III. OTRAS DISPOSICIONES

MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD

42 *Resolución de 27 de diciembre de 2018, de la Subsecretaría, por la que se publica el Convenio en materia de ciberseguridad entre el Ministerio de Política Territorial y Función Pública y el Centro Nacional de Inteligencia.*

El Secretario General de Administración Digital y el Secretario de Estado Director del Centro Nacional de Inteligencia y Director del Centro Criptológico Nacional han suscrito, con fecha 21 de diciembre de 2018, un Convenio en materia de ciberseguridad entre la Administración General del Estado (Ministerio de Política Territorial y Función Pública) y el Centro Nacional de Inteligencia.

Para general conocimiento, y en cumplimiento de lo establecido en el artículo 48.8 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, dispongo la publicación en el «Boletín Oficial del Estado» del referido Convenio como anejo a la presente Resolución.

Madrid, 27 de diciembre de 2018.–El Subsecretario de la Presidencia, Relaciones con las Cortes e Igualdad, Antonio J. Hidalgo López.

ANEJO

Convenio en materia de ciberseguridad entre la Administración General del Estado (Ministerio de Política Territorial y Función Pública) y el Centro Nacional de Inteligencia

En Madrid, a 21 de diciembre de 2018.

De una parte, don Fernando de Pablo Martín, Secretario General de Administración Digital, nombrado para este cargo por el Real Decreto 791/2018, de 29 de junio, actuando en nombre y representación de la Secretaría General de Administración Digital (SGAD) adscrita a la Secretaría de Estado de Función Pública, del Ministerio de Política Territorial y Función Pública (en adelante MTPFP), en ejercicio de las competencias atribuidas por Resolución, de 14 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, sobre delegación de competencias, modificada por la Resolución de 10 de diciembre de 2014, de la Secretaría de Estado de Administraciones Públicas, de conformidad con lo establecido en la disposición adicional segunda del Real Decreto 863/2018, de 13 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Política Territorial y Función Pública.

De otra parte, don Félix Sanz Roldán, Secretario de Estado Director del Centro Nacional de Inteligencia y Director del Centro Criptológico Nacional, en virtud del nombramiento efectuado por Real Decreto 583/2014, de 4 de julio, por el que se nombra a don Félix Sanz Roldán como Secretario de Estado Director del Centro Nacional de Inteligencia; y en el ejercicio de las competencias que tiene atribuidas por el artículo 9.2.c) de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia.

cve: BOE-A-2019-42
Verificable en http://www.boe.es

Ambas partes, en la representación que ostentan, se reconocen mutua capacidad para obligarse y convenir y

EXPONEN

Primero.

Por Acuerdo de Consejo de Ministros de 2 de octubre de 2015 se aprueba el Plan de Transformación Digital de la Administración General del Estado y sus organismos públicos (Estrategia TIC 2015-2020), instrumento fundamental para el impulso de la transformación digital de la Administración, y marco de referencia para la coordinación de todos los actores y recursos del Estado en el objetivo de hacer sostenible el constante proceso de innovación y mejora en la calidad de los servicios públicos.

Segundo.

De acuerdo con el artículo 71 del Real Decreto 863/2018, de 13 de julio de 21 de julio, por el que se desarrolla la estructura orgánica básica del Ministerio de Política Territorial y Función Pública, la Secretaría General de Administración Digital (en adelante SGAD) es el órgano directivo al que corresponde «la dirección, coordinación y ejecución de las competencias atribuidas al Departamento en materia de administración digital, racionalización de las tecnologías de la información y las comunicaciones en el ámbito de la Administración General del Estado y sus Organismos Públicos y del funcionamiento del Servicio Común de Sistemas de Información y Comunicación». En concreto corresponde a la SGAD, entre otras funciones la gestión compartida, mediante coordinación o prestación directa, en un marco de corresponsabilidad, de los servicios comunes del Sistemas de Información y Comunicación, así como el impulso de la consolidación de servicios, infraestructuras TIC, equipamientos y redes informáticas comunes de la Administración General del Estado y sus organismos públicos.

Tercero.

