ORDEN DEL CONSEJERO DE SEGURIDAD, POR LA QUE SE ACUERDA LA APROBACIÓN PREVIA DEL PROYECTO DE DECRETO POR EL QUE SE DESARROLLAN LAS FUNCIONES Y COMPETENCIAS DE LA AGENCIA VASCA DE CIBERSEGURIDAD.

Por Orden de 9 de junio de 2026, del consejero de Seguridad, se acordó el inicio del procedimiento para la elaboración del proyecto de decreto de por el que se desarrollan las funciones y competencias de la Agencia Vasca de Ciberseguridad.

Elaborados el texto y la memoria de análisis de impacto normativo, procede, de conformidad con lo establecido en el artículo 15 de la Ley 6/2022, de 30 de junio, del Procedimiento de Elaboración de las Disposiciones de Carácter General, su aprobación previa, antes de evacuar los trámites de audiencia y consulta que procedan.

RESUELVO

PRIMERO.- Aprobar con carácter previo el texto del proyecto de decreto por el que se desarrollan las funciones y competencias de la Agencia Vasca de Ciberseguridad.

SEGUNDO.- Ordenar la continuación de la tramitación del procedimiento del proyecto de decreto, de conformidad con los trámites establecidos en la Orden de inicio y en la Ley 6/2022, de 30 de junio, para su aprobación.

En Vitoria-Gasteiz, a fecha de la firma electrónica.

Bingen Zupiria Gorostidi
SEGURTASUNEKO SAILBURUA
CONSEJERO DE SEGURIDAD

Donostia - San Sebastián, 1 – 01010 VITORIA-GASTEIZ
tel.: 945 01 87 58

PROYECTO DE DECRETO POR EL QUE SE DESARROLLAN LAS FUNCIONES Y COMPETENCIAS DE LA AGENCIA VASCA DE CIBERSEGURIDAD

EXPOSICIÓN DE MOTIVOS

La creciente digitalización de los sistemas y servicios, así como la interdependencia de las infraestructuras tecnológicas, han convertido la ciberseguridad en un elemento imprescindible para garantizar el adecuado funcionamiento de los servicios públicos, la continuidad de las actividades esenciales y la protección de las personas, los bienes y el interés público. La naturaleza transversal de los riesgos asociados al entorno digital exige, en consecuencia, una actuación pública estructurada, coordinada y dotada de instrumentos específicos que permitan prevenir, detectar y responder de forma eficaz ante incidentes de ciberseguridad.

En este contexto, la Ley 7/2023, de 29 de junio, de creación de la Agencia Vasca de Ciberseguridad, configura a la Agencia como el instrumento público de referencia para la planificación, coordinación y ejecución de las políticas en materia de ciberseguridad en la Comunidad Autónoma de Euskadi, atribuyéndole funciones de carácter estratégico, técnico y operativo orientadas a garantizar un elevado nivel de protección de los sistemas de información y de los servicios públicos y esenciales.

El Decreto 34/2024, de 19 de marzo, por el que se aprueban los Estatutos de la Agencia Vasca de Ciberseguridad, concreta su organización, estructura y régimen de funcionamiento, delimitando el alcance de sus competencias, sin perjuicio de las modificaciones que, en su caso, se introduzcan mediante su posterior desarrollo normativo. Asimismo, el Decreto 318/2024, de 29 de octubre, establece el marco organizativo del Departamento de Seguridad en el que se integra la actuación de la Agencia.

El presente Decreto se ajusta a lo establecido en el marco de la Ley 3/2022, de 12 de mayo, del Sector Público Vasco, que define las entidades incluidas en su ámbito de aplicación, así como en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que regula la actuación administrativa y la tramitación por medios electrónicos. Igualmente, resulta de aplicación el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, que establece los principios y requisitos mínimos en materia de seguridad de la información aplicables al sector público.

