CONVENIO ENTRE EL CENTRO CRIPTOLÓGICO NACIONAL DEL CENTRO NACIONAL DE INTELIGENCIA Y EL CABILDO INSULAR DE TENERIFE, EN MATERIA DE CIBERSEGURIDAD

De una parte, Doña Paz Esteban López, Secretaria de Estado Directora del Centro Nacional de Inteligencia y Directora del Centro Criptológico Nacional (en adelante, CNI-CCN), en virtud del nombramiento efectuado por Real Decreto 266/2020, 4 de febrero («Boletín Oficial del Estado» núm. 31, de 5 de febrero), y en el ejercicio de las competencias que tiene atribuidas por el artículo 9 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

De otra parte, el Sr. Presidente del Cabildo Insular de Tenerife, Sr. D. Pedro Manuel Martín Domínguez, en virtud de nombramiento por acuerdo plenario extraordinario de fecha 24 de julio de 2019, y de acuerdo con el artículo 125.2 de la Ley 8/2015, de 1 de abril, de Cabildos Insulares.

Ambas partes se reconocen plena capacidad jurídica para suscribir el presente Convenio y a tal efecto

EXPONEN

Primero. El Cabildo Insular de Tenerife (en adelante, CIT), de acuerdo al artículo 8 de la Ley Territorial 8/2015, de 1 de abril, de Cabildos Insulares, tiene atribuidas entre otras, las competencias como órgano de gobierno, administración y representación de la Isla, para la prestación directa de servicios públicos a la ciudadanía, así como para la asistencia y la cooperación jurídica, económica y técnica a los municipios, especialmente a los de menor capacidad económica y de gestión, en la prestación de los servicios públicos de competencia municipal.

Segundo. El CIT, además de abordar de forma decidida su modernización, y la de su sector público dependiente, ha establecido, como una prioridad para la actuación insular, la asistencia a la modernización municipal, estableciendo para ello, a través del Reglamento del Servicio de Asistencia Técnica específica en materia de implantación de tecnología de la información, de las comunicaciones y en administración electrónica a los municipios de la Isla, aprobado en Pleno de fecha 29 de junio de 2018, el marco, alcance, condiciones y requisitos exigidos, así como la forma de financiación que en cada caso corresponda.

Tercero. El Centro Nacional de Inteligencia es un Organismo Público, con régimen jurídico propio, contemplado en la Ley 11/2002 de 6 de mayo, reguladora de dicho Organismo, al que se le encomienda, entre otras, el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Cuarto. De acuerdo con el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, el ámbito de actuación de dicho Centro comprende la seguridad de los sistemas de las tecnologías de la información y la comunicación (en adelante, TIC) de la Administración que procesan, almacenan o transmiten información en formato electrónico, que normativamente requieren protección, y que incluyen medios de cifra, y la seguridad de los sistemas de las TIC que procesan, almacenan o transmiten información clasificada.

Dentro de dicho ámbito de actuación, el Centro Criptológico Nacional del Centro Nacional de Inteligencia (en adelante, CNI-CCN) realiza, entre otras, las siguientes funciones:

a) Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y la comunicación de la Administración. Las acciones derivadas del desarrollo de esta función serán proporcionales a los riesgos a los que esté sometida la información procesada, almacenada o transmitida por los sistemas.

b) Formar al personal de la Administración especialista en el campo de la seguridad de los sistemas de las tecnologías de la información y la comunicación.

c) Constituir el organismo de certificación del Esquema nacional de evaluación y certificación de la seguridad de las tecnologías de información, de aplicación a productos y sistemas en su ámbito.

d) Valorar y acreditar la capacidad de los productos de cifra y de los sistemas de las tecnologías de la información, que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura.

e) Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la tecnología de seguridad de los sistemas antes mencionados.

f) Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada en su ámbito de competencia.

g) Establecer las necesarias relaciones y firmar los acuerdos pertinentes con organizaciones similares de otros países, para el desarrollo de las funciones mencionadas.

Por otra parte, el CNI-CCN dispone de los elementos técnicos, humanos materiales y organizativos idóneos para la consecución de los niveles de seguridad óptimos de los sistemas, servicios y redes del CIT y las restantes entidades adheridas al presente Convenio.

Asimismo, el CNI-CCN cuenta con el CCN-CERT, que es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional. Este servicio se creó en el año 2006 y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el Real Decreto 421/2004 regulador del CCN y en el Real Decreto 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el Real Decreto 951/2015 de 23 de octubre.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Quinto. Que es voluntad de ambas partes reforzar y garantizar la seguridad tecnológica, así como la eficacia y la eficiencia de las Administraciones públicas, mediante el ahorro de costes y de racionalización de recursos.

Sexto. Que en el marco normativo de las relaciones entre administraciones públicas establecido por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector, los convenios se consideran un instrumento, de uso generalizado, que se ha acreditado como especialmente eficaz para la gestión de los recursos públicos desde la perspectiva de su aprovechamiento racional, la búsqueda de sinergias y la coordinación de esfuerzos, de lo que, en general, se sigue naturalmente una economía de medios.