De conformidad con lo establecido en el artículo 10 del Real Decreto 806/2014, de 19 de septiembre sobre organización e instrumentos operativos de las Tecnologías de la Información y las Comunicaciones en la Administración General del Estado y sus organismos públicos, los medios y servicios TIC de la Administración General del Estado y sus organismos públicos serán declarados de uso compartido cuando, en razón de su naturaleza o del interés común, respondan a necesidades transversales de un número significativo de unidades administrativas. La declaración de medio o servicio compartido habilitará a la SGAD para adoptar las medidas necesarias para su provisión compartida.

Cuarto.

En reunión celebrada el 15 de septiembre de 2015, la Comisión de Estrategia TIC aprobó el Marco regulador para la declaración de servicios compartidos, así como la primera declaración de servicios compartidos en la que se incluía el servicio de seguridad gestionada que consiste en el conjunto de servicios de ciberseguridad que proporcionan protección a la Administración General del Estado y sus organismos públicos e incluye el equipamiento necesario, así como su configuración, puesta en marcha, mantenimiento y gestión. Está previsto constituir para ello un Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus organismos públicos (en adelante SOC de la AGE).

Este servicio persigue una infraestructura global y única, complementaria al servicio compartido de telecomunicaciones, gestionado por personal especializado.

cve: BOE-A-2019-42
Verificable en http://www.boe.es

Quinto.

El Centro Nacional de Inteligencia (en adelante CNI) de acuerdo con el artículo 4.e) de la Ley 11/2002 de 6 de mayo, reguladora del Centro Nacional de Inteligencia, ostenta competencias relativas a la seguridad de las tecnologías de la información consistentes en «Coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones del Centro».

Sexto.

El Centro Criptológico Nacional (en adelante CCN), según el Real Decreto 421/2004 de 12 de marzo, por el que se regula el Centro Criptológico Nacional, se encuentra adscrito al CNI y su actuación comprende la seguridad de los sistemas de las tecnologías de la información y la comunicación (en adelante TIC) de las Administraciones Públicas que procesan, almacenan o transmiten información en formato electrónico, que normativamente requieren protección, y que incluyen medios de cifra.

Por otra parte, el CCN cuenta con el equipo de respuesta a incidentes de seguridad de la información del Centro Criptológico Nacional (en adelante CCN-CERT), que tiene responsabilidad en los ataques procedentes del ciberespacio sobre sistemas del sector público.

Séptimo.

Las partes coinciden en el objetivo de garantizar la seguridad tecnológica incrementando la eficacia y la eficiencia de la Administración General del Estado, mediante el ahorro de costes y de racionalización de recursos.

Por ello, las partes desean formalizar 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 MPTFP y el 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.

El alcance de la colaboración es la prestación de servicios de seguridad a los servicios de administración electrónica en el ámbito del MPTFP, con exclusión de los servicios protegidos por la infraestructura de seguridad de nube SARA. Asimismo, se incluye en el alcance la protección de los servicios de aquellas entidades a las que la SGAD proporciona servicio de seguridad mediante la infraestructura de seguridad referenciada en el texto del Convenio. Se constituirá para ello un Centro de Operaciones de Ciberseguridad para el Ministerio de Política Territorial y Función Pública (en adelante SOC del MPTFP), que operará como una extensión del Centro de Operaciones de Ciberseguridad de la Administración General del Estado (SOC de la AGE) tendiendo de manera progresiva a unificar y converger las diferentes actuaciones de seguridad que se proporcionen.

cve: BOE-A-2019-42
Verificable en http://www.boe.es

Segunda. *Compromisos de las partes.*

Son actuaciones a realizar:

En relación a la gestión del servicio de seguridad, la SGAD asume:

La dirección estratégica y dirección técnica operativa, así como el seguimiento del proyecto. La SGAD marcará las directrices técnicas a aplicar.

La provisión de equipamiento e infraestructura, salvo la indicada en el propio Convenio.

La definición del modelo de relación y del modelo de gestión del servicio.

La definición de la política de seguridad del servicio y del paquete de documentación para entidades usuarias.

