión de esta información crítica conlleva riesgos inherentes derivados de la exposición a ciberamenazas, como el acceso no autorizado, el sabotaje de sistemas o el uso malicioso de datos confidenciales. Cualquier incidente en este ámbito podría comprometer la integridad de las actuaciones fiscalizadoras, poner en riesgo el derecho a la protección de datos y afectar al buen funcionamiento y la confianza en las instituciones públicas.

IV. Para mitigar estos riesgos y garantizar un alto nivel de seguridad de la información, la Sindicatura requiere la asistencia técnica de la Agencia para implementar medidas de seguridad robustas y continuas para proteger los datos a los que accede. Esto incluye la adopción de sistemas de cifrado, controles de acceso, vigilancia de los sistemas de información y protocolos para garantizar que la información no sea libremente accesible.

V. La Agencia es una entidad de derecho público de la Administración de la Generalidad de Cataluña que actúa con plena autonomía orgánica y funcional, objetividad e independencia técnica y profesional, adscrita al Departamento de la Presidencia. Actúa en cumplimiento de la Ley 15/2017, de 25 de julio de 2017, de la Agencia de Ciberseguridad de Cataluña ("**Ley 15/2017**").

VI. La Agencia tiene como objetivo garantizar la ciberseguridad en el territorio de Cataluña, entendiéndola como la seguridad de las redes de comunicaciones electrónicas y los sistemas de información en los ámbitos de su competencia y respetando siempre las competencias del Estado (artículo 2.4.*a* de la Ley 15/2017, interpretado conforme a los parámetros acotados por la Sentencia del Tribunal Constitucional 142/2018, de 20 de diciembre).

La Ley 15/2017 y sus Estatutos, aprobados por el Decreto 223/2019, de 29 de octubre, atribuyen a la Agencia una serie de funciones clave, entre las que destaca la prevención, detección y respuesta ante incidentes de ciberseguridad (artículo 6.2.*a* de la Ley 15/2017). Estas funciones implican la adopción de medidas de seguridad ante las ciberamenazas que pueden afectar a las infraestructuras tecnológicas, los sistemas de información, los servicios de las tecnologías de la información y la comunicación, y la información que estos tratan.

La Agencia desempeña sus funciones en el marco de la ciberseguridad del sector público catalán, con tareas como la planificación y gestión de la ciberseguridad en la Administración de la Generalidad y su sector público (artículo 6.2.*b* del Decreto 223/2019), la detección y respuesta a incidentes (artículo 6.2.*a* del Decreto 223/2019), y el análisis de riesgos y gestión de la seguridad de las infraestructuras tecnológicas (artículo 6.2.*g* del Decreto 223/2019). Además, la Agencia tiene la responsabilidad de ejercer funciones como equipo de respuesta a emergencias (CERT), coordinar las actuaciones en materia de ciberseguridad con otros organismos nacionales e internacionales, y velar por la continuidad de los servicios y la protección de las infraestructuras de la Generalidad y otras entidades públicas (artículo 6.2.*h* del Decreto 223/2019).

Para la consecución de estos objetivos, la Agencia puede suscribir cualquier tipo de convenio (artículos 1.4 y 8 del Decreto 223/2019).

VII. De este marco normativo se infiere que el objetivo de la Agencia es cubrir todo el territorio de Cataluña, incluyendo todas las administraciones públicas y su sector público, ejerciendo las competencias asignadas y respetando los límites establecidos por la Sentencia del Tribunal Constitucional 142/2018.

VIII. Aunque la Ley 15/2017 no incluye expresamente a la Sindicatura dentro del ámbito operativo de la Agencia, desde estas instituciones se promovió su incorporación en una propuesta de modificación legislativa presentada en el anteproyecto de ley de medidas 2024. Aunque esta modificación no prosperó debido a la finalización de la legislatura, ambas entidades han seguido colaborando de manera informal, como lo demuestran los incidentes pasados, incluyendo la asistencia prestada por la Agencia a la Sindicatura en un ciberataque sufrido en noviembre de 2023 y el asesoramiento respecto a la publicación de informes de control de ciberseguridad en 2024.

IX. La necesidad de formalizar esta colaboración nace de la importancia que tiene la seguridad cibernética en el contexto de la Sindicatura, que tiene acceso a datos sensibles relacionados con la gestión pública. La Agencia aporta a la Sindicatura la experiencia técnica y los recursos necesarios para implementar las medidas de seguridad más adecuadas para proteger esta información ante ciberamenazas. Así, se vela para garantizar la seguridad, la confidencialidad y la integridad de los datos que la Sindicatura maneja en su trabajo de fiscalización del sector público catalán.

X. La Sindicatura y la Agencia formalizan este convenio de cooperación dentro del marco legal establecido por la legislación de contratos y régimen jurídico del sector público. En concreto, el artículo 31 de la Ley 9/2017, de contratos del sector público ("**LCSP**"), permite a las entidades del sector público cooperar entre ellas mediante sistemas de cooperación horizontal —sin relación de dependencia—, mediante convenios que cumplan los requisitos establecidos en el artículo 6 de la misma norma (y en el artículo 12.4 de la Directiva 2014/24/UE). Estos requisitos son: (i) las entidades no deben tener vocación de mercado; (ii) el convenio debe establecer una cooperación con el objetivo común de garantizar la prestación de los servicios públicos que las incumben; y (iii) la cooperación debe ser guiada exclusivamente por consideraciones de interés público.

En interpretación de estos requisitos, la Sentencia de 28 de mayo de 2020 del Tribunal de Justicia de la Unión Europea (asunto C-796/18) admite la cooperación entre entidades públicas cuando esta implique actividades de apoyo a servicios públicos que cada uno los participantes deben prestar, incluso de manera individual, siempre que estas actividades contribuyan a

la realización efectiva de los servicios públicos. Así pues, el TJUE acepta que las relaciones entre entidades públicas pueden presentar los elementos esenciales definitorios de un contrato público —esto es, onerosidad y un objeto comprensivo de una prestación de servicios suministros y obras— y no quedan automáticamente sujetas a la normativa de contratación pública.

Por su parte, la Junta Consultiva de Contratación Pública de Cataluña también ha interpretado esta cuestión a la luz de la normativa europea y los pronunciamientos del TJUE (Informes 7/2020, de 17 de junio, 3/2019, de 13 de marzo y 6/2017, de 16 de mayo). Así, en el Informe 23/2024, de 25 de julio, la Junta Consultiva afirma que "los convenios que establecen una cooperación horizontal entre entidades públicas tienen por objeto garantizar la realización de una misión de servicio público común a las entidades y quedan excluidos del ámbito de aplicación de la normativa sobre contratación pública a pesar de presentar elementos definitorios de los contratos públicos". En estos casos no habrá transferencias financieras entre las partes, más allá del reembolso de los costes reales de los servicios, obras o suministros.

XI. De acuerdo con este marco normativo, el presente convenio se inscribe plenamente en una cooperación horizontal activa entre las dos instituciones. La Agencia aportará el soporte técnico necesario para garantizar que los sistemas de información de la Sindicatura estén protegidos ante ciberamenazas, manteniendo la confidencialidad, integridad y disponibilidad de los datos gestionados por la Sindicatura. Así, la Sindicatura podrá seguir ejerciendo sus funciones de fiscalización con las garantías de seguridad requeridas, asegurando que la información sensible que maneja esté protegida, permitiendo su análisis y difusión de forma segura y en cumplimiento de las normativas aplicables.

Ambas partes manifiestan su voluntad de colaborar al amparo de los artículos 47 a 53 de la Ley 40/2015, de régimen jurídico del sector público ("**Ley 40/2015**"), de la Ley 26/2010, del 3 de agosto, de régimen jurídico y de procedimiento de las administraciones públicas de Cataluña, y de los artículos 6.2 y 31 de la LCSP, dada la naturaleza jurídica pública de ambas entidades y el carácter no contractual de la relación que se pretende materializar, con sujeción a los siguientes

PACTOS

PRIMERO.- OBJETO

1.1. El objeto del presente Convenio es establecer el marco de cooperación que debe permitir mejorar la seguridad cibernética de la Sindicatura, en particular, mediante la colaboración de la Agencia, que aportará el apoyo técnico necesario para garantizar la protección de los sistemas de información de la Sindicatura ante ciberamenazas.