Por otra parte, el sistema vasco de atención de emergencias y protección civil, regulado por el Decreto 153/1997, de 24 de junio (LABI), así como la normativa en materia de autoprotección, en particular el Decreto 277/2010, de 2 de noviembre, modificado por el Decreto 21/2019, de 12 de febrero, establecen el marco para la gestión de situaciones de riesgo y emergencia. En este ámbito, la Orden de 7 de junio de 2024, del Vicelehendakari Primero y Consejero de Seguridad, introduce la obligación de elaborar planes de continuidad en materia de ciberseguridad para determinadas actividades sujetas a la norma vasca de autoprotección, incorporando de forma expresa la dimensión digital en la gestión de la continuidad de las actividades.

En atención a lo anterior, el presente Decreto tiene por objeto, por un lado, desarrollar y concretar el ejercicio de las funciones y competencias atribuidas a la Agencia Vasca de Ciberseguridad en la Ley 7/2023, de 29 de junio, de creación de ésta, dotando de un marco sistemático a sus actuaciones en los ámbitos estratégico, de coordinación, auditoría técnica, gestión del riesgo y operaciones; y, por otro, regular el procedimiento para la elaboración, remisión, supervisión e inspección de los planes de continuidad en materia de ciberseguridad exigibles en el marco de la normativa de autoprotección.

A tal efecto, la norma establece un régimen básico de actuación que permite ordenar de forma coherente la intervención de la Agencia, garantizando en todo caso el respeto al ámbito competencial de las distintas administraciones, organismos y entidades, a quienes corresponde la implantación y gestión de las medidas de seguridad en sus respectivos sistemas y servicios.

Del mismo modo, el Decreto delimita su ámbito subjetivo de aplicación, que comprende tanto a las entidades integrantes del sector público vasco, en los términos previstos en la Ley 3/2022, de 12 de mayo, como a aquellas entidades que gestionan servicios públicos o servicios esenciales en la Comunidad Autónoma de Euskadi, extendiéndose, en lo relativo a los planes de continuidad en materia de ciberseguridad, a los titulares de actividades, centros, establecimientos e instalaciones sujetos a la normativa de autoprotección.

Asimismo, la norma articula los mecanismos de coordinación institucional necesarios para garantizar una actuación coherente entre los distintos agentes implicados, incluyendo su integración en el sistema vasco de gestión de emergencias, y regula la recogida y tratamiento de la información necesaria para el ejercicio de las funciones de la Agencia, incorporando las debidas garantías en materia de confidencialidad, protección de datos y seguridad de la información.

En definitiva, mediante este Decreto se establece el marco jurídico necesario para desarrollar de forma efectiva las funciones de la Agencia Vasca de Ciberseguridad y para integrar la ciberseguridad en los sistemas de planificación, gestión del riesgo y autoprotección, contribuyendo así a reforzar la seguridad, la continuidad y la resiliencia de los servicios públicos y de las actividades esenciales en la Comunidad Autónoma de Euskadi.

En su virtud, de conformidad con lo establecido en el ordenamiento jurídico aplicable, a propuesta del Consejero de Seguridad, previa deliberación y aprobación del Consejo de Gobierno en su sesión celebrada el día [●],

DISPONGO

TÍTULO I
DISPOSICIONES GENERALES

Artículo 1.– Objeto.

El presente Decreto tiene por objeto:

1.– Desarrollar y concretar el ejercicio de las funciones y competencias de la Agencia Vasca de Ciberseguridad (en adelante, la Agencia o Cyberzaintza), en ejecución de lo previsto en la Ley 7/2023, de 29 de junio, y en sus Estatutos aprobados por el Decreto 34/2024 y modificados por el Decreto 15/2026, así como establecer el régimen básico de actuación y los procedimientos esenciales para su ejecución.

2.– Regular el procedimiento para la elaboración, remisión, supervisión e inspección de planes de continuidad en materia de ciberseguridad para ciertas actividades sujetas a la norma vasca de autoprotección, incluyendo su tramitación por medios electrónicos.

Artículo 2.– Ámbito de aplicación.

1.– Las previsiones de este Decreto resultarán de aplicación a las administraciones, organismos y entidades integrantes del sector público vasco, en los términos previstos en la Ley 3/2022, de 12 de mayo, del Sector Público Vasco.