Por todo lo anterior, bajo el principio de la colaboración mutua que debe presidir las relaciones entre las Administraciones públicas, reconociéndose ambas partes, en la representación que ostentan, el CNI-CCN y el CIT acuerdan suscribir el presente Convenio que se regirá por las siguientes

CLÁUSULAS

Primera. OBJETO DEL CONVENIO

El objeto del presente Convenio consiste en fijar los términos y el alcance de la colaboración entre el Cabildo Insular de Tenerife y el CNI-CCN, en materia de seguridad de los sistemas, servicios, y redes TIC de la Administración, que procesan, almacenan o transmiten información en formato electrónico, y que incluyen medios de cifra.

Dentro del ámbito subjetivo del presente Convenio se incluye con su firma a los Ayuntamientos de la Isla de Tenerife con una población inferior a 20.000 habitantes, en virtud del Reglamento del Servicio de Asistencia Técnica específica en materia de implantación de tecnología de la información, de las comunicaciones y en administración electrónica a los municipios de la Isla, aprobado en Pleno del CIT, de fecha 29 de junio de 2018.

Adicionalmente, el mencionado ámbito subjetivo se podrá extender, previo acuerdo de las partes y a través del procedimiento de adhesión previsto en la cláusula sexta de este Convenio, a los restantes Ayuntamientos de la Isla de Tenerife y/o entes del Sector Público dependiente del CIT, que se estimen oportunos. Recibirán la denominación de entidades adheridas, la totalidad de los entes incluidos en el ámbito subjetivo del presente Convenio.

Segunda. OBJETIVOS DE LA COLABORACIÓN

Las actuaciones de colaboración entre ambas partes son las siguientes:

- Actuaciones de intercambio de información técnica en materia de seguridad de los sistemas, servicios y redes en los siguientes campos:
  - Monitorización y acceso a la información recogida por los sensores ya desplegados, o a desplegar, en las entidades adheridas.
  - Información y/o documentación técnica en materia de seguridad: el CNI-CCN dará acceso a las series de guías CCN–STIC desarrolladas para la Administración con objeto de adaptación a los entornos de las entidades adheridas. En caso de su difusión en otros entornos, se deberá citar el origen del documento.
  - Incidentes de seguridad: información técnica y procedimientos de resolución de los mismos para su aplicación en los entornos de actuación del CNI-CCN (Sector Público) y en cualquiera de las entidades adheridas.

- Iniciativas de seguridad desarrolladas por las entidades adheridas y el CNI-CCN con objeto de mejorar la coordinación entre las mismas y, en la medida de lo posible, dar un mensaje común.
- Intercambio de formación y buenas prácticas en el ámbito de las entidades adheridas y el CNI-CCN.

– Actuaciones de promoción del desarrollo de herramientas de seguridad y programas específicos.

- Posibilidad de que las entidades adheridas promuevan el desarrollo y la utilización de herramientas de seguridad informática y productos o programas específicos a propuesta del CNI-CCN
- En este sentido, el CIT, y el resto de entidades adheridas, podrán realizar pruebas a dichas herramientas y programas que le permitan, llegado el caso, completar la funcionalidad de las mismas para utilizarlos en su ámbito de actuación.

– Actuaciones de implementación y funcionamiento de un Centro Virtual de Operaciones de Ciberseguridad (vSOC) que aumente de forma significativa las capacidades actuales de vigilancia y detección de amenazas en la operación diaria de los sistemas de información y comunicaciones de las entidades adheridas, así como la mejora de su capacidad de respuesta ante cualquier ataque.

- Por su naturaleza centralizada, el vSOC facilitará tanto la implantación de las herramientas y/o tecnologías más adecuadas en cada momento, como la adopción de las medidas oportunas para una defensa eficiente.
- La dirección y gestión del vSOC corresponderá al CIT, en el que el CCN-CERT, como CERT gubernamental nacional, actúa como prestador del servicio según las competencias del Real Decreto 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad, modificado por el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y bajo la supervisión de CIT.
- Se incluye en este apartado la realización de acciones de capacitación del personal de las entidades adheridas en aquellos aspectos en los que el CNI-CCN identifique carencias o necesidades de refuerzo.

En el Anexo del presente Convenio se listan las entidades adheridas inicialmente, y se detallan aquellas actuaciones de colaboración que requieren un mayor grado de concreción.

Tercera. FINANCIACIÓN Y FORMA DE PAGO

Cada parte realizará las actuaciones previstas en el presente Convenio con sus propios medios.

Los costes que se deriven de la ejecución del presente Convenio, con el alcance inicial indicado en el Anexo I, será financiado por el CIT, y los mismos tendrán el carácter de costes de compensación para resarcir los gastos al CNI-CCN que genera la actuación de colaboración consistente en la implementación y funcionamiento del Centro Virtual de Operaciones de Ciberseguridad (vSOC), para asumir la sostenibilidad funcional y técnica del mismo.