1.2. La formalización de este Convenio tiene como objetivo contribuir a la ejecución de las políticas públicas en materia de seguridad cibernética, en concreto, para garantizar que la Sindicatura pueda ejercer sus funciones con las garantías de seguridad requeridas, especialmente, en cuanto a la protección de los datos confidenciales y la integridad de sus informes en el marco del control del sector público catalán.

SEGUNDO.- COMPROMISOS Y OBLIGACIONES DE LAS PARTES

Para alcanzar los objetivos perseguidos con el presente Convenio, las Partes se comprometen conjuntamente a asumir los siguientes compromisos:

2.1 Compromisos de la Agencia de Ciberseguridad de Cataluña:

(i) Ayudar a la Sindicatura en la mejora continua de sus capacidades de prevención, protección, detección y respuesta ante incidentes de seguridad. En este sentido, **se colaborará en el establecimiento o actualización de un programa de seguridad de la Sindicatura**, dando soporte en la definición de iniciativas, políticas internas, procedimientos y controles para garantizar la protección de los datos y sistemas. La Agencia orienta este apoyo en base a cinco ejes fundamentales: sistemas de información críticos, personas, cultura, gobernanza e infraestructuras transversales.

(ii) En la línea de lo estipulado en el punto anterior, también se contempla la colaboración en el despliegue del modelo de ciberseguridad definido por la ACC (como paso previo a una integración adecuada con la propia ACC), asesorando técnicamente y proporcionando los soportes necesarios para identificar las prioridades de actuación y establecer las medidas que resulten más adecuadas de acuerdo con el nivel de riesgo y la criticidad de los datos gestionados por la institución.

(iii) Asistencia en la **respuesta a ciberincidentes y asistencia técnica** ante amenazas, ataques o vulnerabilidades que puedan afectar a la Sindicatura.

Este apoyo incluirá acciones de identificación, contención, recuperación y recomendaciones de mejora para reducir riesgos futuros.

(iv) Organizar actividades de sensibilización y formación realizadas directamente por la Agencia, para contribuir a la mejora de la cultura de ciberseguridad en la Sindicatura, con el fin de reforzar la seguridad de sus sistemas y la capacidad de respuesta ante incidentes.

En la ejecución de estas actuaciones de difusión y formación, ambas Partes podrán acordar actuaciones concretas y detalladas para dar cobertura a las necesidades planteadas. La ejecución de estos planes de difusión y formación se podrá llevar a cabo en colaboración con otras administraciones u organismos públicos para maximizar su impacto así como facilitar su organización.

2.2 Compromisos de la Sindicatura de Cuentas de Cataluña:

(i) Utilizar las herramientas, plataformas, soluciones, materiales, información y otros elementos que haya puesto a disposición la Agencia para el ejercicio de las funciones propias de la Sindicatura, de acuerdo con los niveles establecidos de disponibilidad, configuración de los sistemas y usos establecidos.

(ii) Proporcionar los medios técnicos y humanos necesarios para desplegar las prestaciones de ciberseguridad en los servicios de la Sindicatura, organizando las tareas, reuniones o planes de despliegue que sean necesarios para implementar las soluciones acordadas con la Agencia.

(iii) Comunicar a la Agencia cualquier incidente de ciberseguridad que tenga un impacto en los sistemas de la Sindicatura, a través del sistema de respuesta a incidentes de ciberseguridad (CERT), para garantizar el apoyo técnico y la correcta recuperación de los sistemas afectados.

(iv) Facilitar a la Agencia toda la información necesaria para poder acceder a las prestaciones acordadas, incluyendo los datos y documentos que la Agencia necesite para desarrollar las acciones de seguridad, garantizando que estos datos sean exactos, completos y adecuados para el uso en el ámbito de la ciberseguridad.

(v) Difundir, en colaboración con la Agencia, los materiales, informes y campañas de sensibilización y formación sobre ciberseguridad entre el personal de la Sindicatura para asegurar la mejor comprensión y aplicación de las medidas de seguridad establecidas.

(vi) Participar activamente en la promoción de la seguridad cibernética en la Sindicatura, implementando las campañas de seguridad que se consideren necesarias y trabajando con la Agencia en la creación de una cultura de ciberseguridad robusta a todos los niveles de la organización.

2.3 En caso de que se produzca una incidencia o brecha de seguridad derivada de las actuaciones técnicas objeto de este Convenio que pueda afectar la información o los sistemas de la Sindicatura, las Partes cooperarán inmediatamente para identificar las causas, corregir los efectos y restablecer la normalidad en el funcionamiento de los sistemas afectados.

2.3.1 La Sindicatura se compromete a comunicar a la autoridad de control competente cualquier incidencia o brecha de seguridad que produzca una violación de la seguridad de los datos personales en los términos y plazos establecidos por el artículo 33 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 ("**RGPD**"), y la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales ("**LOPD**"). En su caso, también deberá notificarlo a los interesados afectados, conforme al artículo 34 del mismo reglamento.

A estos efectos, la Agencia, en el marco del presente Convenio, prestará a la Sindicatura el soporte técnico, documental e institucional necesario para el análisis de la brecha, la identificación de riesgos para los derechos y libertades de los afectados y la elaboración de la documentación de soporte técnico que sea necesaria para la tramitación de las notificaciones mencionadas. Además, la Agencia colaborará en la defensa de la Sindicatura ante posibles procedimientos administrativos o reclamaciones de responsabilidad vinculadas a la brecha de seguridad, acreditando la trazabilidad de la incidencia y las medidas correctoras adoptadas.

TERCERO.- COMPROMISOS DE CONTENIDO ECONÓMICO

3.1 Inexistencia de compromisos económicos generales: Las Partes acuerdan que la colaboración establecida en este Convenio no implicará una transferencia directa de fondo entre ellas con carácter periódico, exceptuándose los casos donde se requieran reembolsos por costes derivados de las prestaciones, servicios o recursos específicos que deban proporcionar de acuerdo con lo previsto en el presente pacto. Todos los costes generales derivados de la colaboración serán asumidos por cada parte en función de sus propios recursos, de acuerdo con los presupuestos anuales correspondientes.

3.2 Reembolso de costes por acciones concretas: Se prevé con carácter general el reembolso de los costes derivados de las actuaciones concretas que pueda llevar a cabo la Agencia en el ámbito de sus funciones.

El presente Convenio no constituye una prestación de servicios a efectos del Impuesto sobre el valor añadido (IVA), por lo que la aportación realizada, en su caso, no quedará grabada por el referido tributo.

3.2.1 **Tipologías de actuaciones:** La Agencia pondrá a disposición de la Sindicatura el porfolio de actuaciones de ciberseguridad de acuerdo con el modelo de gobernanza establecido y con las necesidades de seguridad identificadas. Las actuaciones en materia de ciberseguridad se dividen en dos categorías:

(i) Gobernanza y despliegue del modelo de ciberseguridad.
(ii) Actuaciones específicas en ciberseguridad.

Lo anterior de conformidad con el Anexo I y II en el presente Convenio.

3.2.2 **Compensación:**

La Agencia comunicará a la Sindicatura los costes derivados de las actuaciones solicitadas. **Los costes detallados para cada actuación serán acordados mediante adendas**, que establecerán tanto actuaciones a acometer como la compensación económica correspondiente.

3.3 Condiciones de reembolso: El reembolso de costes se realizará de acuerdo con las condiciones establecidas en el presente Convenio y con la presentación de la documentación justificativa correspondiente.

3.4 Contribución por actividades conjuntas: En el caso de organizar actividades conjuntas (formación, sensibilización, eventos, etc.), las Partes acordarán previamente la distribución de los costes asociados. Si alguna de las Partes asume totalmente los costes de una actividad, la Parte beneficiaria podrá abonar una cantidad acordada por su participación, según el criterio que se fije en cada caso.

3.5 Previsión anual de los compromisos económicos: Las Partes acordarán, en el marco de la reunión anual de la Comisión de Seguimiento, la previsión de los compromisos económicos derivados de la ejecución del presente convenio para el ejercicio siguiente. Esta previsión deberá tener en cuenta las actuaciones programadas, las prioridades de colaboración y los recursos disponibles, y podrá dar lugar, en su caso, a la aprobación de una adenda para concretar su alcance y los importes correspondientes.

CUARTO.- VIGENCIA

4.1 El presente Convenio tendrá una vigencia de cuatro (4) años contados desde la fecha de su firma.

4.2 La vigencia inicial del Convenio podrá ser prorrogada, de forma expresa y por escrito, por los períodos que convengan las Partes, siempre que consideren que la colaboración sigue siendo necesaria y eficaz para los objetivos establecidos. En todo caso, las prórrogas, sumadas, no podrán exceder un nuevo período de cuatro (4) años adicionales.

