



CONVENIO DE COOPERACIÓN ENTRE LA ADMINISTRACIÓN PÚBLICA DE LA COMUNIDAD AUTÓNOMA DE CANARIAS, A TRAVÉS DE LA PRESIDENCIA DEL GOBIERNO, Y EL AYUNTAMIENTO DE AGÜIMES, PARA LA PRESTACIÓN DE UN SERVICIO DE RESPUESTA ANTE INCIDENTES DE CIBERSEGURIDAD.

REUNIDOS

De una parte, el Ilmo. Sr. D. Alfonso Cabello Mesa, Viceconsejero de la Presidencia, según nombramiento efectuado mediante Decreto 134/2023, de 17 de julio (BOC n.º 141, de 18.7.2023), con facultades para suscribir el presente Convenio en representación de la Administración Pública de la Comunidad Autónoma de Canarias, según delegación efectuada por el Presidente en virtud del Decreto 159/2019, de 30 de agosto, del Presidente, por el que se delegan competencias en materia de convenios de colaboración y de subvenciones (BOC n.º 172, de 6.9.

De otra, D. ÓSCAR HERNÁNDEZ SUÁRES, Alcalde del Ayuntamiento de AGÜIMES (en adelante “el ayuntamiento”)

Reconociéndose ambas partes capacidad legal suficiente, convienen suscribir el presente Convenio de cooperación y a tal efecto

EXPONEN

I.- La Presidencia del Gobierno es el departamento de la Administración Pública de la Comunidad Autónoma de Canarias que ostenta las competencias en materia de ciberseguridad y seguridad de las telecomunicaciones y la comunicación, de conformidad con lo establecido en el Decreto 6/2024, de 25 de enero, del Presidente, por el que se aprueba el Reglamento Orgánico de la Presidencia del Gobierno (BOC n.º 26, de 5.02.2024).

II.- El Gobierno de Canarias, a través de la Viceconsejería de la Presidencia, ha implantado un Equipo de Respuesta a Incidentes de Seguridad Informática (en adelante, CSIRT-CAN), cuya finalidad es la de coordinar y respaldar la respuesta a un evento o incidente de seguridad informática.

III.- La conformación de CSIRT-CAN está alineada con el Esquema Nacional de Seguridad (que prevé que las Administraciones públicas puedan desarrollar sus propias capacidades de respuesta a incidentes, bajo la coordinación del CCN), y con el Real Decreto 43/2021, de 26 de enero por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (que fija entre otros el marco estratégico e institucional de seguridad de las redes y sistemas de información y la gestión de incidentes de seguridad), alineándose con otras comunidades autónomas que ya cuentan con servicios semejantes, como Valencia con *CSIRT-CV*, Cataluña con *CESICAT-CERT*, Andalucía con *AndalucíaCERT*, el País Vasco con Centro Vasco de Ciberseguridad, Galicia con *CSIRT.gal*, Murcia con *CSIRT-CARM*.

IV.- Este CSIRT-CAN dota al Gobierno de Canarias de la asistencia necesaria y adecuada para aumentar la capacidad de prevención, vigilancia y detección de amenazas en los sistemas de información y comunicaciones corporativos de la Administración Pública de la Comunidad Autónoma de Canarias, apoyando, dando soporte y aumentando las capacidades actuales de vigilancia y respuesta en materia de ciberseguridad, en actuación conjunta y coordinada con el Centro de Operaciones de Seguridad (SOC) Corporativo, el cual mantiene la operación de seguridad sobre sistemas de información y redes corporativas del Gobierno de Canarias. Además, CSIRT-CAN ofrece un servicio de respuesta rápida a las Entidades Locales (EELL) canarias que se adhieran y completen la integración técnica necesaria, concretándose en las siguientes acciones:

- Despliegue de sondas que permitan detectar las situaciones de riesgo lo antes posible, en aquellas EELL en que se considere necesario.
- Preparación, formación y concienciación al personal público interno y externo para integrar la ciberseguridad en la cultura corporativa.
- Asesoramiento para el cumplimiento del ENS (Esquema Nacional de Seguridad).

Con esta actuación se dota de un sistema reforzado de Ciberseguridad integral y coordinado entre todas las Administraciones Públicas Canarias.

V.- El proyecto CSIRT-CAN se ha financiado con cargo al mecanismo de Recuperación y Resiliencia (MRR); siendo financiero íntegramente por la Unión Europea – Next Generation EU.

VI.- La Dirección General de Transformación Digital de los Servicios Públicos (DGTDSP), es el órgano encargado de la supervisión, control y especificación de la provisión del servicio prestado por el CSIRT-CAN, así como de su control organizativo, en virtud de las competencias que, en materia de ciberseguridad y seguridad en el ámbito de las telecomunicaciones y tecnologías de la información, le atribuye el artículo 28 del Reglamento Orgánico de la Presidencia del Gobierno, aprobado por Decreto del Presidente 6/2024, de 25 de enero.