2.– Asimismo, las previsiones de este Decreto serán aplicables, en aquellos aspectos dirigidos al tejido empresarial, a todas las empresas, entidades mercantiles y personas físicas que desarrollen una actividad económica, empresarial o profesional en Euskadi, con independencia de que cuenten o no con personal asalariado a su cargo. En el ejercicio de estas actuaciones, se prestará especial atención a las entidades que gestionen servicios esenciales en la Comunidad Autónoma de Euskadi.

3.– También resultarán de aplicación las previsiones de este Decreto a la ciudadanía, en aquellos aspectos en los que el decreto se refiera expresamente a ella.

4.– Exclusivamente en lo que respecta a la función relativa a los planes de continuidad en materia de ciberseguridad para ciertas actividades sujetas a la norma vasca de autoprotección, la presente disposición resultará de aplicación a las personas físicas o jurídicas titulares de actividades, centros, establecimientos, espacios, instalaciones o dependencias cuya operación sea necesaria para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de la ciudadanía, y el eficaz funcionamiento de las Instituciones de Euskadi y sus Administraciones Públicas, siempre que les resulte exigible el cumplimiento de obligaciones en materia de autoprotección.

5.– La Agencia articulará, para el adecuado desarrollo de sus funciones, los servicios que considere más apropiados en cada caso, determinando para cada uno de ellos su aplicabilidad al sector público vasco, el tejido empresarial y la ciudadanía.

TÍTULO II
DESARROLLO DE FUNCIONES

Artículo 3.– Obligación de prestar servicios de ciberseguridad.

La Agencia, en el marco de sus competencias, y atendiendo a la disponibilidad de recursos de que disponga en cada momento, estará obligada a prestar sus servicios de ciberseguridad tanto al sector público vasco como al tejido empresarial y a la ciudadanía, en las condiciones establecidas en su catálogo de servicios.

CAPÍTULO I
FUNCIONES ESTRATÉGICAS

Artículo 4.– Coordinación de actuaciones.

1.– La agencia dará coherencia a las actuaciones del sector público vasco desde una perspectiva integral que favorezca el intercambio de información relevante. Para ello gestionará, coordinará y realizará el seguimiento de las actuaciones que desarrolle en materia de ciberseguridad, identificando las necesidades existentes y canalizándolas para su adecuada atención.

2.– La Agencia coordinará al sector público vasco en la elaboración, desarrollo y actualización de los planes de ciberseguridad de las distintas administraciones, organismos y entidades, con el fin de favorecer un enfoque coherente, alineado y eficaz en la consecución de los objetivos comunes en materia de ciberseguridad.

Artículo 5.– Estrategia de ciberseguridad de Euskadi.

1.– La Estrategia Vasca de Ciberseguridad es el documento marco que establece los objetivos estratégicos y las líneas de actuación en materia de ciberseguridad de la Comunidad Autónoma del País Vasco.

2.– La Estrategia será sometida a un proceso de participación colaborativa, en el que se asegurará la representación tanto del sector público vasco como del tejido empresarial.

3.– La Estrategia se aprobará mediante Acuerdo del Consejo de Gobierno, a propuesta de la persona titular del departamento competente en materia de Seguridad.

4.– Su vigencia será plurianual, y se revisará al menos cada cinco años y cuando las circunstancias tecnológicas, organizativas o de riesgo lo aconsejen.

Artículo 6.– Órganos participantes en la Estrategia de Ciberseguridad.

1.– Existirá un marco de gobernanza de la Estrategia compuesto por, al menos, dos órganos de cooperación interinstitucional: uno de carácter directivo, responsable de establecer las prioridades, orientar las líneas estratégicas y velar por la coherencia de las actuaciones; y otro de carácter técnico, destinado al desarrollo y ejecución de las actuaciones y planes de ciberseguridad.

2.– Las entidades afectadas por la Estrategia deberán participar en los citados órganos de gobernanza, cuando sean requeridas para ello de acuerdo con su ámbito competencial, naturaleza o papel en las líneas de actuación correspondientes. A tal efecto, deberán designar a las personas representantes, garantizando que cuenten con la capacidad técnica y funcional necesaria para contribuir de manera efectiva a las funciones de seguimiento, coordinación y toma de decisiones que dichos órganos tengan atribuidas.