4.3 Para hacer efectiva la prórroga del Convenio, cualquiera de las Partes firmantes podrá comunicar a la otra su voluntad de prorrogar o no el Convenio con una antelación mínima de tres meses antes del fin de su duración inicial o de cualquiera de sus prórrogas. En caso de no acordar la prórroga en el tiempo y forma establecidos, el Convenio se considerará finalizado a la expiración del periodo inicial o prorrogado, según corresponda.

QUINTO.- MECANISMOS DE SEGUIMIENTO, VIGILANCIA Y CONTROL DE LA EJECUCIÓN DEL CONVENIO

5.1 Comisión de Seguimiento: Se constituye una Comisión de Seguimiento con el objetivo de velar por el cumplimiento de los compromisos establecidos en este Convenio. La Comisión estará formada por un máximo de 3 representantes de cada una de las Partes y formarán parte de ella, en todo caso, la persona que ostente la Dirección de la Agencia y un representante de la Secretaría General de la Sindicatura.

5.1.1 La Comisión será responsable de llevar a cabo un seguimiento exhaustivo de la ejecución del Convenio, mediante la revisión de documentación, informes y otras evidencias relacionadas con las acciones de seguridad implementadas. Igualmente, valorará la efectividad de las medidas adoptadas, identificará posibles áreas de mejora y podrá proponer ajustes en las actuaciones a desarrollar.

5.1.2 la Comisión se reunirá siempre que lo solicite alguna de las Partes y, como mínimo, una vez al año, con el fin de evaluar el estado de la colaboración, el grado de logro de los objetivos y la resolución de incidencias que puedan haber surgido.

5.1.3 Asistirán a las reuniones los responsables designados por las Partes, que analizarán conjuntamente los resultados obtenidos y acordarán, en su caso, las acciones correctoras pertinentes. En la reunión anual se llevará a cabo, igualmente, la rendición de cuentas sobre los compromisos técnicos y económicos asumidos.

5.2 Informes de seguimiento: La Agencia remitirá a la Sindicatura informes de seguimiento con la periodicidad que determine la Comisión, con información sobre la evolución de las actuaciones implementadas, las incidencias detectadas y las medidas adoptadas. Los informes se entregarán dentro del plazo máximo de treinta días a contar de la finalización de cada periodo acordado.

5.3 resolución de discrepancias: En caso de que se detecten discrepancias o problemas en la ejecución o interpretación del Convenio, las Partes acordarán conjuntamente medidas correctivas y establecerán un plazo para su implementación. Si las discrepancias persisten, se hará uso de la mediación u otros mecanismos que las partes consideren adecuados para resolver cualquier disputa.

SEXTO.- MODIFICACIÓN Y DESARROLLO

6.1 Este Convenio podrá ser modificado de mutuo acuerdo por las Partes, modificación que habrá que recoger por escrito justificando las circunstancias que la aconsejan y asegurando que se mantiene el objeto y finalidad del Convenio.

6.2 Las modificaciones deberán formalizarse mediante adendas firmadas por las Partes, que pasarán a formar parte integrante del Convenio.

6.3 Las partes podrán desarrollar aspectos técnicos u operativos del Convenio mediante protocolos de actuación, siempre que estos no contradigan el contenido del presente Convenio ni modifiquen su naturaleza jurídica.

6.4 En caso de que durante la vigencia del Convenio se apruebe una modificación normativa que incluya expresamente la Sindicatura en el ámbito subjetivo de actuación de la Agencia, las Partes se comprometen a modificar este Convenio con el fin de adaptarlo al nuevo marco legal. Esta modificación se producirá en la siguiente sesión de la Comisión de Seguimiento que se celebre con posterioridad a la entrada en vigor de la norma.

SÉPTIMO.- INCUMPLIMIENTO DE LOS COMPROMISOS ASUMIDOS

7.1 En caso de incumplimiento por alguna de las Partes de cualquiera de los compromisos asumidos en este Convenio, la Parte afectada lo pondrá en conocimiento de la Comisión de Seguimiento, que requerirá formalmente a la Parte incumplidora su enmienda en un plazo máximo de treinta (30) días naturales desde la recepción del requerimiento.

7.2 Si transcurrido este plazo el incumplimiento persiste y no se ha llegado a ningún acuerdo en el seno de la Comisión de Seguimiento, la Parte afectada podrá notificar formalmente a la otra Parte su decisión de resolver el Convenio.

7.3 La resolución anticipada por esta causa deberá ser comunicada fehacientemente a la otra Parte, e implicará la finalización de las obligaciones pendientes, sin perjuicio del seguimiento de las medidas necesarias para garantizar la protección de la información o la finalización ordenada de las actividades en curso.

OCTAVO.- RESPONSABILIDAD

8.1 Cada Parte será responsable de las actuaciones que lleve a cabo en el marco del presente Convenio, de acuerdo con las funciones y compromisos asumidos. La Agencia, como entidad especializada en materia de ciberseguridad, prestará el soporte técnico acordado con la diligencia exigible, de acuerdo con los estándares técnicos aplicables en cada caso.

8.2 La Sindicatura continuará siendo responsable del contenido y la custodia de la información que trata en el ejercicio de sus funciones, incluyendo aquellos supuestos en los que, a pesar de contar con la asistencia de la Agencia, se produzca una incidencia que afecte a esta información. Sin embargo, las Partes se comprometen a actuar con la máxima diligencia para prevenir y mitigar cualquier riesgo en este ámbito, dentro del marco de colaboración establecido por el presente Convenio.

8.3 La Agencia no será responsable de los daños derivados de la información o instrucciones incorrectas, incompletas o inexactas facilitados por la Sindicatura, ni tampoco de los daños derivados del incumplimiento por parte de la Sindicatura de las recomendaciones o medidas propuestas por la Agencia en el marco de esta colaboración.

8.4 En ningún caso se exigirá ningún tipo de indemnización entre las Partes derivada de la ejecución del presente Convenio, dada la naturaleza institucional de la colaboración y el carácter no contractual de la relación. Sin embargo, la Comisión de Seguimiento establecida en el pacto QUINTO será la encargada de valorar cualquier incidencia relevante y proponer las medidas correctoras que sean necesarias.

NOVENO.- EXTINCIÓN Y EFECTOS

9.1 El presente Convenio se extingue por el cumplimiento de las actuaciones que constituyen su objeto o por resolución anticipada por alguna de las causas establecidas a continuación.

9.2 Son causas de resolución del Convenio:

a) El transcurso del plazo de vigencia del Convenio sin que se haya acordado una prórroga.
b) El mutuo acuerdo expreso y por escrito de las Partes.
c) El incumplimiento de los compromisos asumidos por alguna de las Partes. En este caso, la Parte cumplidora podrá requerir por escrito a la otra que cumpla en los términos previstos en el pacto séptimo.
d) La existencia de una causa de imposibilidad sobrevenida, legal o material, que impida el cumplimiento de las obligaciones asumidas.
e) Cualquier otra causa prevista en el presente Convenio o en la normativa de aplicación.

9.3 La finalización del Convenio dará lugar a su liquidación, con el objetivo de determinar las obligaciones y compromisos pendientes de ejecución, así como el cierre técnico y administrativo de las actuaciones desarrolladas en su marco.

9.4 La extinción del Convenio, por cualquier causa diferente al incumplimiento de alguna de las Partes, no dará lugar al reintegro de las cantidades percibidas, siempre que estas se hayan destinado a la ejecución de las actuaciones comprometidas en el marco de este Convenio.

9.5 Sin perjuicio de lo previsto en los apartados anteriores, si en el momento de extinguirse el Convenio hubiera actuaciones en curso de ejecución, estas continuarán ejecutándose hasta su completa finalización, de acuerdo con lo que establezcan los pactos económicos y técnicos previos.

DÉCIMO.- CONFIDENCIALIDAD

10.1 Las Partes se comprometen a mantener el carácter confidencial de toda la información, documentación, datos y conocimientos a los que tengan acceso en el marco de la ejecución del presente Convenio y que no tengan carácter público, con independencia de su formato o soporte.

10.2 Esta obligación de confidencialidad afecta, entre otros, la información sobre medidas de ciberseguridad, vulnerabilidades detectadas, resultados de análisis o auditorías, metodologías, procedimientos internos, así como cualquier otra información facilitada por la otra Parte en el marco de las actuaciones derivadas del Convenio.