VII. Conforme establece el artículo 70.bis.3) de la citada ley 7/1985, las Entidades Locales y, especialmente, los municipios, deberán impulsar la utilización interactiva de las tecnologías de la información y la comunicación para facilitar la participación y la comunicación con los vecinos, para la presentación de documentos y para la realización de trámites administrativos.

Ello implica que se deban implantar mecanismos y procedimientos de prevención, vigilancia y detección de amenazas en sus sistemas de información y comunicaciones. El CSIRT-CAN asistirá en la consecución de estos objetivos.

VIII. Ambas partes consideran de gran utilidad la provisión del servicio prestado por el CSIRT-CAN, al ayuntamiento, lo que contribuirá ineludiblemente a una mejora de las capacidades actuales de vigilancia y respuesta en materia de ciberseguridad.

Por lo expuesto, las Partes acuerdan suscribir el presente convenio que se regirá por las siguientes

CLÁUSULAS

Primera.- Objeto del Convenio.

1. El presente Convenio tiene por objeto articular la cooperación entre la Administración pública de la Comunidad Autónoma de Canarias (en adelante, APCAC), a través de la Presidencia del Gobierno, y el ayuntamiento para establecer las condiciones para la prestación y puesta a disposición de los servicios de Ciberseguridad avanzados de la Administración Pública de la Comunidad Autónoma de Canarias (en adelante CSIRT-CAN), en los ayuntamientos de canarias que se adhieran al presente Convenio.

En particular el objeto de la colaboración se concreta en los siguientes puntos:

- 1) Puesta a disposición del ayuntamiento de los diversos servicios de seguridad (servicios reactivos, servicios preventivos, de formación y concienciación) del CSIRT-CAN.
- 2) Establecimiento de un marco de colaboración para la solicitud por parte del ayuntamiento de los servicios de seguridad en el CSIRT-CAN y su prestación.
- 3) La relación de servicios puestos a disposición del ayuntamiento por parte del CSIRT-CAN se detallan en el Anexo I del presente Convenio. En cualquier caso, cada ayuntamiento que se adhiera podrá suscribirse a los servicios que considere.
- 4) El ayuntamiento podrá modificar, por escrito, la lista de servicios a los que desea estar suscritos de la relación de los servicios ofertados por el CSIRT-CAN.

El acceso, gestión y control de autorizaciones de los usuarios finales del ayuntamiento a los servicios objeto de este Convenio se efectuarán mediante la web del CSIRT-CAN y sus sistemas de autenticación. Ambas partes realizarán los trabajos que sean necesarios en sus plataformas tecnológicas para alcanzar este objetivo lo antes posible, garantizando el nivel de seguridad en dicho acceso que en cada caso proceda.

2. El CSIRT-CAN será puesto a disposición del ayuntamiento a través de la Dirección General de Transformación Digital de los Servicios Públicos (en adelante DGTDSP), de Presidencia de Gobierno.

Segunda.- Condiciones para la puesta a disposición del CSIRT-CAN.

1. Las condiciones para la puesta a disposición del CSIRT-CAN del ayuntamiento se establece en el presente Convenio y en sus anexos. Todo ello sin perjuicio de los acuerdos que en el desarrollo de éste se recojan en las actas de la Comisión de Seguimiento, o en las actas de las Subcomisiones de Seguimiento, que pudieran crearse.

Las actas formarán parte integrante de la relación entre ambas partes.

Tercera.- Compromisos de la APCAC, a través de la Presidencia del Gobierno.

La APCAC, a través de la Presidencia del Gobierno, y mediante la Dirección General de Transformación Digital de los Servicios Públicos como responsable del CSIRT-CAN, se compromete con el ayuntamiento a:

1. Poner a su disposición, a petición y de acuerdo con el tamaño del municipio, en función del número de habitantes como se recoge en el Anexo II, todos los medios técnicos, personales y de gestión necesarios para la correcta prestación de servicios de seguridad de entre los detallados en el presente convenio y recogidos en el Anexo I.

2. Esta puesta a disposición de medios será establecida para atender a la prestación de los servicios acordados entre ambas partes en cada momento y recogidos en el Anexo I. Adicionalmente se incluye la cesión a la entidad local del Paquete de Ciberseguridad detallado en el Anexo II a fin de reforzar sus sistemas de Ciberseguridad.

3. Se establecerá un plan de comunicación y difusión del CSIRT-CAN y formación a través de plataforma WEB del portal CSIRT-CAN para contribuir a las tareas de concienciación en la materia de seguridad TIC en el ámbito de la administración municipal. En los citados planes de difusión y formación, incluidos en los anexos III y IV, se establecerán los calendarios y jornadas adecuadas para dar cobertura a nivel local deseado de acuerdo con las peticiones de los destinatarios. En estas acciones ambas partes podrán colaborar con otras administraciones públicas o instituciones para facilitar la capilaridad de las jornadas así como facilitar su organización.