El resto de actuaciones que se lleven a cabo, no generarán coste para las respectivas partes. La financiación del presente Convenio se llevará a cabo por cada parte con cargo a sus propios presupuestos ordinarios de funcionamiento.

Así mismo, con el fin de facilitar la gestión, la aportación dineraria del CIT será ingresada por este Organismo en la cuenta corriente de titularidad del Ministerio de Defensa facilitada al efecto, que se indica a continuación:

TITULAR: CENTRO NACIONAL DE INTELIGENCIA
IBAN: ES18 0030 1316 4700 0172 6271
SWIFT: ESPCESMMXXX

En el momento que se haga la transferencia, para evitar demoras y agilizar el proceso, el CIT lo comunicará por correo electrónico (ccn@cni.es/ccn@ccn.cni.es) al CNI-CCN para conocimiento y seguimiento de la misma.

La aportación dineraria del CIT será transferida al CNI-CCN, la primera tras la firma del presente Convenio, y las sucesivas a los 12, 24 y 36 meses de la citada firma, una vez que haya sido aprobada la justificación en los términos de lo previsto en la presente cláusula. El importe de la transferencia de crédito de cada período para la actuación relativa al vSOC previsto en el presente Convenio es el siguiente:

- 2020: 127.000 €.
- 2021: 300.000 €.
- 2022: 210.000 €.
- 2023: 210.000 €.

El importe anual para una posible prórroga del Convenio será también de 210.000 €.

La justificación de las actuaciones del Convenio se realizará por períodos de doce (12) meses, de forma que una vez finalizado el período anterior a justificar, y en el plazo máximo de dos (2) meses, se deberá elaborar y presentar ante la Comisión de Seguimiento la siguiente documentación:

- El CIT y el CNI-CCN deberán elaborar y presentar una memoria de actuación justificativa del cumplimiento de los compromisos acordados, con indicación de las actuaciones realizadas y de los resultados obtenidos.
- El CNI-CCN deberá presentar, para las actuaciones vinculadas al vSOC, una memoria económica justificativa de los gastos derivados de la ejecución del Convenio. Asimismo, el CNI-CCN deberá presentar un certificado de su órgano competente que certifique que los gastos derivados del Convenio han sido aplicados al desarrollo de las acciones contempladas en el mismo.

Cuarta. MECANISMOS DE SEGUIMIENTO, VIGILANCIA Y CONTROL

Al objeto de impulsar las actuaciones previstas en este Convenio y garantizar su desarrollo integral, de acuerdo con lo establecido en el artículo 49.1.f de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, se crea una comisión de seguimiento, vigilancia y control del Convenio y de los

compromisos adquiridos por los firmantes, que ejercerá sus funciones de acuerdo con lo establecido en los artículos 51.2.c) y 52.3 de la citada Ley.

Esta Comisión estará compuesta por cinco (5) miembros: cuatro (4) con voz y voto, dos (2) de ellos nombrados por el CIT y los otros dos (2) designados por el Secretario General del CNI-CCN. El quinto miembro, que ostenta las funciones de secretario de la comisión, con voz, pero sin voto, será designado por el CIT. La Presidencia la ostentará uno de los representantes del CIT, con voto de calidad.

La comisión se reunirá de forma ordinaria, al menos, una vez al año, sin perjuicio de las reuniones extraordinarias que se convoquen. Para la adopción de acuerdos se exigirá que asistan a la reunión la mayoría de los miembros. Los acuerdos se tomarán por mayoría y quedarán debidamente reflejados en acta que será firmada por todos los asistentes.

Entre otras asumirá las siguientes funciones:

- Diseño, definición, delimitación, planificación y ejecución de las concretas actividades técnicas derivadas del objeto de las actuaciones de colaboración objeto del presente Convenio.
- Evaluación del estado de las infraestructuras TIC gestionadas por las entidades adheridas, en el ámbito dentro de su alcance, con el objetivo de consensuar la evolución de las mismas y adecuar las actuaciones objeto del Convenio a las infraestructuras tecnológicas existentes en cada momento.
- Comunicación y seguimiento de la ejecución de las actuaciones de colaboración.
- Acuerdos específicos que considere oportunos, que no impliquen modificación del Convenio, para la mejor realización del objeto de éste.
- Elaboración conjunta de un informe de conclusiones dentro del primer año de vigencia del presente Convenio.
- Propuesta para modificación del Convenio.
- Emisión de un informe técnico sobre controversias que puedan surgir entre las partes en relación con la ejecución, interpretación, modificación, efectos o resolución del presente Convenio.

Las cuestiones litigiosas o controversias que puedan surgir entre las partes en relación con la ejecución interpretación, modificación, resolución y efectos del presente Convenio, deberán solventarse por mutuo acuerdo de las partes en la Comisión de seguimiento, vigilancia y control.

En lo no previsto en el presente Convenio, y a falta de normas propias, la Comisión de Seguimiento se regirá por lo establecido, para los órganos colegiados, en la Sección 3ª del Capítulo II del Título Preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Las reuniones de la Comisión de Seguimiento podrán celebrarse por medios telemáticos.