10.3 Las Partes adoptarán las medidas técnicas y organizativas necesarias para preservar la confidencialidad de la información y evitar su alteración, la pérdida, el tratamiento o el acceso no autorizados.

10.4 Solo podrá acceder a la información confidencial el personal propiamente autorizado por cada Parte, que deberá conocer y cumplir las obligaciones derivadas de este pacto. En ningún caso la información confidencial podrá ser divulgada a terceros sin el consentimiento previo y expreso de la Parte que la ha facilitado, excepto en caso de obligación legal o requerimiento judicial o administrativo.

10.5 Las obligaciones de confidencialidad se entienden sin perjuicio del cumplimiento de las obligaciones de transparencia y publicidad que correspondan a cada una de las Partes de acuerdo con la normativa vigente en materia de transparencia y acceso a la información pública.

10.6 La obligación de confidencialidad continuará vigente una vez extinguido el Convenio, mientras la información conserve este carácter, y al menos durante un plazo de cinco (5) años desde la fecha de finalización.

UNDÉCIMO.- PROTECCIÓN DE DATOS

11.1 Las Partes se comprometen a cumplir, en todo momento, la normativa vigente en materia de protección de datos de carácter personal, en especial el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales.

11.2 En caso de que la ejecución de los autos derivados del presente Convenio requiriera el intercambio o acceso a datos personales, las Partes determinarán de forma expresa y por escrito el régimen de responsabilidad de cada Parte, atendiendo a las funciones respectivas conforme al Reglamento (UE) 2016/679.

11.3 En todo caso, las Partes adoptarán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, y velarán por el respeto de los derechos de las personas interesadas, especialmente en relación con el deber de información, el acceso y la rectificación de los datos, la limitación del tratamiento, la portabilidad y la supresión.

11.4 Las obligaciones en materia de protección de datos de carácter personal continuarán vigentes una vez extinguido el Convenio, mientras sea necesario para garantizar el cumplimiento de los principios y obligaciones derivados de la normativa aplicable.

DUODÉCIMO.- RÉGIMEN JURÍDICO Y RESOLUCIÓN DE CONFLICTOS

12.1 El presente Convenio tiene carácter administrativo y queda sujeto a las previsiones de los artículos 47 y siguientes de la Ley 40/2015, la Ley 26/2010 y demás normas de derecho administrativo que resulten de aplicación y supletoriamente por el derecho civil.

12.2 El Convenio queda excluido del ámbito de aplicación de la LCSP, de acuerdo con el artículo 6 de la misma, por tratarse de un instrumento de cooperación interadministrativa que fomenta la colaboración entre dos entidades del sector público para la ejecución de funciones públicas propias de las entidades participantes, en el ámbito de la ciberseguridad y la fiscalización del sector público de Cataluña. Sin perjuicio de esta exclusión, los principios de la LCSP podrán aplicarse de forma supletoria para resolver dudas interpretativas o lagunas que puedan surgir durante la ejecución del Convenio.

12.3 Las Partes se comprometen a resolver, de manera amistosa, cualquier desacuerdo que pueda surgir en la interpretación y cumplimiento del presente Convenio, preferentemente por la Comisión de Seguimiento. En caso de no ser posible un acuerdo en este ámbito, las cuestiones litigiosas que puedan surgir serán resueltas, en su caso, por la jurisdicción contencioso-administrativa, con sumisión expresa a los órganos jurisdiccionales de la ciudad de Barcelona, con renuncia expresa de su propio fuero.

DECIMOTERCERO.- PUBLICIDAD Y TRANSPARENCIA

De conformidad con el artículo 14 de la Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información y buen gobierno, el presente convenio se publicará en el Registro de Convenios de Colaboración y Cooperación de la Generalidad, el cual se integra en el Portal de Transparencia.

* *

Y en prueba de conformidad, las Partes firman electrónicamente el presente Convenio, a un solo efecto, en el lugar y la fecha indicados.

Miquel Salazar Canalda
Sindicatura de Cuentas de Cataluña

Laura Caballero Nadales
Agencia de Ciberseguridad de Cataluña

ANEXO I - DESCRIPCIÓN DE LAS ACTUACIONES PREVISTAS EN EL MODELO DE CIBERSEGURIDAD DE LA AGENCIA

A continuación se describen las acciones a implementar en cada fase del despliegue del modelo, detallando las tareas que corresponden tanto a la Agencia de Ciberseguridad de Cataluña (en adelante, la Agencia) como a la entidad donde se hará efectivo el despliegue.

1.1. Fase preliminar

Se incluyen en esta fase aquellas acciones previas necesarias para desplegar el modelo integral de ciberseguridad (en adelante, el Modelo) de la Agencia.

Corresponde a la Agencia la ejecución de las siguientes acciones:

1. **Identificación del alcance del despliegue**. Análisis previo de la entidad con el objetivo de concretar el alcance del desarrollo y detectar particularidades específicas del ámbito que requieran una especial atención u orientación concreta.

2. **Identificación y revisión de las amenazas** que afectan al ámbito objeto del desarrollo del modelo, en base a las alertas existentes, información de inteligencia operativa y tendencias para este ámbito.

3. **Cuestionario preliminar** con el objetivo de disponer de un contexto suficiente de la entidad para poder abordar las siguientes fases de implementación del Modelo. En este cuestionario se recogerá la siguiente información:

    - Contactos y matrices de escalado ante incidentes
    - Direccionamientos de red
    - Dominios públicos
    - Redes sociales
    - Arquitectura de red
    - Gestión de identidades, control de acceso y autorizaciones
    - Elementos de seguridad transversal
    - Sistemas de información
    - Puesto de trabajo
    - Servicios de correo electrónico
    - Directorio activo

4. **Activación de servicios universales**. Mediante la información recogida a través del cuestionario preliminar, se habilitarán de una manera ágil determinados servicios y procedimientos (monitorización digital, alertas tempranas, procedimientos de gestión de incidentes, etc.) para atender y gestionar adecuadamente las ciberamenazas y los ciberincidentes de la entidad mientras se implementan las sucesivas fases del Modelo.

Corresponde a la entidad la ejecución de las siguientes acciones:

1. Informar sobre el contexto de la entidad y requerimientos específicos, ya sean técnicos o legales, que supongan una especial atención a tener en cuenta durante el despliegue del Modelo, y puedan incidir sobre el catálogo de ciberamenazas a las que está sujeta la entidad.
2. Facilitar la información solicitada en el cuestionario preliminar, para que la Agencia pueda planificar y ejecutar las siguientes fases del despliegue.
3. Convertirse en el interlocutor con los servicios de la entidad, proveedores y servicios de tecnología y ciberseguridad que estén operando en la entidad.
4. Incorporar los servicios y procedimientos establecidos en esta fase preliminar, para gestionar las ciberamenazas y ciberincidentes que puedan suceder mientras se despliegan las sucesivas fases del Modelo.

1.2. Fase 1 - Diagnóstico

En esta fase se identificará el grado actual de exposición a las principales ciberamenazas que sean de aplicación en el ámbito de desarrollo del Modelo.

Corresponde a la Agencia la ejecución de las siguientes acciones:

1. **Análisis de la arquitectura de seguridad:** consultoría del estado de ciberseguridad de la entidad realizada mediante entrevistas y recogida de información, basada en una matriz de controles de ciberseguridad que se consideren necesarios para poder reducir el grado de exposición a las principales ciberamenazas del ámbito. El análisis incluirá, entre otros, controles relativos a la seguridad de la red, de los sistemas de información, los puestos de trabajo, la gestión de identidades y los accesos, la continuidad de los servicios, etc.

2. **Análisis técnico de debilidades y riesgos de ciberseguridad:** ejecución de un conjunto de actividades y pruebas técnicas sobre la infraestructura tecnológica responsabilidad de la entidad, orientadas a identificar el grado de exposición a las ciberamenazas aplicables, utilizando metodologías reconocidas y simulando la forma de actuar de los ciberatacantes. Siempre que sea posible, en estas pruebas se utilizarán el mismo tipo de técnicas y herramientas que usan los ciberatacantes para acceder y explotar vulnerabilidades de la infraestructura tecnológica de una entidad. El alcance y duración de las pruebas dependerá del contexto de amenazas y la complejidad tecnológica de la entidad.