4. El CSIRT-CAN prestará los servicios de seguridad de acuerdo con los estándares profesionales vigentes en la materia y, en todo caso, de acuerdo con las condiciones técnicas establecidas en el Anexo I y II del presente Convenio y se obliga a gestionar y obtener, a su cargo, todas las licencias, permisos y autorizaciones que pudieran ser necesarias para la puesta a disposición de los servicios de acuerdo con el presente convenio.

Cuarta.- Compromisos del ayuntamiento.

1. El ayuntamiento se compromete a:

- a) Poner a disposición del CSIRT-CAN los medios técnicos y personal necesarios para organizar y coordinar la realización de las actividades y la prestación de los servicios objeto de este Convenio en la administración local.
- b) Nombrar a dos Responsables Técnicos para la interlocución diaria con el CSIRT-CAN, debiendo comunicar la variación de los mismos en el momento en que se produzca.
- c) Ceder un espacio con las condiciones físico-técnicas adecuadas para la ubicación de equipamiento que se cede por parte del Gobierno de Canarias para la prestación de los servicios de Ciberseguridad.
- d) Los suministros básicos, electricidad, condiciones ambientales y servicios de telecomunicaciones, vinculados a las instalaciones donde se ubique el equipamiento hardware, será por cuenta de la administración local.
- e) Comunicar cualquier petición, reclamación o necesidad de servicios de seguridad para darle la respuesta adecuada mediante los servicios y medios puestos a disposición por parte del CSIRT-CAN.
- f) Gestionar y obtener, a su cargo, todas las licencias, permisos y autorizaciones que pudieran ser necesarias para la prestación de los servicios del CSIRT-CAN.

- g) Participar de forma activa tanto internamente como externamente en todas aquellas acciones orientadas a la comunicación, difusión, concienciación y formación incluidos en el anexo III y IV.
- h) Publicar en el Boletín Oficial de la Provincia el presente convenio.
- i) Registrar un tratamiento de datos personales responsabilidad de la entidad local para la prestación de los servicios del CSIRT-CAN, con la finalidad de dar cumplimiento a la normativa en materia de protección de datos personales.

Quinta.- Comisión de Seguimiento.

1. Para la gestión, seguimiento y control del presente Convenio, se constituye una Comisión de Seguimiento, como órgano mixto de composición paritaria, compuesta por cuatro miembros, con voz y voto, dos representando a la Administración Pública de la Comunidad Autónoma de Canarias y dos del ayuntamiento.

Su régimen de funcionamiento y convocatorias será el previsto en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, para los órganos colegiados, si bien sus acuerdos serán adoptados por mayoría de ambas representaciones.

2. La Comisión de Seguimiento estará conformada:

2.1. Por parte de la Administración pública de la Comunidad Autónoma de Canarias:

- a) La persona titular de la Dirección General de Transformación Digital de los Servicios Públicos.
- b) La persona responsable del Área de Seguridad de los Sistemas de Información de la Dirección General de Transformación Digital de los Servicios Públicos.

Los miembros de la Comisión podrán estar asistidos por el personal técnico o jurídico que consideren adecuado para optimizar el desempeño de sus funciones.

3. La Comisión se reunirá como mínimo una vez al año, o bien cuando lo solicite alguna de las partes, para supervisar el desarrollo del marco de colaboración establecido, valorar los resultados obtenidos e identificar nuevas propuestas de actuación y colaboración.

4. Corresponde a la Comisión las funciones siguientes:

- a) La modificación y actualización de los Anexos.
- b) La resolución, de manera consensuada, de las controversias que puedan plantearse sobre la interpretación, aplicación, modificación, resolución y efectos del presente Convenio.
- c) Cuantas otras se deriven del presente Convenio.

Sexta.- Subcomisiones de Seguimiento.

1. Para la puesta a disposición del CSIRT-CAN en los ayuntamientos adheridos, se crearán

Subcomisiones de Seguimiento compuestas por cuatro personas, dos representando a la APCAC y dos al ayuntamiento.

Las personas en representación de la APCAC serán designadas por la persona titular de la Dirección General de Transformación Digital. Las personas en representación del ayuntamiento serán designadas por la persona titular de la Alcaldía o la persona titular de la Concejalía en quién delegue.

3. Estas Subcomisiones se reunirá al menos una vez al mes, durante la fase de despliegue de los equipos que se ceden, y después al menos una vez al año durante la vigencia del convenio para supervisar el despliegue del CSIRT-CAN en el ayuntamiento. Sus acuerdos y propuestas serán elevados a la Comisión de Seguimiento a los efectos de su valorar e identificación de nuevas propuestas de actuación y colaboración.

3. Corresponde a las Subcomisiones de Seguimiento las siguientes funciones:

a) Designar al personal técnico responsable de la implantación de los equipos y del software, así como, de la configuración y puesta en explotación.

b) Realizar el seguimiento de la implantación del equipamiento y de las aplicaciones cedidas y de las modificaciones y mejoras que puedan ser realizadas será el ayuntamiento.

Séptima.- Titularidad de los equipos y software del CSIRT-CAN.