Quinta. MODIFICACIÓN DEL CONVENIO

El presente Convenio podrá ser objeto de modificación por mutuo acuerdo de las partes, cuando resulte necesario para la mejor realización de su objeto, mediante la formalización de la correspondiente adenda.

La adenda será suscrita por el CIT y el CNI-CCN.

Asimismo mediante adenda se reflejará, en su caso, el nuevo régimen económico del Convenio, así como si alguna de las entidades adheridas, no previstas inicialmente, participa en la financiación y la cuantía, acordada por la Comisión de seguimiento, para la misma.

Sexta.- **SISTEMA DE ADHESIÓN**.

Aquellos Ayuntamientos de la isla de Tenerife de más de 20 mil habitantes, no previstos en el ámbito subjetivo inicial, y las Entidades del Sector Público pertenecientes al Cabildo Insular de Tenerife, que estuvieran interesadas en adherirse al presente Convenio, deberán formalizar su adhesión mediante el procedimiento descrito a continuación:

- Ayuntamientos de la isla de Tenerife de más de 20 mil habitantes.- La adhesión se llevará a cabo a través del procedimiento previsto en el artículo 9.5 del Reglamento del Servicio de la Asistencia Técnica específica en materia de implantación de tecnología de la información, de las comunicaciones y en administración electrónica, aprobado mediante Acuerdo Plenario de fecha 26 de octubre de 2018 y publicado en el Boletín Oficial de la Provincia de Santa Cruz de Tenerife, nº 138 de 16 de noviembre de 2018.
- Entidades del Sector Público dependiente del Cabildo Insular de Tenerife.- La adhesión se formalizará mediante la suscripción de un Acuerdo de adhesión, según modelo que figura en el Anexo II del presente Convenio., que irá acompañado de la certificación del acuerdo del órgano de gobierno correspondiente de la Entidad del Sector Público, por el que se adopta la decisión de solicitar adhesión al presente Convenio.

Para la incorporación de nuevas entidades, será necesario PREVIAMENTE:

- Revisar y acordar por la Comisión de Seguimiento, los posibles incrementos de costes derivados de la incorporación de cada entidad, así como, en su caso, la participación de las mismas en la financiación y cuantía de la misma.
- Tramitar el correspondiente procedimiento de adhesión con las entidades a incorporar, descrito anteriormente.

Séptima.- VIGENCIA, DURACIÓN Y PRÓRROGA

Tendrá una vigencia de cuatro (4) años desde la fecha de la firma, pudiendo ser prorrogado de forma expresa, por un nuevo período de hasta cuatro (4) años conforme a lo dispuesto en el artículo 49, letra h) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, mediante comunicación previa y por escrito de las partes dentro de los tres (3) meses anteriores a la finalización de su vigencia o de cualquiera de sus prórrogas.

Desde su firma por ambas partes, este Convenio se encontrará perfeccionado y será plenamente eficaz entre las partes y frente a terceros sin necesidad de ulteriores trámites, conforme a lo dispuesto en la normativa reseñada en la cláusula Décimo primera, que recoge el régimen jurídico específico de este Convenio.

Octava.- EXTINCIÓN

El presente Convenio se extinguirá según establece el Artículo 51.1 de la Ley 40/2015, de 1 de octubre, bien por el cumplimiento de las actuaciones que constituyen su objeto o por incurrir en causa de resolución. Sin perjuicio de lo indicado en el artículo 51 de Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, son causas de resolución del presente Convenio:

a) El transcurso del plazo de vigencia del Convenio sin haberse acordado la prórroga del mismo.

b) El acuerdo unánime de todos los firmantes.

c) El incumplimiento de las obligaciones y compromisos asumidos por parte de alguno de los firmantes. En este caso cualquiera de las partes notificará a la parte incumplidora un requerimiento para que cumpla en un determinado plazo con las obligaciones o compromisos que se consideran incumplidos.

   Este requerimiento será comunicado al responsable del mecanismo de seguimiento, vigilancia y control de la ejecución del Convenio y a las demás partes firmantes. Si transcurrido el plazo indicado en el requerimiento persistiera el incumplimiento, la parte que lo dirigió notificará a las partes firmantes la concurrencia de la causa de resolución y se entenderá resuelto el Convenio.

   La resolución del Convenio por esta causa podrá conllevar la indemnización de los perjuicios causados.

d) Por decisión judicial declaratoria de la nulidad del Convenio.

e) Por declaración de situación de interés para la seguridad nacional del artículo 24 de la Ley 36/2015, de 28 de septiembre, de seguridad nacional, si su alcance afectase al objeto del presente Convenio.

f) Por cualquier otra causa distinta de las anteriores prevista en otras leyes.