3. **Análisis del cumplimiento inicial del Esquema Nacional de Seguridad**: de entrada el Modelo incluirá el análisis del perfil de cumplimiento específico de requisitos fundamentales de seguridad (PCE RFS). En función del tipo de entidad y de su grado de madurez se podrán aplicar otras categorías del ENS o perfiles de cumplimiento. La evaluación de este estado de cumplimiento inicial se llevará a cabo a partir de la respuesta del formulario preliminar para el despliegue del Modelo y las visitas presenciales y entrevistas por parte del equipo de proyecto de la Agencia.

4. **Elaboración y presentación del informe de diagnóstico**: entrega a la entidad de un primer informe de diagnóstico con los resultados de los diferentes análisis técnicos, de evaluación de controles y de cumplimiento normativo. El informe incorpora un anexo con el detalle de las metodologías, resultados de los análisis técnicos, de los controles de ciberseguridad, de las vulnerabilidades identificadas, de las técnicas MITRE probadas y del resultado del diagnóstico de acuerdo con el cumplimiento del ENS.

Corresponde a la entidad la ejecución de las siguientes acciones:

1. **Soporte en la ejecución de las evaluaciones de controles**, facilitando la información y documentación necesaria que permita dar respuesta tanto a los controles técnicos como de cumplimiento normativo planteados, aportando el detalle necesario para su correcta validación e interpretación en el marco temporal definido para la evaluación. A tal efecto habrá que designar los interlocutores, planificar temporalmente las entrevistas, asignando el tiempo y los espacios necesarios para que las sesiones de evaluación se puedan llevar a cabo con la calidad y los plazos previstos en esta fase.

2. **Soporte en la ejecución de pruebas y análisis técnicos**, facilitando la información, medios, condiciones, acceso y usuarios necesarios para llevarlas a cabo en el marco temporal pactado inicialmente.

3. **Analizar el informe de diagnóstico** presentado por la Agencia como entregable de esta fase, para conocer y validar los aspectos de mejora detectados y proceder a la mitigación de las debilidades más críticas informadas.

1.3. Fase 2 - Plan de seguridad

En esta fase se elaborará y se pondrá a disposición de la entidad el Plan de seguridad que permitirá aumentar la protección y la resiliencia de la entidad ante las ciberamenazas. El plan está compuesto por el conjunto de proyectos derivados del diagnóstico de seguridad realizado durante la fase anterior, así como por las acciones necesarias para llevar a la entidad a la adecuación y certificación en el cumplimiento del ENS.

En su caso, en esta fase, se elaborarán también los planes de protección requeridos por la normativa de protección de infraestructuras críticas o servicios esenciales.

Corresponde a la Agencia la ejecución de las siguientes acciones:

- Elaboración del Plan de seguridad, que incluirá los siguientes contenidos:
    - Estado de ciberseguridad de la entidad

  - Grado de cumplimiento del ENS de acuerdo con el perfil de cumplimiento específico o, en su defecto, con la categoría del ENS que se haya determinado que aplique a la entidad.
  - Detalle de los análisis técnicos y de arquitectura de la infraestructura tecnológica.
  - Relación y detalle de los proyectos, en base a las pruebas y diagnósticos realizados durante la fase anterior, identificando como prioritarias aquellas acciones más relevantes y urgentes a abordar para reducir las debilidades y hacer frente a las principales amenazas. Los proyectos identificarán su impacto tanto en relación con la protección frente a las ciberamenazas aplicables en la entidad (de acuerdo con las funciones de ciberseguridad incluidas en el perímetro de seguridad definido por la Agencia con este propósito), como en relación con el cumplimiento del ENS.
  - Se introducirá una estimación a alto nivel del coste de las iniciativas en base a órdenes de magnitud obtenidas a lo largo del desarrollo del Modelo a diferentes ámbitos por parte de la Agencia a partir de la tipología de entidad, sus volumetrías de sistemas de información y personas y la complejidad y localización de sus sistemas de información, entre otros aspectos que se puedan analizar. Esta estimación inicial tendrá como objetivo dar visibilidad a las necesidades presupuestarias y las capacidades asociadas a la implementación del plan que deberá ejecutar la entidad, quedando fuera del alcance del despliegue del Modelo.

- Presentación del Plan de seguridad, con una explicación completa y detallada, para garantizar la comprensión de los resultados, de los proyectos asociados y de las implicaciones en su ejecución.

<u>Corresponde a la entidad la ejecución de las siguientes acciones</u>:

- Implementación, seguimiento y gobernanza del Plan de seguridad impulsando todas aquellas acciones generales y específicas para alcanzar su consecución (dotación presupuestaria, dotación de capacidades y recursos, etc.).
- Revisión y evaluación del Plan de seguridad, con el objetivo de entender la viabilidad, impacto, y priorización de las medidas previstas ante los órganos de decisión de la entidad.
- Implementación de las medidas propuestas en el plan, coordinándose con los actores pertinentes, y ejecutando un seguimiento de su ejecución hasta su finalización.
- Ejecución de proyectos o planes de acción específicos para la implementación de medidas de elevada complejidad.
- Actualización y documentación del Plan de seguridad para su trazabilidad, auditoría y mejora continua.
- Presentación y seguimiento del Plan de seguridad a la Dirección y/o al Comité de Seguridad de la entidad, para disponer del apoyo necesario para la ejecución de las actuaciones previstas y consecución de los objetivos del plan.

1.4. Fase 3 - integración operativa

Durante esta fase se desplegarán los procesos y servicios necesarios para la integración de la entidad con la Agencia.

Corresponde a la Agencia la ejecución de las siguientes acciones:

- Definición y entrega a la entidad del modelo de relación y protocolos de respuesta ante incidentes.
- Configuración y entrada en funcionamiento de los servicios de detección de amenaza e inteligencia operativa, que deben permitir a la entidad disponer de información proactiva de amenazas y la monitorización digital.
- Despliegue de capacidades de prevención a través de los análisis de exposición a la amenaza sobre los activos publicados.
- Despliegue de capacidades de respuesta mediante las matrices de escalado y los protocolos de gestión de incidentes establecidos.
- Despliegue de las capacidades de detección a través de la integración de las fuentes de los principales activos de seguridad de la entidad en el SOC de la Agencia o SOC Operativo.
- En caso de que la entidad disponga de un SOC Operativo, muchas de las capacidades y servicios descritos en los anteriores puntos se desplegarán y llevarán a cabo mediante el modelo de integración y gobierno operativo de los diferentes SOC Operativos a través el SOC Táctico de la Agencia, y que se encuentran descritos en el anexo III. Desde el SOC Táctico de la Agencia se definirán las estrategias de prevención, detección, protección y respuesta ante ciberamenazas, que el SOC Operativo de la entidad deberá tener como referencia para adaptar a sus propias estrategias.

Corresponde a la entidad la ejecución de las siguientes acciones:

- Aprobación en la entidad del modelo de relación y protocolos establecidos con la Agencia.
- Facilitar la información y llevar a cabo las acciones necesarias para habilitar en la entidad las capacidades de identificación de amenazas, prevención y respuesta a incidentes, de acuerdo con los servicios activados por parte de la Agencia.
- Llevar a cabo las tareas necesarias para habilitar el mantenimiento e integración de las fuentes de los principales activos de seguridad identificados, asegurando su incorporación al SOC de la Agencia para su monitorización.
- Iniciar el despliegue y mantener las capacidades de protección en la entidad, de acuerdo con lo que se determine en el Plan de seguridad, y con el objetivo de disponer de un perímetro de protección adecuado para los sistemas de información, puestos de trabajo y personas.
- En caso de que la entidad disponga de un SOC Operativo, esta tendrá la responsabilidad de garantizar que el SOC Operativo dote de visibilidad al SOC Táctico respecto a la actividad gestionada de la entidad y el grado de exposición a la amenaza, aportando a la Agencia el conocimiento del entorno y el contexto necesario para hacer frente a las amenazas,

ataques e incidentes, haciendo más productiva y operativa la estrategia definida por la entidad. En este sentido la entidad local garantizará la coordinación operativa con el SOC Táctico, a través de un seguimiento periódico según lo que se establezca en el Modelo de integración y gobierno del SOC Operativo de la entidad.

1.5. Fase 4 - Protección

La fase 4 del Modelo es una etapa recurrente que prevé la ejecución de funciones y servicios orientados a ofrecer una protección continua y unas capacidades para gobernar el despliegue del modelo y hacer seguimiento del Plan de seguridad. En este sentido las actualizaciones y nuevas iteraciones de las fases del modelo se invocarán desde esta fase de operación continua.