El ayuntamiento, su personal, representantes o personas licenciatarias no tendrán que, a menos que dispongan de una autorización por escrito por parte del CSIRT-CAN:

- Abrir, retirar, modificar o, de otra forma, disponer del hardware.
- Interconectar, interceptar o de cualquier otra forma interferir con cualquier equipo empleado por el CSIRT-CAN para la prestación de servicios.
- Intentar ejecutar pedidos o otras acciones para ganar acceso a los equipos, hardware o software del CSIRT-CAN.

Cualquier información, datos, software o elementos que se encuentren en el hardware o infraestructura del CSIRT-CAN, incluyendo discos, memorias, así como el contenido de los mismos, son y permanecerán propiedad del CSIRT-CAN. La corporación local no podrá, ni permitirá a ningún tercero bajo ninguna circunstancia, leer, copiar, borrar o cualquier otra forma de disponer o alterar la mencionada información, contenidos o datos. Tampoco podrá ni permitirá a ningún tercero bajo ninguna circunstancia copiar, realizar ingeniería inversa, compilar o decompilar la información, datos, software o cualesquiera otros elementos de los equipos del CSIRT-CAN.

A la finalización del período de garantía, 31 de diciembre de 2027, los equipos y el software pasarán a ser propiedad de la corporación local en el que se encuentren emplazados.

Octava.- Obligaciones y compromisos económicos para las partes.

El presente Convenio de Cooperación no supone incremento del gasto público ni para la Administración Pública de la Comunidad Autónoma de Canarias ni para el ayuntamiento, ni da lugar a derechos u obligaciones de contenido económico para las Partes, asumiendo cada una

de ellas el cumplimiento de las obligaciones que dimanen del mismo con sus propios medios materiales y personales

En el caso de que la prestación de servicios del CSIRT-CAN a las corporaciones locales se ampliara de forma sustantiva, se añadieran nuevos servicios o prestaciones, o se modificaran sustancialmente las especificaciones de los equipos instalados o el número de licencias acordadas entre ambas partes será necesaria la adhesión al nuevo Convenio que se adopte a tal efecto.

Novena.- Responsabilidad.

Cada parte será responsable de los servicios prestados de acuerdo con lo establecido en este Convenio y en los Anexos de servicio correspondientes. Así, el CSIRT-CAN será responsable de poner a disposición y de prestar los servicios a las corporaciones locales adheridas de acuerdo con las condiciones manifestadas en el presente Convenio, de la correcta puesta en disposición de los servicios a los destinatarios finales y de la correcta distribución de los mismos atendiendo y canalizando las peticiones y solicitudes que pudieran llevarse a cabo.

En ningún caso, el CSIRT-CAN será responsable de cualquier pérdida de beneficios, interrupción del negocio, pérdida de datos, costes de cobertura, daños indirectos, especiales, incidentales o emergentes de cualquier clase, relativos o resultantes de la prestación de los servicios (excepto que específicamente se manifestara lo contrario en el servicio debido a su misma naturaleza) objeto de este Convenio, o de los daños causados por el retraso en la prestación de los servicios a menos que estos daños o perjuicios hayan sido causados dolosamente o por negligencia grave por parte del CSIRT-CAN.

Asimismo, tan sólo podrá exigirse la responsabilidad del CSIRT-CAN de acuerdo con esta cláusula cuando los daños y perjuicios sufridos no deriven del incumplimiento por parte del destinatario del servicio de las obligaciones propias, las contenidas en este Convenio o en el convenios o acuerdos establecidos al efecto con el destinatario final de servicios. La corporación local se compromete a hacer un correcto uso de los servicios del CSIRT-CAN puestos a disposición y a facilitar, si fuera necesario, el acceso del personal del CSIRT-CAN en las instalaciones del destinatario de los servicios para su correcta prestación.

El CSIRT-CAN no será responsable, en ningún caso, de cualquier daño o perjuicio que sea causado por la falta de veracidad, descripción, corrección o cualquier otra circunstancia respecto de la información facilitada al CSIRT-CAN que pudiera impedir o dificultar la correcta prestación de sus servicios.

Décima.- Protección de datos personales.

1.-La DGTDSP tratará los datos de carácter personal a los que tenga acceso de acuerdo con lo que establece el Reglamento (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante Reglamento general de protección de datos- RGPD) y .la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD). A tal efecto adoptará e implantará las medidas de seguridad establecidas en dicha Ley Orgánica, en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, y demás normativa de aplicación.

Asimismo, toda la información a la que se acceda por razón del presente Convenio será considerada como confidencial y será tratada con las medidas técnicas y organizativas que garanticen un uso adecuado a esta categorización.

2.- De acuerdo con lo que establece el artículo 28 del RGPD el acceso por parte de la DGTDSP a los datos que le envíe la entidad local para la prestación de los servicios de seguridad TIC recogidos en este Convenio, no se considera cesión ni comunicación de datos, puesto que el acceso y tratamiento de los datos es necesario para la realización de los servicios del CSIRT-CAN y se llevará a cabo siempre bajo las instrucciones de la administración local (como responsable del tratamiento).