Novena.- CONFIDENCIALIDAD DE LA INFORMACIÓN Y PROTECCIÓN DE DATOS

Las Partes se comprometen a guardar absoluta confidencialidad sobre la existencia y el contenido de este Convenio. Igualmente, a causa de la ejecución de las funciones contenidas en este Convenio, es probable que se llegue a tener acceso directo o indirecto con medios, procedimientos o informaci6n relativas o pertenecientes al Centro Nacional de Inteligencia y, por tanto, clasificada por el ordenamiento jurídico español vigente con el grado de SECRETO.

Las Partes manifiestan conocer los deberes y obligaciones asociados a dichas materias, y en concreto el especialmente grave de reserva, conforme a lo establecido en la Ley 9/1968, de 5 de abril, sobre secretos oficiales; en su reglamento, aprobado mediante el Decreto 242/1969, de 20 de febrero, y en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. Esta obligación de confidencialidad y reserva afecta a toda la información clasificada a la que se tenga acceso, con independencia del momento, medio o lugar, y se mantendrá vigente de manera permanente e indefinida, con independencia de la eventual finalización del presente Convenio y de los accesos (o la causa de los accesos) a la información clasificada.

Décima.- CESIÓN DE COMPETENCIAS

El presente Convenio no supone, en ningún caso, la cesión de competencias de una de las partes a la otra, ni tampoco la concesión, expresa o implícita, de derecho alguno respecto a patentes, derechos de autor o cualquier otro derecho de propiedad intelectual o industrial.

Décimo primera.- RÉGIMEN JURÍDICO ESPECÍFICO DEL CONVENIO

Siendo parte de este Convenio el Centro Nacional de Inteligencia, es de aplicación el régimen jurídico específico que se establece en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público en la Disposición adicional decimoctava.

En virtud de dicho precepto, la tramitación administrativa de un Convenio que, como el presente, y en consonancia con el artículo 5.1 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, contenga datos que puedan conducir al conocimiento de la organización, estructura interna, medios, personal, instalaciones del Centro Nacional de Inteligencia y todo lo que pueda conllevar al conocimiento de lo anterior, constituyen información clasificada, con el grado de SECRETO.

Al mismo tiempo es obligación del Centro Nacional de Inteligencia, conforme al Artículo 4.f) de esa misma Ley "velar por el cumplimiento de la normativa relativa a la protección de la información clasificada". Simultáneamente, la Ley 9/1968, de 5 de abril, sobre secretos oficiales, Artículo 8.a), señala: "Solamente podrán tener conocimiento de las «materias clasificadas» los órganos y las personas debidamente facultadas para ello y con las formalidades y limitaciones que en cada caso se determinen".

En virtud de lo expuesto, en el ámbito del presente Convenio, ambas partes se abstendrán de realizar cualquier trámite encaminado a la autorización, registro o publicidad del Convenio en virtud del régimen común de convenios administrativos contemplado en el Capítulo VI del Título preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, evitando, entre otros los dirigidos a:

1. Recabar la autorización previa del Ministerio de Hacienda y Administraciones Públicas para su firma, modificación, prórroga y resolución, Artículo 50.2.c de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
2. Publicar el Convenio en el BOE u otro Boletín Oficial, Artículo 48.8 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
3. Enviar el Convenio al Registro Electrónico estatal de Órganos e Instrumentos de Cooperación del sector público estatal en el Registro de Convenios. Artículo 48.8 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
4. Remitir al Tribunal de Cuentas en los de más de 600.000 euros. Artículo 53 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público

Décimo segunda.- RÉGIMEN DE TRANSPARENCIA

De acuerdo con lo dispuesto en el artículo 5.1 de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia y al Artículo 8.a) de la ley 9/1968, de 5 de abril, sobre secretos oficiales, es de aplicación lo previsto en la Disposición adicional primera, apartado 2 de la Ley 19/2013, de 9 de

diciembre, de transparencia, acceso a la información pública y buen gobierno en la que se prevé que "se regirán por su normativa específica, y por esta Ley con carácter supletorio, aquellas materias que tengan previsto un régimen jurídico específico de acceso a la información", siendo aplicable a este instrumento lo previsto en el artículo 14.1.a) de esa misma norma.

Décimo tercera. JURISDICCIÓN

Las cuestiones litigiosas o controversias que puedan surgir entre las partes en relación con la ejecución, interpretación, modificación, efectos o resolución del presente Convenio, de no existir el mutuo acuerdo de la Comisión de seguimiento, serán de conocimiento y competencia del orden jurisdiccional de lo Contencioso-Administrativo, de conformidad con la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

Y, de conformidad con cuanto antecede, en el ejercicio de las facultades que legalmente corresponden a cada uno de los firmantes, obligando con ello a las Instituciones que representan, suscriben el presente Convenio.

EL PRESIDENTE DEL CABILDO INSULAR DE TENERIFE	LA SECRETARIA DE ESTADO DIRECTORA DEL CNI-CCN
Don Pedro Manuel Martín Domínguez	Doña Paz Esteban López

ANEXO I

DETALLE DE LAS ACTUACIONES DE COLABORACIÓN

Las actuaciones que se relacionan a continuación recaen sobre el objeto del presente Convenio y son las necesarias para la consecución de su finalidad, sin perjuicio de que a lo largo de la vigencia del Convenio se identifiquen nuevas actuaciones de colaboración necesarias para el buen fin del Convenio.