Corresponde a la Agencia la ejecución de las siguientes acciones, que incluirán el despliegue de funciones y servicios recurrentes de la Agencia:

- **Servicios de Operaciones de Ciberseguridad de la Agencia** (en adelante, SOC de la Agencia): Servicio 24×7 de monitorización del estado de seguridad de la entidad y respuesta a incidentes, mediante el despliegue de capacidades de inteligencia operativa, detección, prevención y respuesta, una vez integradas las herramientas tecnológicas de seguridad de la entidad. En caso de que la entidad disponga de un SOC Operativo este servicio se facilitará tal y como está previsto en el modelo de integración y gobierno de los SOC Operativos, a través del SOC Táctico de la Agencia.

- **Oficina de Gobernanza y Cumplimiento**: ofrecerá acompañamiento periódico a las entidades y seguimiento de las acciones de los planes de acción para hacer seguimiento de la evolución de la entidad hacia el logro de los objetivos fijados en el Plan de seguridad, así como resolver vulnerabilidades y reducir la exposición a la amenaza. Con un seguimiento con periodicidad mensual, se pondrán a disposición de la entidad cuadros de mando con las métricas e indicadores necesarios para facilitar esta función. También podrá ofrecer acompañamiento a la entidad en la ejecución de las tareas previas y auditoría interna en relación con la preparación a la certificación del Esquema Nacional de Seguridad.

- **Oficina de Comunicación y Cultura de Ciberseguridad**: ofrecerá contenidos y estrategias para que la entidad pueda capacitar y concienciar a la totalidad de su plantilla, con niveles y objetivos de formación adaptados a los perfiles y necesidades correspondientes. En este sentido la oficina ofrecerá el apoyo en la actividad formativa de acuerdo con los siguientes tres niveles:

    - **Nivel básico de formación,** dirigido a todos los empleados públicos de la entidad.
    - **Nivel avanzado de formación**, dirigido a empleados públicos que deben desarrollar capacidades técnicas o legales en relación con la materia con el fin de contar con un abanico más amplio de conocimientos y habilidades.

- **Itinerarios de perfiles especializados de ciberseguridad,** desarrollados a través de la Ciberacademia de la Agencia de Ciberseguridad, con diferentes itinerarios formativos dirigidos específicamente a los técnicos del mundo local que quieren profundizar y ampliar conocimientos, en habilidades y competencias.

- **Oficina Técnica de Ciberseguridad:** oficina dotada con técnicos especialistas en ciberseguridad que tendrán como objetivo ofrecer una prescripción, orientación experta y recomendaciones sobre arquitecturas de seguridad, guías y buenas prácticas a implementar en el diseño y evolución de aplicaciones y sistemas de información.

- **Servicio continuo de cálculo de la superficie de exposición ante ciberamenazas.** Servicio recurrente de pentesting y de realización de análisis de exposición a la amenaza para una actualización periódica del conocimiento de la exposición ante amenazas a la entidad.

- **Simulacros de incidentes.** Sesiones preparatorias con las entidades para que conozcan como se gestiona una cibercrisis y evaluar la capacidad de gestión frente a un ciberincidente y su grado de preparación a través de ejercicios teóricos y prácticos, sin afectación en los entornos de las entidades.

Corresponde a la entidad la ejecución de las siguientes acciones:

- **En relación con los servicios proporcionados por el SOC de la Agencia y para el servicio continuo de cálculo de la superficie de exposición ante amenazas:**

  - Notificar las amenazas e incidentes identificados al SOC de la Agencia o SOC Operativo, y a los interlocutores que formen parte del proceso de escalado y toma de decisiones, para su evaluación y tratamiento.
  - Dar respuesta a las alertas reportadas por el SOC de la Agencia o SOC Operativo.
  - Adoptar la estrategia, acciones, protocolos y procedimientos previstos por el SOC de la Agencia o SOC Operativo como respuesta a un incidente de seguridad.
  - Disponer de capacidades técnicas para llevar a cabo las acciones necesarias (despliegue de políticas, parches, configuraciones, instalación de softwares, adquisición de evidencias, restauración de copias de seguridad, etc.) para hacer frente a los ciberincidentes.
  - Implementar las acciones prescritas desde el SOC de la Agencia o SOC Operativo de la entidad, destinadas a mejorar la protección y operación de la seguridad y relativas a la gestión del perímetro de seguridad, la prevención de amenazas, la protección ante ciberataques y la identificación, análisis y gestión de vulnerabilidades.
  - Soporte en la ejecución de pruebas y análisis técnicos, facilitando la información, medios, condiciones, acceso y usuarios necesarios para llevarlas a cabo en el marco temporal pactado inicialmente.

- **En relación con la Gobernanza y Cumplimiento:**

  - Asumir la gestión y gobierno del Plan de seguridad de la entidad para garantizar la existencia de recursos técnicos y las capacidades necesarias en el ámbito directivo y/o del Comité de Seguridad.
  - Llevar a cabo las tareas necesarias para permitir la implementación de las diferentes fases del Modelo.
  - Impulsar el cumplimiento normativo de la entidad con el objetivo de lograr, en la siguiente fase, la certificación de cumplimiento en el ENS y de cualquier otra normativa sectorial o específica que les sea de aplicación.
  - Ejecutar y participar en los procesos de adecuación, despliegue de los proyectos, actuaciones y medidas de seguridad necesarias, para cumplir con el marco normativo y legal de ciberseguridad aplicable a la entidad.
  - Llevar a cabo, para las categorías necesarias, las tareas previas para verificar la adecuación al ENS como paso previo para su certificación.
  - Llevar a cabo los trabajos necesarios, para elaborar, adaptar y mantener la documentación y procedimientos relacionados con el marco organizativo, normativo y operativo en referencia al cumplimiento del ENS siguiendo, cuando estén disponibles, las indicaciones, guías y modelos de referencia a disposición de la entidad.
  - Visibilizar el estado de situación y avance del Plan de seguridad a la Dirección y/o al Comité de Seguridad mediante, entre otras herramientas e información, los indicadores y cuadros de mandos que se pongan a disposición.

- **En relación con la Oficina Técnica en Ciberseguridad:**

  - Realizar las acciones necesarias para velar por la seguridad durante el ciclo de vida de las aplicaciones, adquisición de productos y en la gestión de proveedores, como elementos clave para alcanzar un alto nivel de protección y cumplir con los estándares y normativas vigentes.

- **En relación con la Comunicación y Cultura de Ciberseguridad:**

  - Promover y ejecutar iniciativas formativas de acuerdo con los diferentes niveles propuestos y con el apoyo de la oficina de formación prevista en el Modelo.
  - Adaptar los contenidos, organización y diseño de las actividades formativas a la realidad organizativa y funcional de la entidad.
  - Buscar los recursos y soporte organizativo necesarios para llevar a cabo las acciones formativas previstas.

1.6. Fase 5 - Certificación en el ENS

En esta fase del Modelo se prevé la certificación del Esquema Nacional de Seguridad mediante la realización de auditorías de conformidad. La certificación se podría llevar a cabo desde el Órgano de Auditoría Técnica (OAT) de la Agencia como entidad reconocida por el Centro Criptológico Nacional (CCN), previa conformidad de las partes.

Como se ha comentado en apartados anteriores, el Modelo ofrece por defecto la certificación en el Perfil de Cumplimiento de Requisitos Fundamentales de Seguridad (PCE RFS) que incluye los requisitos mínimos que una entidad debería abordar. El PCE RFS va dirigido a aquellas entidades con dificultades para abordar el proceso de adecuación del ENS o, a aquellas donde se determina que la aplicación de las medidas del PCE RFS son suficientes teniendo en cuenta la postura de seguridad adoptada.

En función del ámbito y de la madurez de las entidades, se prevé que las recertificaciones previstas cada dos años, estén enfocadas a perfiles de cumplimiento específico o categorías del ENS superiores, en su caso.
El enfoque de las recertificaciones se basa en un proceso de mejora continua del cumplimiento impulsado por las entidades.

Inicialmente el alcance previsto de la certificación corresponderá a los servicios identificados en el perfil de cumplimiento específico o en la categoría determinada.

Corresponde a la Agencia la ejecución de las siguientes acciones, en función de la categoría o del perfil de cumplimiento específico a certificar:

- **Certificación en los PCE:** El OAT de la Agencia realizará las auditorías de certificación de los diferentes PCE en todo su ciclo de vida con la revisión de evidencias recogidas en las fases anteriores del modelo, y de acuerdo con el proceso y la metodología µCeENS establecidos por el CCN para los PCE. Como resultado, el OAT de la Agencia emitirá el certificado de conformidad de cumplimiento del ENS, en caso de resultar satisfactoria la auditoría.