La DGTDSP actuará como encargado del tratamiento de los datos que le suministre las respectivas entidades locales responsables del tratamiento de los tipos de datos personales de: los logs de navegación y de direcciones Ips de los usuarios (como interesados) de las respectivas entidades locales, y, en consecuencia, no aplicará ni utilizará los datos para otra finalidad que no sea la ejecución de los servicios de seguridad TIC que se establecen en este Convenio. Asimismo, tampoco comunicará estos datos a terceros, salvo que la entidad local lo solicite o autorice expresamente. La entidad local será responsable en todo caso de recoger las autorizaciones y consentimientos necesarios para permitir y garantizar el acceso de la DGTDSP a los datos necesarios para su prestación de servicios del CSIRT-CAN. El objeto, la duración, naturaleza y finalidad del tratamiento de datos personales se enmarcan en lo dispuesto en el presente Convenio.

Para ello la DGTDSP:

- a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;
- b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza legal;
- c) los servicios del CSIRT-CAN serán prestados por un encargado de tratamiento vinculado a la DGTDSP, mediante licitación pública y financiado con cargo al mecanismo de Recuperación y Resiliencia (MRR); siendo financiado por la Unión Europea – Next Generation EU, el cual tomará todas las medidas necesarias de conformidad con el artículo 32 del RGPD;
- d) asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;
- e) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;
- f) pondrá a disposición del responsable toda la información necesaria para demostrar el

cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable. LA DGTDSP informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

3.- Para la prestación de los servicios del CSIRT-CAN, la DGTDSP recurre a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, A ese subencargado se le imponen, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en este Convenio, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del RGPD y de la LOPDGDD. Si ese otro encargado incumple sus obligaciones de protección de datos, la DGTDSP seguirá siendo plenamente responsable ante la administración local del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

4.-Finalizada la prestación de los servicios, los datos de carácter personal tratados por la DGTDSP para la prestación de los servicios del CSIRT-CAN acordados será destruida o devuelta a la entidad local de acuerdo con sus instrucciones, excepto en lo que se refiere a los datos técnicos previstos en la cláusula siguiente.

Decimoprimera.- Confidencialidad y uso de información técnica.

Toda información o documentación relacionada con los servicios del CSIRT-CAN que cualquiera de las partes aporte en el desarrollo y ejecución de este Convenio tendrá la consideración de confidencial y será titularidad de quien lo aporte. Esta información no podrá utilizarse para fines distintas de la ejecución de las prestaciones de este Convenio, salvo los casos recogidos expresamente, ni comunicarse a terceros sin el consentimiento expreso de su titular, salvo en aquellos casos en que la comunicación sea estrictamente necesaria para la prestación de servicios (en este caso cada una de las partes comunicará con anterioridad los terceros que intervienen en la prestación de servicios). Las partes acuerdan dar el carácter de confidencial al Convenio, obligándose a no revelar a terceros su contenido sin el consentimiento expreso de la otra parte. Esta obligación de confidencialidad estará vigente durante el Convenio y posteriormente a su finalización por cualquier motivo.

Ninguna de las partes adquirirá ningún derecho sobre la información confidencial o de otros derechos de propiedad intelectual o industrial de cualquier tipo de la otra parte como resultado del presente Convenio. Sin embargo, el CSIRT-CAN podrá utilizar la información técnica recibida y tratada en virtud del presente Convenio, previamente anonimizada y una vez eliminadas todas las referencias a cualquiera entidad o persona, para realizar los tratamientos estadísticos u otros necesarios y para incorporarla en la base de datos de conocimiento del CSIRT-CAN. El CSIRT-CAN también podrá utilizar la información recibida para la elaboración de informes, estadísticas y otros documentos, así como para aumentar la base de conocimiento y la mejora de servicios en materia de seguridad.

Decimosegunda.- Eficacia del Convenio y prórroga.

El presente Convenio de cooperación tendrá efectos desde su firma y tendrá vigencia hasta el 31 de diciembre de 2027.

En cualquier momento antes de la finalización del plazo previsto anteriormente, la APCAC y el ayuntamiento podrán acordar unánimemente su prórroga mediante adenda por un periodo de hasta cuatro años adicionales o su extinción.

Sin perjuicio de lo anterior, el presente Convenio, así como las modificaciones, prórrogas y anexos o adendas a los mismos, deberán publicarse en el Boletín Oficial de Canarias, dentro de los veinte días siguientes a su firma, conforme previene el artículo 29.2 de la Ley 12/2014, de 26 de diciembre, de transparencia y de acceso a la información pública, e inscribirse en el Registro General de Convenios del sector público de la Comunidad Autónoma de Canarias, creado por el Decreto 11/2019, de 11 de febrero, de la Presidencia del Gobierno, por el que se regula la actividad convencional y se crean y regulan el Registro General Electrónico de Convenios del Sector Público de la Comunidad Autónoma y el Registro Electrónico de Órganos de Cooperación de la Administración Pública de la Comunidad Autónoma de Canarias.