La interlocución con los responsables de seguridad de las entidades dentro del alcance para la definición e implementación de la política de seguridad a aplicar y las posibles excepciones solicitadas a las mismas.

Por su parte, el CCN asume:

A nivel operativo: la gestión y seguimiento del servicio de seguridad mediante el que se mejorarán las capacidades de vigilancia y detección de incidentes en los sistemas de la SGAD y se optimizará la capacidad de reacción y respuesta ante cualquier ataque, de conformidad con los criterios e información suministrada por la SGAD. La gestión técnica operativa del equipo de técnicos expertos prestadores de los servicios en el alcance del Convenio, para la que el CCN designará uno o varios responsables técnicos. Estos realizarán la interlocución técnica con los interlocutores expresamente designados por SGAD 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 CCN.

Por su naturaleza centralizada, el servicio de seguridad ofrecido 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 SGAD pondrá a disposición del CCN la infraestructura de seguridad de su propiedad que, se encuentra gestionada por un equipo de personal experto en seguridad, para su posible utilización. El personal experto estará disponible hasta el 31 de diciembre de 2018, siendo necesario proporcionar alternativa a partir de ese momento.

En el anexo I del presente Convenio se especifica detalladamente la relación de actividades que integran las actuaciones de colaboración.

Tercera. *Régimen económico.*

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

En particular, el MPTFP realizará una aportación económica en el marco de la ejecución del presente Convenio, que tendrá como objetivo cubrir los gastos que genera la actuación del inicio del SOC del MPTFP al que se refiere la cláusula anterior, así como para asumir la sostenibilidad funcional y técnica de la misma.

El MPTFP realizará la correspondiente transferencia de crédito al Ministerio de Defensa y repercusión en el presupuesto del CCN desde las aplicaciones presupuestarias del MPTFP:

– 15.29.467G.227.06 de Servicios Centrales del MPTFP.
– 25.04.921P.227.06 de Servicios Periféricos del MPTFP.

El CCN determinará las aplicaciones presupuestarias en las que repercutirá esta modificación presupuestaria.

cve: BOE-A-2019-42
Verificable en http://www.boe.es

La transferencia inicial se realizará con la publicación del Convenio en el BOE, y las sucesivas, con el inicio del ejercicio presupuestario.

El importe de la transferencia de crédito de cada anualidad para la actuación relativa al SOC del MPTFP es el siguiente:

– 2019: 400.000 euros, que se desglosa en 258.000 euros para Servicios Periféricos y 142.000 euros para Servicios Centrales.

– 2020: 400.000, que se desglosa en 258.000 euros para Servicios Periféricos y 142.000 euros para Servicios Centrales.

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 miembros: Cuatro con voz y voto, dos de ellos nombrados por el Secretario General de Administración Digital y los otros dos designados por el titular del CCN. El quinto miembro, que ostentará las funciones de Secretario de la Comisión, con voz pero sin voto, será designado por el titular de la SGAD.

La Presidencia la ostentará uno de los representantes de la SGAD, con voto de calidad.

La Comisión se reunirá de forma ordinaria, al menos, cada tres meses, 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 el MPTFP en el ámbito dentro del 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.

En cualquier caso, las partes firmantes se comprometen a solventar por acuerdo mutuo, en el seno de la Comisión de Seguimiento, cuantas diferencias resulten de la interpretación y cumplimiento de este Convenio, sin perjuicio de la competencia del orden jurisdiccional contencioso administrativo para el conocimiento de cuantas cuestiones y litigios pudieran surgir.

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

cve: BOE-A-2019-42
Verificable en http://www.boe.es

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.

Sexta. *Vigencia, duración y prórroga.*

El presente Convenio surtirá efectos una vez inscrito en el Registro Electrónico estatal de Órganos e Instrumentos de Cooperación y publicado en el «Boletín Oficial del Estado», según lo establecido en la disposición adicional séptima apartado segundo y el artículo 48.8 de la Ley 40/2015, del Régimen Jurídico del Sector Público, y tendrá una vigencia de dos (2) años, desde su publicación en el «Boletín Oficial del Estado», pudiendo prorrogarse de forma expresa, por un máximo de dos (2) años 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. Dentro del referido plazo de tres (3) meses las partes podrán comunicar su renuncia a la prórroga del Convenio.