ALCANCE

En el ámbito subjetivo del presente Convenio de colaboración se integran inicialmente, y para todas las actuaciones previstas, las siguientes entidades adheridas:

- Cabildo Insular de Tenerife.
- Ayuntamientos de la Isla de Tenerife de menos de 20.000 habitantes (ordenados de menor a mayor población empadronada según datos del INE 2019):
  - 38052 Vilaflor de Chasna
  - 38044 Tanque, El
  - 38012 Fasnia
  - 38042 Silos, Los
  - 38010 Buenavista del Norte
  - 38034 San Juan de la Rambla
  - 38015 Garachico
  - 38018 Guancha, La
  - 38004 Arafo
  - 38005 Arico
  - 38041 Sauzal, El
  - 38025 Matanza de Acentejo, La
  - 38051 Victoria de Acentejo, La
  - 38040 Santiago del Teide
  - 38046 Tegueste
  - 38039 Santa Úrsula
  - 38032 Rosario, El

A través del procedimiento de adhesión establecido, se podrá ampliar este ámbito subjetivo a otros Ayuntamientos de la Isla de Tenerife, y/o entidades del Sector Público dependiente del CIT.

Centro Virtual de Operaciones de Ciberseguridad (vSOC)

Mediante este Convenio de colaboración se debe implantar y mantener el funcionamiento de un Centro Virtual de Operaciones de Ciberseguridad (vSOC) con cobertura sobre los servicios y usuarios de las entidades adheridas. La implantación se realizará en tres (3) fases diferenciadas (establecidas para los entes incluidos en el alcance inicial del convenio y que habría que adaptar en el supuesto de incorporación de nuevas entidades):

- Arranque (Año 1): Implantación en los 5 ayuntamientos de menor población y el CIT.
- Despliegue (Año 2): Implantación en los 12 ayuntamientos restantes (y soporte de todo lo anterior).
- Permanente (Año 3 y siguientes): Explotación del vSOC en 17 ayuntamientos + CIT.

El alcance del acuerdo de colaboración incluye la gestión y seguimiento de la implantación y funcionamiento del vSOC mediante el que se mejorarán las capacidades de vigilancia y detección de incidentes en los sistemas del CIT y las restantes entidades adheridas, y se optimizará la capacidad de reacción y respuesta ante cualquier ataque, de conformidad con los criterios e información suministrada por las mismas.

De igual manera, el CNI-CCN asumirá la gestión técnica operativa del equipo de técnicos expertos necesarios para cumplir con el alcance del Convenio, para la que el CNI-CCN designará uno o varios responsables técnicos. Estos realizarán la interlocución técnica con los interlocutores expresamente designados por el CIT para la dirección operativa, al nivel de profundidad requerido por los mismos. Será necesaria, por tanto, dedicación a tiempo completo de al menos un coordinador técnico de proyecto por parte del CNI-CCN.

El CIT y/o las entidades adheridas que así lo determinen, podrán poner a disposición e incorporar temporalmente, al funcionamiento y operación del vSOC, y como máximo dos (2) recursos a la vez, al personal propio que estimen oportuno, con el objetivo de participar y colaborar en la operación, además de promover la formación, especialización y experiencia en ciberseguridad de su personal técnico.

REQUISITOS Y CARACTERÍSTICAS TÉCNICAS DEL vSOC

Las actuaciones previstas, así como los sistemas de información que los sustentan, deberán prestarse de conformidad a los requisitos de seguridad establecidos en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y al Real Decreto 3/2010, de 8 de enero por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y sus normas de desarrollo.

El CNI-CCN proporcionará:

- El equipamiento necesario para la prestación del servicio, pudiendo reutilizar el actual si lo considera oportuno, en este sentido el CIT, pone a disposición del vSOC para sí mismo y las entidades adheridas inicialmente, los elementos de infraestructura indicados en el apartado de descripción de servicios de seguridad requeridos que puedan ser reutilizados.

– El CIT pondrá a disposición del vSOC un espacio físico, para la ubicación del mismo en la Isla de Tenerife, con capacidad para equipar hasta un máximo de cuatro (4) puestos de operador. El espacio incluirá el suministro eléctrico y el acceso a Internet.

– El personal técnico especializado (personal del vSOC) realizará toda la gestión operativa, el soporte a usuarios y las labores que requieren mayor nivel de conocimiento en "inteligencia de ciberseguridad", es decir, las relacionadas con detección proactiva, investigación y tratamiento de incidentes de seguridad, incluyendo entre los mismos los reportados por el servicio del SAT-INET del CCN-CERT y los del servicio antiDDoS, con la evaluación de peligrosidad de las excepciones solicitadas por los usuarios, con el tratamiento de malware, etc.