Decimotercera.- Modificación y Resolución del Convenio.

1. El CSIRT-CAN se reserva el derecho a modificar las condiciones de prestación de los servicios y a introducir en ellos todas las mejoras, novedades y actualizaciones que considere adecuadas para su prestación de acuerdo con los estándares de calidad reconocidos en el mercado de seguridad. En cualquier caso, el CSIRT-CAN informará de las modificaciones a la administración municipal y procederá a definir las mejoras o modificaciones de los servicios para que el ayuntamiento quede debidamente informado.

2. El presente Convenio podrá resolverse cuando concurra alguna de las siguientes causas de resolución:

A) El transcurso del plazo de duración del Convenio sin haberse acordado la prórroga del mismo.

B) El acuerdo unánime de todos los firmantes o decisión de una de las partes. Cuando un ayuntamiento, en su caso, revoque por su cuenta su adhesión al Convenio, los efectos se mantendrán para el resto.

C) Denuncia expresa de cualquiera de las partes estableciéndose un plazo de preaviso de un mes.

D) El incumplimiento de las obligaciones y compromisos asumidos por parte de alguno de los firmantes. En este caso, cualquiera de las partes podrá notificar 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 a la Comisión de Seguimiento y a las demás partes firmantes.

Si trascurrido 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.

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

3. Los efectos de la resolución del presente Convenio serán la conclusión de todas y cada una de las obligaciones de prestación y recepción de servicios en el momento de la efectiva resolución, así como la devolución, en su caso, de los equipos o medios técnicos puestos a

disposición por parte del CSIRT-CAN o cualquier otro elemento aportado por la prestación de los servicios recogidos en el presente convenio. En cualquier caso, a la cláusula decimoprimeras respecto a la confidencialidad de la información sobrevivirá a la terminación del presente Convenio.

Decimocuarta.- Naturaleza administrativa y régimen Jurídico

1. El presente Convenio tiene naturaleza administrativa, quedando excluido del ámbito de aplicación de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo, 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, conforme dispone su artículo 6, al no tener por objeto prestaciones propias de los contratos, rigiéndose por lo dispuesto en el Capítulo VI del Título Preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, y por el Decreto 11/2019, de 11 de febrero, por el que se regula la actividad convencional y se crean y regulan el Registro General Electrónico de Convenios del Sector Público de la Comunidad Autónoma y el Registro Electrónico de Órganos de Cooperación de la Administración Pública de la Comunidad Autónoma de Canarias.

2. No obstante lo dispuesto en el apartado anterior, se aplicarán los principios previstos en la legislación estatal en materia de contratos del sector público a los efectos de resolver las dudas y lagunas que puedan surgir en relación a la interpretación y aplicación del presente Convenio.

Decimoquinta.- Resolución de controversias y jurisdicción competente.

1. La resolución de las controversias que pudieran plantearse sobre la interpretación, aplicación, modificación, resolución y efectos del presente Convenio deberán de solventarse de mutuo acuerdo entre las partes, a través de los acuerdos que se adopten en la Comisión de Seguimiento prevista en el mismo.

2. Agotada dicha vía y para el supuesto de que las referidas controversias no hubieran podido ser solucionadas, el conocimiento de las cuestiones litigiosas competirá a los órganos jurisdiccionales contencioso-administrativos, siendo la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Canarias la competente para conocer en única instancia de los recursos que se deduzcan en relación con el presente Convenio, en virtud de lo prevenido en el artº. 10.1, apartado g) de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en su redacción actual.

Decimosexta.- Mecanismos de evaluación.

Inmediatamente después de la finalización de cada uno de los años de vigencia del Convenio, por la persona responsable de la Dirección General de Transformación Digital de los Servicios Públicos, y por la persona responsable del ayuntamiento, se emitirán sendos informes técnicos sobre la repercusión, cumplimiento y evaluación de las acciones previstas en el presente Convenio. Tales informes serán sometidos a la Comisión de Seguimiento, que procederá a su examen y valoración a los efectos prevenidos en el apartado p) del artículo 7 del Decreto 11/2019, de 11 de febrero, por el que se regula la actividad convencional y se crean y regulan el Registro General Electrónico de Convenios del Sector Público de la Comunidad Autónoma y el Registro

Electrónico de Órganos de Cooperación de la Administración Pública de la Comunidad Autónoma de Canarias.

Y para que así conste, y en prueba de conformidad, se firma electrónicamente este documento.

EL VICECONSEJERO DE PRESIDENCIA

EL ALCALDE

43269521N
OSCAR RAMON
HERNANDEZ
(R: P3500200E)

Firmado digitalmente
por 43269521N
OSCAR RAMON
HERNANDEZ (R:
P3500200E)
Fecha: 2025.09.18
14:06:29 +01'00'

ANEXO I

SERVICIOS INCLUIDOS EN EL CONVENIO.