3.– La participación en los órganos de gobernanza comprenderá, al menos:

a) La asistencia y participación activa en las sesiones que se convoquen.
b) La aportación de información relevante para el seguimiento y evaluación del grado de cumplimiento de la Estrategia.
c) La colaboración en las actuaciones de coordinación que se deriven de los acuerdos adoptados en el seno de dichos órganos.

4.– La Agencia liderará el proceso de elaboración, revisión y seguimiento de la Estrategia de Ciberseguridad de Euskadi. Así mismo, actuará como órgano de apoyo al modelo de gobernanza de la Estrategia, asumiendo las funciones de gestión operativa, seguimiento de los acuerdos adoptados y asistencia técnica. Para ello podrá establecer los criterios organizativos, mecanismos de funcionamiento y canales de comunicación necesarios para garantizar una participación eficaz y alineada con los objetivos estratégicos definidos.

Artículo 7.– Modelo de ciberseguridad.

1.– El Modelo de Ciberseguridad de Euskadi constituye el instrumento común de referencia para promover un uso seguro y coherente de los medios electrónicos en el sector público vasco, estableciendo los criterios para la implantación progresiva de una ciberseguridad sólida, coherente y alineada.

2.– El Modelo constituirá el instrumento principal para articular y dar coherencia al conjunto de marcos de referencia, directrices y normas técnicas impulsado por la Agencia. A tal efecto, el Modelo incorporará, al menos, los siguientes elementos:

a) Una estructura formal de roles y responsabilidades en materia de ciberseguridad, que permita articular el Modelo.
b) Un enfoque de evolución por niveles de desarrollo progresivos, que permita adaptar la aplicación de los controles y medidas de ciberseguridad al contexto, recursos, madurez y criticidad de cada entidad.
c) Dominios funcionales de ciberseguridad, en los que se agruparán de manera coherente los controles, criterios técnicos, directrices y normas técnicas, facilitando su comprensión, aplicación y seguimiento.

3.– La Agencia elaborará el Modelo, promoverá su conocimiento e impulsará su adopción e implantación progresiva, desarrollando acciones de promoción, asistencia, formación, herramientas de apoyo, guías prácticas y cualesquiera otros mecanismos que puedan resultar de utilidad para este fin.

4.– La Agencia realizará evaluaciones del cumplimiento del Modelo por parte del sector público vasco, efectuará labores de seguimiento de su grado de adopción, identificará necesidades de mejora y formulará recomendaciones orientadas al refuerzo de la seguridad y la resiliencia de todo el sector público vasco.

5.– La Agencia realizará revisiones periódicas del Modelo, con el fin de adaptarlo a la evolución de las amenazas, de la tecnología y del marco normativo y regulatorio aplicable.

CAPÍTULO II
FUNCIONES OPERATIVAS

Artículo 8.– Concienciación y Capacitación en Ciberseguridad

1.– La Agencia organizará y promoverá actividades de concienciación y formación en materia de ciberseguridad, dirigidas al sector público vasco, a los distintos colectivos profesionales y a la ciudadanía, mediante la difusión de buenas prácticas, experiencias de referencia y conocimiento especializado en el ámbito de la ciberseguridad, con el objetivo de reforzar la cultura de ciberseguridad, el uso seguro de los medios digitales y la adecuada gestión de los riesgos asociados.

2.– La Agencia difundirá los contenidos elaborados por los medios y canales más apropiados en cada caso. Para ello, llevará a cabo la organización de jornadas, talleres, sesiones divulgativas y acciones de transferencia de conocimiento, así como el apoyo a iniciativas orientadas a la mejora de las capacidades técnicas y organizativas en ciberseguridad.

Artículo 9.– Preparación ante incidentes de ciberseguridad

1.– La Agencia evaluará el nivel de preparación tanto del sector público vasco como del tejido empresarial en relación con sus capacidades de respuesta a incidentes de ciberseguridad.

2.– La Agencia realizará simulacros que contribuyan a entrenar la capacidad de respuesta a incidentes de ciberseguridad tanto del sector público vasco como del tejido empresarial, con el objetivo de identificar aspectos de mejora.