Gestión operativa y configuración del entorno de seguridad perimetral

Se dispondrá durante todo el período de vigencia del Convenio, de los recursos técnicos, humanos y materiales necesarios y adecuados para la prestación de los servicios de soporte y asistencia técnica, mantenimiento, gestión de incidencias y resolución de problemas. El número de usuarios es aproximadamente de unos 3.000 incluyendo los de todas las entidades adheridas inicialmente.

Se realizará la gestión de los eventos e incidentes de seguridad para evitar o minimizar su impacto. Se monitorizará de manera continua el funcionamiento de los servicios de seguridad desplegados, así como todos los elementos que componen la plataforma de seguridad para asegurar la detección temprana de cualquier incidente de seguridad, indisponibilidad, vulnerabilidad, incumplimiento de las políticas de seguridad, etc., que afecte a cualquiera de ellos.

Será responsabilidad del CNI-CCN la gestión de la infraestructura que incorpore al Convenio y que sea necesaria para la prestación del servicio, control de versiones y configuraciones, así como la gestión de la reparación de las averías que pudiesen surgir. De igual forma, será responsabilidad del CIT la parte correspondiente a la infraestructura que ponga a disposición del Convenio.

Habrá de informar, con al menos cinco (5) días laborables de antelación, de las paradas programadas del servicio y contar con la aprobación de los directores técnicos del CIT para sustituir, actualizar y reconfigurar equipos y sistemas obsoletos, averiados o inadecuadamente configurados. Cualquier parada programada en los servicios deberá planificarse para causar la mínima indisponibilidad, y deberán producirse en horario de mínimo impacto para el servicio (mínima demanda, mínima criticidad del tráfico cursado y demás métricas relativas al impacto).

El personal técnico al cargo de la gestión operativa de la plataforma deberá contar con certificaciones y amplia experiencia en las tecnologías utilizadas en los equipos. Se requiere estabilidad del personal dedicado al proyecto que preste el servicio con el suficiente nivel de satisfacción.

El horario de atención a usuarios para incidencias o incidentes no críticos es de 8h a 18:30h, durante los días laborables. En todo caso deberá garantizarse la prestación de este servicio durante todo el año incluyendo períodos vacacionales o de asistencia del personal a actividades de formación. De igual manera, se deberá contar con personal técnico cualificado para intervenciones fuera del horario laboral habitual.

Se utilizará la herramienta de gestión de incidencias proporcionada por el CIT para la atención de incidencias de usuarios, mientras que para el caso de incidentes de seguridad podrá utilizarse otra herramienta (LUCIA, etc.).

Deberán presentarse al menos los siguientes informes periódicos:

- El estado de los diversos elementos de seguridad y las tareas realizadas sobre cada uno de ellos durante ese período. Se incluirá en estos informes estadísticas de uso de las plataformas (principales sitios visitados en navegación, "top ten" de consumo de ancho de banda por servicios y por usuarios, etc.).
- Incidentes o eventos de seguridad detectados, bien por el personal al cargo de la gestión operativa en su búsqueda proactiva, o por las distintas sondas de detección de intrusiones o por el elemento correlador de eventos.
- Peticiones tramitadas y cerradas. Se detallarán todas las peticiones tanto de provisión como de administración cerradas en el mes objeto del informe, indicando la fecha y hora de apertura, la fecha y hora de fin, los trabajos realizados y en caso de retraso en su tramitación las causas del mismo.
- Elaboración de informes de incidentes de seguridad de nivel de criticidad CRÍTICO, MUY ALTO o ALTO y su entrega a las Entidades en los plazos establecidos.

Mantenimiento y soporte del hardware y del software

Será responsabilidad del CNI-CCN la gestión de las incidencias y averías de los equipos que integren el servicio. La corrección y reparación de las averías pueden implicar la sustitución de equipos, desplazamiento del personal, mano de obra, etc.

De igual forma, será responsabilidad del CIT la parte correspondiente a la infraestructura que ponga a disposición del Convenio.

DESCRIPCIÓN DE SERVICIOS DE SEGURIDAD REQUERIDOS

Deberán realizarse como mínimo las siguientes actuaciones (equivalentes a las mismas) dentro del vSOC:

- Protección mediante cortafuegos de distintos fabricantes.
- Sistemas de detección (IDS) y prevención (IPS) de intrusiones.
- Servicio de protección de punto final (EDR).
- Servicio gestionado de correlación de eventos (SIEM).
- Elementos de monitorización de servicios.
- Herramientas de hacking ético.

El CIT pondrá a disposición del vSOC, para sí mismo, y/o para las entidades adheridas en las que sea viable y eficiente su reutilización para todas las partes, los siguientes elementos, siempre que el CNI-CCN estime conveniente su uso:

- Sistema cortafuegos corporativo en alta disponibilidad.
- Sistemas de detección (IDS) y prevención (IPS) de intrusiones, asociado al cortafuegos corporativo.

- Servicio de protección de punto final (EPP) (para sus propios usuarios).
- Elementos de monitorización de servicios.