Servicios reactivos: Son servicios prestados destinados a minimizar el impacto de una amenaza o incidente. Se despliegan una vez detectado un evento de seguridad indeseado e inesperado o, a solicitud de alguna de las administraciones públicas canarias que haya identificado alguna anomalía en su infraestructura tecnológica, entre otros se incluyen en este convenio los siguientes:

- **Generación de Alertas y advertencias:** Consisten en la diseminación de información descriptiva de ataques o intrusiones, de vulnerabilidades o amenazas, virus informáticos o falsas alarmas, contenidos ilícitos o dañinos y recomendaciones para enfrentarse a los mismos, consejos y guías de protección, o bien acciones de recuperación para los sistemas afectados.
- **Gestión de Incidentes:** Recepción, análisis, clasificación, categorización y priorización de las peticiones e informes recibidos para luego proceder a su gestión según la misión y función del centro. Servicios de asistencia técnica y coordinación de la recuperación de los sistemas, tales como los de apoyo a servicios policiales o judiciales encargados de la investigación del incidente.
- **Gestión de Vulnerabilidades:** Servicios de diagnóstico y auditoría de los sistemas informáticos de los usuarios, apoyo técnico mediante el desarrollo de soluciones, parches de software o de configuración que resuelvan las vulnerabilidades encontradas, y servicios de coordinación de las actividades de mitigación del riesgo mediante la notificación e intercambio de información con entidades nacionales e internacionales.

Servicios proactivos: cuya función es reducir los riesgos de seguridad mediante distribución de información e implantación de sistemas de protección y detección.

- **Auditoría o evaluación de seguridad:** Revisión de infraestructuras y configuraciones, repaso de buenas prácticas y procedimientos, detección de vulnerabilidades y posibles huecos o fallos de seguridad y pruebas de penetración en los sistemas, Así como coadyuvar al cumplimiento legal, especialmente en protección de datos personal, Esquema Nacional de Seguridad o la ISO 27001.
- **Detección de intrusiones:** Instalación de sensores en dispositivos, sistemas y aplicaciones distribuidos por toda la red de usuarios adscritos y el análisis en detalle de la información recopilada.
- **Distribución de información:** Orientados a proporcionar a los usuarios del centro información útil y actualizada de forma amigable sobre alertas, guías metodológicas, soluciones disponibles, estadísticas, referencias documentales, etc.
- **Anuncios y Avisos:** Información sobre estadísticas de incidentes, vulnerabilidades e intrusiones. Acceso a bases documentales de guías y consejos

Servicios Especiales o de valor añadido: cartera de servicios que pretenden mejorar los procesos de trabajo tanto de la comunidad a la que se da servicio como del propio CSIRT-CAN.

ANEXO II

PAQUETES DE CIBERSEGURIDAD.

El objeto de este convenio consiste, entre otros, proporcionar en el momento de adhesión a determinadas entidades locales de un Paquete de Ciberseguridad compuesto por diversos sistemas, instalándose en sus propias dependencias. De esta forma se le dota de equipamiento de seguridad, que servirá tanto para la propia entidad local, como para suministrar inteligencia al CSIRT-CAN.

Este Paquete de Ciberseguridad estará dimensionado en función del tamaño de la entidad local según tipología de tamaño poblacional:

Clasificación	Criterio	Municipios/Cabildos
Muy Grande	Más de 900.000 hab.	1
Grande	Más de 100.000 hab.	4
Mediano	Entre 20.000 y 100.000 hab.	16
Pequeño	Hasta de 20.000 hab.	31
Total		52

El suministro se entregará e instalará de forma ordenada, atendiendo a una planificación aprobada por la DGTDSP/CSIRT-CAN, en cuya elaboración y actualización se tendrán en cuenta criterios como:

- Fecha de registro de la firma del convenio.
- Ubicación geográfica de la entrega.
- Prioridades y objetivos que determine la DGTDSP o el CSIRT-CAN en cada momento.

El contenido del paquete de Ciberseguridad está compuesto por:

- Firewall, dimensionado según la clasificación del municipio o cabildo.
- Sondas, dimensionado según la clasificación del municipio o cabildo.
- Herramientas de protección (MicroClaudia y EDR)
- Herramientas de autenticación para segundo Factor de Autenticación

La cesión de los diferentes elementos del Paquete de Ciberseguridad se realizará de forma excepcional y única. En cuanto al mantenimiento de los diferentes elementos, una vez finalizado el periodo de garantía, será responsabilidad exclusiva de la parte que lo reciba, quien en caso de querer mantener los mismos, deberá asumir todos los costos y encargarse de su conservación a partir de la cesión.

ANEXO III

PROMOCIÓN.

En relación al principio de comunicación, información y publicidad se debe dar visibilidad al origen de los fondos recibidos de tal manera que en la documentación y medios de difusión de sus acciones y en cuanta publicidad se haga, deberán hacer constar junto con el emblema de la Unión Europea la declaración de financiación que establezca “Financiado por la Unión Europea Next Generation EU” junto al logo del Plan de Recuperación, Transformación y Resiliencia (Anexo VI).