Artículo 10.– Vigilancia digital y alerta temprana

1.– La Agencia desarrollará y mantendrá actualizado un modelo específico de ciberinteligencia para Euskadi mediante el cual, llevará a cabo la monitorización proactiva de amenazas relacionadas con la ciberseguridad en el entorno digital, con el fin de identificar, analizar y anticipar posibles riesgos y actividades maliciosas que puedan tener afección en la Comunidad Autónoma de Euskadi.

2.– Dicho modelo permitirá identificar el nivel de riesgo individual de las entidades desde una perspectiva de ciberseguridad y ofrecerá así mismo una visión de conjunto, lo que permitirá

a la Agencia llevar a cabo medidas globales para contribuir a mejorar el nivel de protección de toda la Comunidad Autónoma de Euskadi.

3.– En caso de que se identifique alguna de dichas amenazas, la Agencia realizará funciones de alerta temprana a las entidades, difundirá avisos y prestará apoyo técnico a la respuesta, facilitando información relevante, recomendaciones y orientaciones técnicas, para que las entidades puedan tomar las medidas oportunas para mitigar el riesgo.

4.– La Agencia establecerá los canales y procedimientos de notificación para la comunicación de alertas de ciberseguridad.

Artículo 11.–Auditorías tecnológicas de seguridad

1.– La Agencia analizará el nivel de vulnerabilidad de las infraestructuras tecnológicas, los sistemas de información, las aplicaciones, los servicios digitales y los activos del sector público vasco, con el objeto de identificar debilidades susceptibles de ser explotadas y contribuir a la reducción del riesgo de ciberseguridad. Así mismo, llevará a cabo auditorías tecnológicas a demanda de las entidades.

2.– Cuando se identifiquen vulnerabilidades críticas, vulnerabilidades explotadas activamente o debilidades que puedan suponer un riesgo grave o inmediato, la Agencia lo notificará a la entidad afectada con la mayor celeridad posible, facilitando la información técnica disponible y las recomendaciones de contención, mitigación o corrección que resulten aplicables.

Artículo 12.–Centro de Operaciones de Ciberseguridad

1.– La Agencia desplegará un centro de operaciones de seguridad (SOC) para monitorizar, analizar y gestionar los eventos de seguridad que afecten o puedan afectar a las infraestructuras tecnológicas y los sistemas de información del sector público vasco, orientado prioritariamente a la monitorización de activos críticos.

2.– El Centro de Operaciones de Ciberseguridad tendrá como finalidad:

d) La monitorización de eventos de seguridad.
e) La identificación temprana de amenazas, vulnerabilidades y comportamientos anómalos, mediante la correlación y análisis de los eventos de seguridad monitorizados.
f) La detección de incidentes de ciberseguridad, facilitando una respuesta coordinada y oportuna.
g) El apoyo técnico a la contención, mitigación y recuperación ante incidentes, en coordinación con los responsables de los sistemas afectados y con los equipos de respuesta correspondientes.
h) La recopilación y análisis de información técnica relevante para proponer medidas que mejoren las capacidades de protección de las entidades.

3.– El Centro de Operaciones de Seguridad monitorizará los eventos provenientes de los sistemas de información y operación de las entidades que lo soliciten mediante los instrumentos de colaboración correspondientes.

4.– El Centro de Operaciones de Seguridad actuará en los casos en los que tenga capacidad directa, y en el resto de los casos identificará y notificará a las entidades afectadas los eventos y los potenciales incidentes de ciberseguridad detectados, para que éstas puedan iniciar las actuaciones de respuesta necesarias.

Artículo 13.–Equipo de respuesta a incidentes

1.– La Agencia ejercerá las funciones de Equipo de Respuesta a Incidentes de Ciberseguridad (CSIRT) competente en la Comunidad Autónoma de Euskadi y coordinará los CSIRT y entidades equivalentes en su ámbito de actuación.

2.– La Agencia actuará como capacidad común de respuesta a incidentes de ciberseguridad de las entidades del sector público vasco a las que les prestará servicio de DFIR, lo que

incluye el apoyo, coordinación, contención, análisis de artefactos, erradicación y recuperación frente a incidentes, facilitando así el alineamiento y la eficacia global.