La tramitación, suscripción y efectos de la prórroga que en su caso se acuerde queda sometida al régimen jurídico de Convenios del capítulo VI del título preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público y resto de normativa aplicable.

Séptima. *Extinción del Convenio.*

El presente Convenio se extinguirá según establece el artículo 51.1 de la Ley 4072015, de 1 de octubre, bien por el cumplimiento de las actuaciones que constituyen su objeto o por incurrir en causa de resolución.

Serán causas de resolución las siguientes:

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

– El acuerdo unánime de todos los firmantes.

– 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 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.

– Por decisión judicial declaratoria de la nulidad del Convenio.

– 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.

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

Octava. *Confidencialidad de la información y protección de datos.*

Las partes se comprometen al intercambio de la información técnica en materia de seguridad necesaria para el cumplimiento efectivo de todos los términos del presente Convenio con las garantías de confidencialidad que en cada caso sean requeridas. La información técnica intercambiada se ciñe a cuestiones de seguridad de los sistemas, servicios, y redes TIC de la MPTFP.

La información técnica, datos de seguridad, soportes, programas, aplicaciones y en general, cualquier intercambio y utilización de medios y técnicas aportados por ambas

cve: BOE-A-2019-42
Verificable en http://www.boe.es

partes al Convenio, permanecerán exclusivamente en el ámbito de relación de las mismas y del personal técnico que colabore en las actividades, obligándose a mantener en régimen de confidencialidad estos medios y técnicas por plazo indefinido y con independencia de la duración de este Convenio. Se excluye de la categoría de información confidencial toda aquella que haya de ser revelada de acuerdo con las leyes o con una resolución judicial.

Toda la información y documentación intercambiada, en el marco del Convenio, será propiedad de las respectivas partes. En todo caso, la documentación generada (CCN) en el ámbito del presente Convenio, será propiedad del MPTFP.

Las actuaciones objeto del presente Convenio que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad la normativa reguladora de la protección de datos de carácter personal.

Las partes podrán dar publicidad a la existencia del presente Convenio en la forma en que ambas lo determinen de mutuo acuerdo.

Novena. *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.

Décima. *Naturaleza del Convenio y resolución de cuestiones litigiosas.*

El presente Convenio, de naturaleza jurídico-administrativa, queda sometido al régimen jurídico de Convenios del capítulo VI del título preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Undécima. *Publicidad y transparencia.*

De conformidad con lo dispuesto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, el presente Convenio será publicado en los términos previstos en su artículo 8.1.b), sin perjuicio de la publicación e inscripción a las que se refiere el artículo 48.8 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, así como de las obligaciones correspondientes por ambas partes en materia de fiscalización y control por el Tribunal de Cuentas u organismo autonómico equivalente.

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 Secretario General de Administración Digital, Fernando de Pablo Martín.–El Secretario de Estado Director del Centro Nacional de Inteligencia y Director del Centro Criptológico Nacional, Félix Sanz Roldán.

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.

cve: BOE-A-2019-42
Verificable en http://www.boe.es

Alcance

Mediante este Convenio de colaboración se debe prestar servicios de seguridad perimetral a los servicios de administración electrónica y a los usuarios de las siguientes entidades y organizaciones:

– Todos los órganos y organismos adscritos al MPTFP.
– En general, cualquier entidad a la que la Secretaría General de Administración Digital deba prestar servicio a futuro mediante esta misma infraestructura de seguridad.
– Consejo de Administración de Patrimonio Nacional (CAPN), adscrito al Ministerio de la Presidencia Relaciones con las Cortes e Igualdad.

El alcance del acuerdo de colaboración incluye la gestión y seguimiento del servicio de seguridad mediante el que se mejorarán las capacidades de vigilancia y detección de incidentes en los sistemas de la SGAD y se optimizará la capacidad de reacción y respuesta ante cualquier ataque, de conformidad con los criterios e información suministrada por la SGAD.