A lo largo de la implantación del CSIRT-CAN se realizará una labor de difusión y promoción del centro para darlo a conocer tanto internamente, en la administración pública de la Comunidad Autónoma Canaria, como ante el resto de actores de la Comunidad Autónoma Canaria. Este tipo de acciones incluyen:

- La creación del portal web de CSIRT-CAN, alojado en la infraestructura corporativa del Gobierno de Canarias, en el que se publique información sobre el centro, noticias y alertas de seguridad.
- La realización de jornadas, la preparación de mercadotecnia, la creación y difusión de contenido multimedia, y otras acciones de promoción.
- Dinamización y gestión de RRSS:

Esta promoción tendrá carácter estratégico, puesto que de la misma dependerá el crecimiento con la progresiva incorporación de entidades locales canarias, por lo que se regirá por un Plan de Promoción.

Participación y colaboración

CSIRT-CAN ofrecerá la participación y colaboración con otras entidades, entre otras, la participación en foros y plataformas de reconocido prestigio para la coordinación y colaboración entre CSIRT, tanto de ámbito nacional como internacional, así como la colaboración con las autoridades competentes en materia de Ciberseguridad nacional.

En materia de seguridad de las redes y sistemas de información, CSIRT-CAN asumirá la colaboración, la comunicación y la notificación de incidentes con el CCN-CERT, con otros CSIRT de referencia y con las autoridades competentes si fuese necesario, en los términos que determina Real Decreto 43/2021, de 26 de enero (por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información).

De esta forma, actuará como catalizador de information sharing entre diferentes organismos y centros nacionales e internacionales con el objeto de prevenir y detectar problemas de seguridad, con el fin de reducir el impacto asociado en caso de que estos se materialicen.

Eventos

Se organizarán eventos presenciales en materia de seguridad de la información, Ciberseguridad y protección de datos personales. Se organizarán antes de 31/12/2026 al menos dos eventos, uno por cada provincia.

ANEXO IV

FORMACIÓN Y CONCIENCIACIÓN

El portal Web incluirá un apartado de Ejercicios de auto-formación en conceptos de concienciación de seguridad, donde los usuarios podrán realizar un seguimiento de cursos multimedia, planteándose casos y donde puedan obtener una auto-baremación.

Los módulos de concienciación de auto-formación serán interactivos e incluirán módulos de conocimiento en las siguientes áreas:

I. Securización de e-mail: conceptos fundamentales

II. Securización de e-mail: conceptos avanzados

III. Protección mediante contraseñas

IV. Amenazas internas

V. Otras temáticas:

- Protección de datos y destrucción de información
- GDPR
- Seguridad de aplicaciones en los móviles
- Seguridad de dispositivos móviles
- Protección contra el ransomware
- Redes sociales seguras
- Navegación web más segura
- Nociones esenciales de seguridad
- Tipos de ingeniería social
- Ataques por malware

Se tendrán en cuenta las necesidades, los conocimientos previos y los riesgos y las amenazas a las que se exponen los diferentes colectivos dentro de la organización para personalizar y dirigir las acciones de concienciación y formación a cada uno de ellos. Por tanto, deberán incluirse módulos de concienciación para los diferentes colectivos que sería la siguiente:

- Módulos para altos cargos
- Módulos para cargos intermedios y personas clave
- Módulos para el área de IT y Seguridad

Concienciación en Ciberseguridad

Para los ayuntamientos a los que se les despliegue un Paquete de Ciberseguridad, se incluirá una jornada doble PRESENCIAL (misma formación impartida en dos turnos, de al menos 2 horas) de Concienciación en Ciberseguridad. A tal fin se proporcionará un plan de Concienciación detallado (contenido, duración, número de asistentes). La ejecución de las jornadas se consensuará con los interlocutores de los ayuntamientos.

Ejercicios de Phishing

Se realizarán campañas de Phishing a las personas usuarias de los ayuntamientos adheridos a los que se les proporcione el Paquete de Ciberseguridad así como de la administración pública de la comunidad autónoma canaria.

Se realizarán al menos tres campañas hasta el 31 de diciembre de 2026. Las campañas serán personalizadas.

Las simulaciones de phishing permitirán conocer vulnerabilidades de la entidad ante una variedad de engaños. Estas simulaciones pueden evaluar a las personas usuarias con varios tipos de amenazas, como:

- Enlaces adjuntos.
- Solicitudes de datos personales.
- Adjuntos maliciosos.

Las campañas de phishing proporcionarán métricas útiles para medir el grado de conocimiento y concienciación adquirido durante la duración del plan de concienciación de la entidad local.

ANEXO V

LOGOS PARA PROYECTOS QUE SE FINANCIEN CON FONDOS PROCEDENTES DEL INSTRUMENTO EUROPEO DE RECUPERACIÓN («NEXT GENERATION EU»).



**Financiado por
la Unión Europea**
NextGenerationEU

Extraído de la web: Identidad visual | Plan de Recuperación, Transformación y Resiliencia Gobierno de España. (planderecuperacion.gob.es)