3.– La Agencia establecerá y promoverá modelos de colaboración y mecanismos de coordinación con otros CSIRT y equipos de respuesta, de ámbito local, autonómico, estatal e internacional, con el fin de favorecer el intercambio de información, la gestión eficaz de incidentes de ciberseguridad y la reducción del impacto y del tiempo de recuperación ante ciberataques, teniendo en cuenta el carácter transfronterizo de las ciberamenazas.

Artículo 14.–Análisis de Incidentes de Ciberseguridad

1.– La Agencia investigará tecnológicamente los incidentes de ciberseguridad que afecten o puedan afectar al sector público vasco, el tejido empresarial o la ciudadanía, especialmente aquellos particularmente relevantes para el sector público vasco o que, por su naturaleza, alcance o impacto potencial, se considere necesario.

2.– La Agencia elaborará informes técnicos orientados a la mejora de la prevención, detección y respuesta frente a ciberamenazas, y formulará recomendaciones técnicas y organizativas dirigidas a reducir el riesgo de recurrencia y reforzar la resiliencia de los sistemas.

3.– Los resultados de las investigaciones y análisis realizados se utilizarán, principalmente, para alimentar el Modelo de Ciberseguridad de Euskadi, apoyar la elaboración de recomendaciones, alertas y medidas preventivas dirigidas al conjunto del sector público vasco y contribuir a la evaluación y mejora continua del nivel de ciberseguridad en el uso de medios electrónicos.

4.– En el ejercicio de sus funciones operativas, la Agencia prestará apoyo técnico especializado en materia de ciberseguridad a las autoridades competentes, a requerimiento de estas, para el adecuado desarrollo de actuaciones relacionadas con la prevención e investigación de conductas ilícitas, incluida la asistencia técnica en actuaciones de intervención sobre sistemas y en la obtención, análisis y tratamiento de evidencias electrónicas.

CAPÍTULO III
FUNCIONES DE AUDITORÍA Y GOBIERNO DEL RIESGO

Artículo 15.–Órgano de Auditoria Técnica.

1.– La Agencia actuará como Órgano de Auditoría Técnica (OAT), ejerciendo funciones de auditoría de los sistemas de información del sector público vasco, de conformidad con lo previsto en la normativa aplicable y, en particular, en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), con el objeto de verificar el grado de adecuación de los sistemas, servicios y procesos a los requisitos de seguridad establecidos.

2.– Las auditorías de conformidad con el ENS se llevarán a cabo conforme a lo establecido en el citado Real Decreto, así como en las guías, instrucciones y criterios técnicos dictados por el órgano competente en materia de acreditación del ENS. Para ello, la Agencia establecerá los procedimientos y formatos necesarios, tanto para el desarrollo del proceso de auditoría como para la comunicación de los resultados a las entidades auditadas y, cuando proceda, al órgano competente en materia de acreditación.

3.– La Agencia garantizará que las auditorías de conformidad con el ENS se realicen con plena independencia, imparcialidad y confidencialidad, de acuerdo con los principios que rigen la actuación del OAT y con los procedimientos internos establecidos a tal efecto.

4.– Las auditorías se realizarán a instancia de las entidades responsables de los sistemas o de los órganos competentes.

5.– Las entidades auditadas deberán colaborar activamente en el desarrollo del proceso de auditoría, facilitando el acceso a la información, sistemas, instalaciones y personas que resulten necesarios para la correcta ejecución de la auditoría, en los términos previstos en la normativa aplicable.

6.– Las actuaciones de auditoría técnica tendrán carácter técnico y no sancionador, sin perjuicio de las competencias que correspondan a otros órganos o autoridades en materia de control, supervisión o régimen sancionador.

7.– La implantación de las medidas correctoras corresponderá a las entidades responsables de los sistemas auditados.

Artículo 16.–Evaluaciones técnicas

1.– La Agencia realizará evaluaciones técnicas periódicas sobre el grado de implantación, adecuación y eficacia de las medidas de ciberseguridad desplegadas en el ámbito del sector público vasco, con el fin de disponer de una visión consolidada y objetiva del estado de las políticas públicas en materia de ciberseguridad desplegadas y de su evolución temporal.