De igual manera, el CCN asumirá la gestión técnica operativa del equipo de técnicos expertos prestadores de los servicios en el alcance del Convenio, para la que el CCN designará uno o varios responsables técnicos. Estos realizarán la interlocución técnica con los interlocutores expresamente designados por SGAD 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 CCN.

Por otra parte, se debe realizar la atención a las incidencias de los usuarios de todas estas entidades, que se encuentran ubicados tanto en diversos centros de la Comunidad de Madrid, como en sedes periféricas de los distintos organismos, como pueden ser por ejemplo las Delegaciones del Gobierno, Subdelegaciones del Gobierno y Direcciones Insulares, pero que acceden a Internet a través de las dos sedes mencionadas.

Además de lo anterior, se requiere disponer de personal especializado en la detección proactiva y en el tratamiento de incidentes de seguridad. Entre estos últimos se incluye el tratamiento de las alertas recibidas desde el sistema del SAT-INET del CCN y de las recibidas desde el servicio antiDDoS ofrecido por el Lote 3 del concurso de comunicaciones centralizado, que deben ser atendidas en horario 24x7.

Requisitos y características técnicas del servicio demandado

Se requiere un servicio de gestión de la seguridad perimetral de las entidades en el alcance. Los servicios prestados, así como los sistemas de información que los sustentan, deberán prestarse de conformidad a los requisitos de seguridad establecidos en la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, 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 CCN proporcionará tanto el equipamiento necesario para la prestación del servicio, pudiendo reutilizar el actual si lo considera oportuno, como el personal técnico (personal del SOC del MPTFP) que 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 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 acuerdo, 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 13.000, incluyendo los de todas las entidades.

cve: BOE-A-2019-42
Verificable en http://www.boe.es

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.

Dentro del servicio de soporte y asistencia técnica se incluirán estudios de viabilidad de servicios, de implantación de nuevos proyectos, ayuda a la resolución de problemas de interconexión de equipos de la plataforma de seguridad y otros equipos de la SGAD o de las propias entidades, etc., siempre que encuentren cabida en el marco de gestión definido en el presente pliego.

Se realizará la actualización continua de toda la documentación relativa a la infraestructura de seguridad perimetral, a los incidentes de seguridad y a los procedimientos de gestión operativa, configuración y mantenimiento de la misma. Se mantendrá actualizado el inventario detallando tanto la descripción física de los equipos como las versiones del software que tienen en cada momento. La documentación será propiedad de las entidades y estará en todo momento a disposición de los interlocutores válidos de la misma. De igual manera, el personal asignado tanto al servicio de gestión operativa como al de soporte remoto 24 x 7 dispondrán de acceso a aquella parte de la documentación que necesiten conocer para la adecuada prestación del servicio.

Será responsabilidad del CCN la gestión de la infraestructura necesaria para la prestación del servicio, control de versiones y configuraciones, así como la gestión de la reparación de las averías que pudiesen surgir.

Habrá de informar, con al menos cinco días laborables de antelación, de las paradas programadas del servicio y contar con la aprobación de los directores técnicos de la SGAD 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 8 h a 18:30 h, durante los días laborables. En todo caso deberá garantizarse la prestación de este servicio durante todo el año incluyendo periodos 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.

El servicio de monitorización y soporte 24 x 7 deberá realizar su labor durante todos los periodos horarios no cubiertos por el personal adscrito al servicio de gestión operativa.

Se utilizará la herramienta de gestión de incidencias proporcionada por la SGAD 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 periodo. 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 intrusión 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

cve: BOE-A-2019-42
Verificable en http://www.boe.es

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 Extrema, Muy Alta o Alta y su entrega a las entidades en los plazos establecidos.

– Mantenimiento y soporte del hardware y del software: Será responsabilidad del 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.