- **Certificaciones en las diferentes categorías del ENS:** una vez la entidad esté adecuada, mediante la consecución de las acciones identificadas en el Plan de seguridad y con la implementación por parte de la entidad de todas las medidas necesarias del ENS, y superado el proceso de auditoría interna, el OAT de la Agencia ejecutará el proceso de auditoría mediante el uso de herramientas y la realización de las correspondientes sesiones en la entidad. A tal efecto se podrán utilizar las herramientas previstas por el CCN-CERT en la preparación y ejecución de estos procesos de auditoría.

Corresponde a la entidad la ejecución de las siguientes acciones:

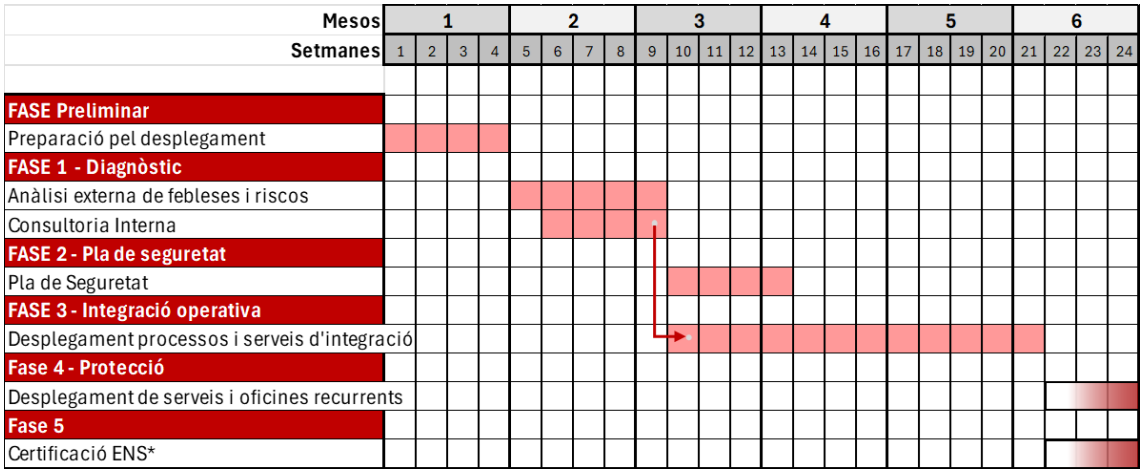
- Ofrecer toda la colaboración necesaria para abordar el proceso de auditoría de certificación.
- Garantizar la disponibilidad de las evidencias necesarias para el proceso de auditoría.
- Garantizar un buen uso del certificado de la auditoría y del distintivo asociado.
- Tener el compromiso para mantener y evolucionar el cumplimiento del ENS, en su caso, en las futuras recertificaciones y llevar a cabo las acciones necesarias.
- Llevar a cabo las tareas necesarias asociadas al gobierno y mantenimiento de la certificación.
- Cuando se realicen auditorías de conformidad con el ENS de categoría media o alta, la Sindicatura deberá comprometerse a suscribir con el OAT los siguientes dos acuerdos que constan en el anexo III del presente Convenio:
    - Acuerdo de derechos y obligaciones de quien se certifica del ENS.
    - Acuerdo de uso de marcas de certificación.

***

ANEXO II - PLANIFICACIÓN TEMPORAL EN EL DESPLIEGUE DEL MODELO

Para el despliegue del Modelo de ciberseguridad, de forma orientativa se prevé de promedio el siguiente calendario temporal para cada una de las fases previstas en el modelo.

Esta planificación de referencia se adecuará durante la fase preliminar de acuerdo con las dimensiones y capacidades de la entidad.



(*) El calendario de certificación en el ENS dependerá de la entidad, de acuerdo con la ejecución que lleve a cabo de las acciones previstas en el Plan de seguridad.

***

ANEXO III - MODELO DE ACUERDO DE DERECHOS Y OBLIGACIONES DE QUIEN SE CERTIFICA EN EL ENS Y DE USO DE MARCAS DE CERTIFICACIÓN

ACUERDO DE USO DE MARCAS DE CERTIFICACIÓN (SELLOS Y CERTIFICADOS)

ACUERDO ENTRE EL AUDITADO CERTIFICADO, O EN PROCESO, Y EL OAT

Las organizaciones, o sus áreas o unidades, que estén certificadas de la conformidad de alguno de sus sistemas de información respecto a las disposiciones del Esquema Nacional de Seguridad (en adelante, ENS), gozarán de una serie de derechos, a la vez que estarán sujetas a una serie de obligaciones de uso de las marcas de certificación, detalladas en este documento.

En consecuencia, [NOMBRE Y APELLIDOS] con DNI [NIF], en calidad de [POSICIÓN en la organización auditada] de [NOMBRE de la organización auditada] reconoce que tiene capacidad suficiente para suscribir este acuerdo.

DETALLE DEL ACUERDO DE USO DE MARCAS DE CERTIFICACIÓN

USO DE LAS MARCAS DE CERTIFICACIÓN

Este Acuerdo se refiere a las marcas de certificación del ENS, basándose en sellos oficiales, cuyo modelo base es propiedad del Centro Criptológico Nacional (CCN), así como certificados de conformidad, cuyo modelo es propiedad del OAT, siguiendo contenidos mínimos y directrices del CCN.

Las marcas de certificación otorgadas por el OAT a la organización, área o unidad que certifica alguno de sus sistemas de información para los fines de dicho documento, estarán alineadas con la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la instrucción técnica de seguridad (ITS), de conformidad con el Esquema Nacional de Seguridad y con cualquier resolución posterior que la reemplace o modifique.

Asimismo, se concretará en base a anexos de la Guía CCN-CERT IC-01/19 sobre criterios generales de auditoría y certificación del ENS, o cualquier otra guía CCN-STIC que se considere.

El uso de la marca de certificación únicamente está autorizado en las condiciones fijadas en el presente documento, comprometiéndose a respetarlo las organizaciones, áreas o unidades con algún sistema de información certificado de conformidad con las disposiciones del ENS. Lleva aparejada la licencia de uso de la marca, en los términos previstos, en calidad de organización que ha obtenido la certificación para alguno de

sus sistemas de información. El uso de esta marca (certificado o sello de certificación) para un período renovable, habitualmente de dos años, se limita estrictamente a la organización, área o unidad que su(s) sistema(s) de información ha(n) estado certificado(s) satisfactoriamente respecto a las disposiciones del ENS para el OAT en calidad de organismo de certificación, no habiendo sido retirados o suspendidos los certificados por el OAT.

La marca de certificación mostrada en el anexo I es un ejemplo de los tres sellos de certificación disponibles en función de la categoría del sistema: BÁSICA, MEDIA O ALTA. Además, el organismo de certificación expondrá a la organización cliente el sistema de información de la que ha sido certificado, un certificado de conformidad con las disposiciones del ENS para la CATEGORÍA y alcance acordados. El OAT se reserva el derecho de reemplazar el sello de certificación mostrada en el anexo I, o el certificado de conformidad con el ENS, por otro en cualquier momento, de común acuerdo con el CCN, aunque siempre se advertirá a las organizaciones, áreas o unidades titulares del certificado de dicha circunstancia, al igual que de cualquier otro cambio que se produzca en el esquema de certificación, siempre alineado con las ITS o guías correspondientes editadas por el CCN.

Únicamente pueden usar la marca de certificación (sello y certificado de conformidad) las organizaciones, áreas o unidades el sistema de información de las que haya sido certificado satisfactoriamente por un OAT reconocido por el CCN, por una entidad de certificación (EC) acreditada por ENAC, o directamente por el CCN en casos especiales.

La autorización del derecho de uso de la marca de certificación (sello y certificado de conformidad) se obtiene con la consecución y posteriores renovaciones de la certificación de conformidad con las disposiciones del ENS. No sustituirá en ningún caso la garantía ni la responsabilidad sobre los servicios soportados por el sistema de información certificado que, de acuerdo con la ley, corresponde al licenciatario de la marca de certificación.

COMPROMISOS DEL LICENCIATARIO

La organización, área o unidad con licencia de uso de la marca de certificación, en calidad de organización certificada, adquiere los siguientes compromisos:

I. Cumplir con todos los requisitos que pueda estipular el esquema de certificación del ENS con relación al uso de las marcas de conformidad y la información relacionada con los servicios soportados por el sistema de información certificado.