PRODUCTOS, PROCEDIMIENTOS Y DOCUMENTACIÓN QUE EL CIT/ENTIDADES ADHERIDAS ENTREGARÁN AL CNI-CCN

El CIT y/o las entidades adheridas, procederán en virtud de este Convenio la entrega al CNI-CCN de la documentación y/o procedimientos que este pueda requerir para la puesta en marcha del vSOC, tales como inventarios, esquemas y documentación sobre la arquitectura, informes o cualquier otra documentación requerida expresamente por el CNI-CCN.

INDICADORES Y NIVELES DE SERVICIO

En la primera comisión de seguimiento del Convenio, con el objeto de ver la evolución de los servicios operados en el marco del Convenio se definirá un conjunto de indicadores, así como los niveles de servicio esperados, que serán revisados en todas las futuras comisiones de seguimiento en las que se podrá introducir indicadores adicionales, o revisar para su eliminación aquellos que hayan perdido sentido.

SERVICIOS AÑADIDOS POR EL CNI-CCN

Dada la experiencia del CNI-CCN en el campo de la ciberseguridad ofrece a la ejecución del Convenio varios puntos adicionales para mejorar y dotar un mayor nivel de seguridad.

Las siguientes tareas son realizadas conforme a la idea del SOC de la AGE y se propone su materialización en el presente Convenio:

- Establecimiento del nivel de seguridad y estado de las infraestructuras de sistemas y red.
- Correlación, prevención y monitorización de los registros del organismo para prevenir ataques y exfiltración de información.
- Incorporación de puntos finales para evaluar la seguridad de equipos, controlar acciones mal intencionadas y protección contra malware.

El CNI-CCN considera tener un conocimiento del estado de la red y de las infraestructuras de los sistemas de información como un factor clave en el desarrollo del Convenio.

Según el resultado del estado de seguridad se pueden conocer puntos débiles o lugares donde focalizar o reforzar los niveles de seguridad. Se plantea que el inicio de estado de seguridad sea una acción continua y con la ampliación a los desarrollos de los organismos y aplicativos, en el actual Convenio será una evaluación del estado de la seguridad.

Con la información del estado de la seguridad, se establecerán las fuentes principales generadoras de registros de seguridad. Toda fuente de seguridad se incorporará al SIEM gestionado por los operadores del CNI-CCN para obtener información de ciberseguridad. Los registros de ciberseguridad del organismo dan un valor añadido para detectar anomalías en la red, ataques al organismo y controlar el estado de seguridad del organismo. Para realizar las anteriores tareas, el SIEM debe

automatizar muchas acciones dando a los operadores la información precisa y poder hacer investigaciones de seguridad de valor para el organismo.

El último punto es la incorporación de sistemas de protección de los equipos finales. Los equipos finales son los objetivos de los ataques actuales y la principal fuente de exfiltración de información por acciones mal intencionados o códigos maliciosos. La instalación de la protección de puntos finales dota de una protección muy exhaustiva de los equipos además de ampliar la correlación y eficiencia del SIEM que se instalará en el organismo

ANEXO II

ACUERDO DE ADHESIÓN

D./Dña. (nombre y cargo……, en representación de (Entidad Sector Público)……..

DECLARA

Que el Cabildo Insular de Tenerife y el Centro Criptológico Nacional del Centro Nacional de Inteligencia han suscrito con fecha……un Convenio de colaboración en materia de ciberseguridad que tiene por objeto fijar los términos y el alcance de la colaboración entre el Cabildo Insular de Tenerife y el CNI-CCN, en materia de seguridad de los sistemas, servicios, y redes TIC de la Administración, que procesan, almacenan o transmiten información en formato electrónico, y que incluyen medios de cifra.

Que el Convenio de colaboración suscrito incluye, inicialmente, al Cabildo Insular de Tenerife y a los Ayuntamientos de la isla de Tenerife con una población inferior a 20.000 habitantes.

Que en el Convenio, está previsto en su cláusula PRIMERA la posibilidad de extender el ámbito subjetivo a los restantes Ayuntamientos de la isla de Tenerife y/o entes del Sector Público Insular dependientes del Cabildo Insular de Tenerife, conforme al procedimiento de adhesión previsto en la cláusula SEXTA del Convenio.

Que reunida la Comisión de seguimiento del citado Convenio, en los términos expuestos en la cláusula SEXTA del mismo, se ha acordado respecto a la financiación lo siguiente: (……..)

Que el (órgano competente) de (Entidad Sector Público), ha acordado con fecha……solicitar la adhesión al Convenio de fecha……., suscrito entre el Cabildo Insular de Tenerife y el Centro Criptológico Nacional del Centro Nacional de Inteligencia, en materia de ciberseguridad.

MANIFIESTA

La voluntad de (Entidad Sector Público)……,cuya representación ostenta, de adherirse expresamente a todas y cada una de las cláusulas del Convenio mencionado, asumiendo las obligaciones derivadas del mismo y con sujeción a todas sus cláusulas.

A tal efecto se adjunta el acuerdo del órgano de gobierno de fecha.....

Lugar, fecha y firma