– Monitorización y soporte 24 x 7: Deberá proporcionarse un servicio de monitorización y soporte 24 x 7 x 365 de toda la plataforma de seguridad, para velar de manera proactiva por la disponibilidad de la plataforma y tratar cuantos incidentes ocurran fuera del horario laboral. Este servicio se podrá prestar habitualmente en modo remoto, salvo en aquellos casos en los que sea necesario acudir en modo presencial a cualquiera de los centros donde se aloje la plataforma de seguridad para resolver una incidencia. En ese caso deberán acudir presencialmente a resolverlo sin ningún tipo de coste adicional. Se deberá llevar un registro de incidencias y notificarlas a los responsables autorizados de las entidades.

Se proporcionará a los interlocutores válidos de las entidades al menos un teléfono de contacto del SOC del MPTFP que no sea de tarificación adicional (que no sea 902 o similar), atendido en horario 24 x 7 en castellano, así como una dirección de correo electrónico en la que poder contactar.

El CCN configurará una conexión remota debidamente securizada, el equipamiento y las herramientas de monitorización necesarias que permitan al equipo al cargo del 24 x 7 detectar la posible indisponibilidad de los diversos elementos que componen la plataforma de seguridad así como los demás incidentes de seguridad que puedan afectarles. Siempre utilizando la infraestructura actual del organismo. Si se considera necesaria por ambas partes se verá la forma de financiación de la nueva adquisición y migración.

Descripción de servicios de seguridad requeridos

Las entidades cuentan en la actualidad con los servicios de seguridad que se enumeran a continuación, cuyo detalle será compartido con el CCN. Deberán prestarse servicios como mínimo equivalentes a los mismos.

– Protección mediante cortafuegos de distintos fabricantes.
– Sistemas de detección (IDS) y prevención (IPS) de intrusiones.
– Servicios de protección del correo electrónico de pasarela.
– Plataforma de navegación segura y autenticada.
– Servicio de resolución DNS interna y de navegación
– Plataforma de acceso remoto (terminador de túneles VPN).
– Equipamiento gestor de ancho de banda.
– Servicio gestionado de correlación de eventos (SIEM).
– Elementos de monitorización de servicios.
– Elementos específicos adicionales pertenecientes al Instituto Nacional de Administración Pública (INAP):

• Cortafuegos que protegen los servicios del INAP.

– Elementos específicos adicionales pertenecientes a la Mutualidad General de Funcionarios Civiles del Estado (MUFACE):

• Cortafuegos que protegen los servicios de MUFACE.

– Herramientas de hacking ético:
– Se dispone en la actualidad de varias máquinas adicionales que prestan servicios auxiliares en la prestación del servicio.

cve: BOE-A-2019-42
Verificable en http://www.boe.es

Productos, procedimientos y documentación que la sgad/entidades entregarán al CCN

La SGAD/Entidades procederán en virtud de este Acuerdo a la entrega al CCN de la documentación y/o procedimientos que este pueda requerir para la puesta en marcha del servicio, tales como inventarios, esquemas y documentación sobre la arquitectura, informes o cualquier otra documentación requerida expresamente por el 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 CCN

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

Las siguientes tareas son realizadas conforme a la idea del SOC de la AGE y poder realizar su materialización en el Convenio.

Las medidas que el CCN aplicará son:

– 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 ENDpoints para evaluar la seguridad de equipos, controlar acciones mal intencionadas y protección contra malware.

– Auditorías de seguridad.

El CCN considera tener un conocimiento del estado de la red y de las infraestructuras de los sistemas de información un factor clave en el desarrollo del Convenio. Según el resultado de dicho estado de seguridad se pueden conocer puntos débiles o lugares donde focalizar o reforzar los niveles de seguridad. En el futuro SOC de la AGE será uno de los servicios iniciales de entrada de los organismos. 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 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 de información precisa y poder hacer investigaciones de seguridad de valor para el organismo. Actualmente el CCN desarrolla un SIEM para realizar los objetivos mencionados y mejorar la seguridad de la empresa.

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 ENDpoint, para una posterior adquisición si el organismo considera su idoneidad, dota de una protección muy exhaustiva de los equipos además de ampliar la correlación y eficiencia del SIEM que se instalará en el organismo.

cve: BOE-A-2019-42
Verificable en http://www.boe.es