II. Mantener los sistemas de información en el ámbito de la certificación de conformidad con el ENS, para los que se ha concedido el derecho de uso de la marca de certificación, conforme a las disposiciones del Esquema Nacional de Seguridad.

III. Aceptar las decisiones tomadas respecto a la aplicación del presente esquema de certificación, según las condiciones establecidas en cada caso.

IV. Facilitar al equipo auditor todos los medios necesarios para realizar las verificaciones que implica la aplicación del presente esquema de certificación.

V. Usar la marca de certificación únicamente en la forma establecida en el presente documento y exclusivamente en relación con su alcance de certificación.

VI. Proceder a realizar la solicitud de una auditoría complementaria ante cualquier modificación que se desee hacer en el alcance y categoría de los sistemas respecto a los que se le haya concedido el derecho de uso de la marca de certificación.

VII. Abstenerse de hacer uso de la marca de certificación cuando haya riesgo de confusión con actividades, productos, procesos, servicios, sistemas de información o partes de la organización que no disfruten del derecho de uso de esta marca de certificación.

VIII. Informar al OAT de cambios en la organización que puedan afectar los sistemas de información en el ámbito del Esquema Nacional de Seguridad, el alcance, o la categoría de la certificación.

CONDICIONES DE APLICACIÓN

El uso de la Marca de Certificación debe cumplir las siguientes condiciones:

I. El Certificado de Conformidad tendrá que aparecer siempre completo, de acuerdo con el literal, y no es posible suprimir conceptos, logotipos, o recortar partes. Debe quedar clara qué organización obtiene la certificación de su sistema de información, así como el OAT que la concede, así como especialmente su vigencia, alcance, categoría, fecha de emisión y validez.

II. Si la organización, área o unidad el sistema de información de la que está certificada debe entregar a un tercero una copia del Certificado de Conformidad o de cualquier otro documento de certificación, esta deberá ser una copia fidedigna del mismo que lo reproduzca en su totalidad, no pudiendo enmendarse o suprimirse parte del contenido a proporcionar.

III. No estará autorizada la utilización de marcas de conformidad por parte de organizaciones sin sistemas de información certificados, con independencia de que exista cierta relación o dependencia con alguna otra organización que sí disponga de ellos.

IV. Si se produce, o se requiere, un cambio que afecte parcial o totalmente la identidad legal que ha obtenido la certificación, deberá exponerse el caso en el Comité de Certificado del OAT que la estudiará y decidirá la forma de abordarlo. En determinados casos se puede requerir elevar una consulta al CCN con el resultado de transferir directamente el certificado a la nueva entidad legal, o bien iniciar un nuevo proceso de certificación.

V. Las organizaciones, áreas o unidades con su sistema de información en proceso de certificación no podrán incluir en sus comunicaciones la marca de certificación con el ENS hasta la finalización del proceso y hasta que les haya sido facilitado por el OAT el correspondiente Certificado de Conformidad con el ENS, que quedará registrado con su referencia identificativa exclusiva.

VI. El sello que se muestre corresponderá claramente a la categoría de los sistemas certificados (BÁSICA, MEDIA o ALTA) en función del tipo de

auditoría realizada en el proceso de certificación, viniendo esta asimismo reflejada en el Certificado de Conformidad con el ENS expedido por el OAT.

VII. En material de papelería únicamente se podrá usar la marca de certificación si está claramente asociada a la organización (tal como aparece en su certificado) y al sistema de información certificado, no pudiendo llegar a interpretarse que podría alcanzar otros sistemas de información que no lo están.

VIII. En material promocional de cualquier índole (anuncios de prensa, TV, Internet, etc., únicamente se podrá usar la marca de certificación si está claramente asociada a la organización certificada (tal como aparece en su certificado) y al sistema de información certificado, no pudiendo llegar a interpretarse que podría abarcar otros sistemas de información que no lo están.

IX. El uso conjunto de otras Marcas de Certificación junto con la de certificación de la conformidad con el ENS, tendrá que ser analizado caso a caso. Para ello la organización solicitante comunicará por escrito al OAT su intención de hacer esta utilización conjunta de marcas. El Comité de Certificación si estima que no entra en contradicción con las normas aquí descritas, informará en su caso al CCN, trasladando la decisión de este a la unidad u organización certificada.

X. Los Sellos de conformidad con el ENS deben reproducirse literalmente, completos, eligiendo el modelo asociado a la categoría del sistema, no estando permitido emplear únicamente el logo genérico del ENS que consta en su interior para denotar que la organización está certificada, puesto que se interpreta como un uso incompleto e ilícito.

XI. Cuando los Sellos de conformidad se ubiquen en una página web, portal o sede electrónica, si se pincha sobre ellos debe visualizarse el Certificado de Conformidad completo.

XII. Según se determina en el artículo 38.2 del RD 311/2022, los sujetos responsables de los sistemas de información certificados de conformidad con el ENS darán publicidad a los correspondientes portales de internet o sedes electrónicas a las certificaciones de conformidad con el ENS, atendiendo a lo dispuesto en la ITS de Conformidad y la guía CCN-CERT IC-01/19.

XIII. Cuando excepcionalmente en un mismo documento se incluyan servicios, tanto amparados como no amparados por la certificación, se señalarán las actividades no amparadas mediante un asterisco o similar, incluso con el mismo tipo de letra que el usado en el cuerpo del documento, en un lugar visible y próximo a la marca, de forma que se perciba a simple vista, la siguiente leyenda *"los [servicios, productos o sistemas según proceda] marcados no están amparados por la Certificación de conformidad con el Esquema Nacional de Seguridad".* En estos casos, la organización, área o unidad certificada someterá a la consideración del OAT los documentos donde piensa colocar la marca, indicando el lugar de su ubicación y los servicios que estarán relacionados.

XIV. La organización certificada no podrá hacer uso de la marca una vez finalizado el periodo de validez del certificado sin su renovación, o después de la entrada en vigor de una suspensión temporal, retirada o renuncia del derecho de uso.

VIGILANCIA DEL USO DE MARCAS DE CERTIFICACIÓN POR EL OAT

Durante todo el periodo de validez de la marca de certificación, que para el ENS se establece inicialmente en dos años, el OAT tiene que realizar todas las verificaciones consideradas necesarias respecto a su buen uso, o encargar su realización a un tercero. Es habitual que estas se lleven a cabo cada 6 meses.

En caso de uso indebido de la marca de certificación, el organismo de certificación a través de su Comité de Certificación puede advertir de ello inicialmente, pudiendo llegar a suspender o retirar inmediatamente la certificación y el derecho a utilizar la marca de certificación.

La organización, área o unidad certificada puede apelar la decisión del Comité de Certificación al Comité de Imparcialidad, si ha sido constituido por el OAT, o lo que es más habitual, al CCN.

RENUNCIA VOLUNTARIA AL USO DE LA MARCA DE CERTIFICACIÓN

La organización, área o unidad certificada puede renunciar o suspender por un periodo de tiempo el uso de la marca de certificación. Notificará por escrito al OAT y realizará todos los cambios necesarios respecto a sus posibles medios de comunicación. Ante estas circunstancias el OAT le informará respecto a los términos y condiciones para la terminación temporal o definitiva del uso de la marca de certificación.

ACEPTACIÓN

Como prueba de aceptación, se firma este acuerdo en [Población], el DD de MES de AAAA, que tendrá sus efectos jurídicos en el momento en el que la organización, área o unidad que lo ha suscrito certifique su sistema de información conforme a las disposiciones del ENS y actúe en calidad de organización, área o unidad certificada por la Agencia de Ciberseguridad de Cataluña.

Directora de la Agencia
Ciberseguridad de Cataluña

El representante del AUDITADO

ANEXO I. REPRODUCCIÓN DE LOS SELLOS OFICIALES DE CERTIFICACIÓN

En cuanto al diseño de los sellos de certificados se estará a lo que dispone la última versión publicada de la guía técnica CCN-STIC-809, junto con sus anexos, y la Resolución de 13 de octubre de 2016 de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad (ITS) de conformidad con el Esquema Nacional de Seguridad, y modificaciones posteriores.

Se reproducen a continuación los sellos proporcionados por el CCN, que asimismo pueden descargarse del portal del ENS:

Certificación. Categoría Básica (RD 311/2022)

Certificación. Categoría Media (RD 311/2022)

Certificación. Categoría Alta (RD 311/2022)