2.– Las evaluaciones podrán atender al grado de adopción del Modelo de Ciberseguridad de Euskadi, a indicadores técnicos de riesgo, madurez, resiliencia y capacidad de respuesta o al cumplimiento de la normativa y regulación aplicable en materia de ciberseguridad.

3.– Las evaluaciones técnicas se realizarán con carácter periódico y, al menos, bienalmente, conforme a una metodología homogénea definida por la Agencia, que permita la comparación de resultados, la identificación de tendencias y la detección de áreas de mejora. Dichas evaluaciones técnicas se llevarán a cabo aplicando criterios de proporcionalidad y minimización de impacto operativo, en función de la naturaleza, criticidad y nivel de riesgo de los sistemas y servicios analizados.

4.– Como resultado de las evaluaciones realizadas, la Agencia elaborará informes técnicos de evaluación, de carácter agregado o específico según proceda, que incluirán análisis de situación, conclusiones y recomendaciones orientadas a la mejora de las capacidades de ciberseguridad.

5.– Los resultados de las evaluaciones técnicas se utilizarán para orientar la actualización del Modelo de Ciberseguridad de Euskadi, como fuente de información para la elaboración de la Estrategia de Ciberseguridad de Euskadi, para apoyar la definición de prioridades y actuaciones de refuerzo en materia de ciberseguridad y para contribuir a la mejora continua del nivel de ciberseguridad en el uso de medios electrónicos en el sector público vasco.

6.– Las evaluaciones técnicas tendrán carácter técnico y no sancionador, y no implicarán la asunción por parte de la Agencia de responsabilidades directas sobre la gestión u operación de los sistemas de información de las entidades analizadas, ni sustituirán los controles que correspondan a otros órganos de control interno o externo.

Artículo 17.–Gestión del riesgo

1.– La Agencia recopilará la información pertinente de las entidades que gestionan servicios públicos o servicios esenciales en la Comunidad Autónoma de Euskadi en relación con el estado de la seguridad de la información, con el fin de disponer de una visión agregada y actualizada de los riesgos, capacidades y niveles de protección existentes.

2.– La información recopilada podrá referirse al nivel de implantación de medidas de seguridad, la identificación de activos y servicios esenciales o la exposición a amenazas. Dicha información podrá ser obtenida bien directamente por la Agencia en el ejercicio de sus propias funciones o bien indirectamente a través de los datos facilitados por las propias entidades.

3.– A partir de la información recopilada, la Agencia realizará análisis y valoraciones de riesgo en materia de ciberseguridad, con el objetivo de identificar escenarios de riesgo relevantes, dependencias críticas y necesidades de refuerzo.

4.– Sobre la base de los análisis realizados, la Agencia podrá proponer medidas técnicas, operativas, organizativas o de coordinación orientadas a la reducción del riesgo y al refuerzo de la protección de los servicios públicos y esenciales. Así mismo los resultados se utilizarán para facilitar información relevante a las partes interesadas en el ámbito de sus competencias y apoyar la coordinación y la toma de decisiones en materia de ciberseguridad.

Artículo 18.–Apoyo a los planes de ciberseguridad

1.– La Agencia prestará apoyo metodológico para la definición de objetivos, líneas de actuación, prioridades y medidas contenidas en los planes de ciberseguridad, promoviendo su alineamiento con el Modelo de Ciberseguridad de Euskadi, desarrollando para ello cuantos materiales y acciones considere necesarios.

2.– La Agencia establecerá mecanismos de seguimiento y apoyo orientados a facilitar la ejecución de los planes de ciberseguridad, identificando dificultades comunes y proponiendo actuaciones de refuerzo o ajuste cuando resulte conveniente. La Agencia establecerá sinergias que permitan optimizar recursos y reforzar la eficacia de las actuaciones.

CAPÍTULO IV
COORDINACIÓN INSTITUCIONAL Y COOPERACIÓN

Artículo 19.–Cooperación interadministrativa.

1.– La Agencia impulsará mecanismos de coordinación técnica en materia de ciberseguridad entre las administraciones que integran el sector público vasco, con el fin de garantizar una actuación coherente y eficaz.

2.– La Agencia podrá establecer los acuerdos de colaboración y convenios necesarios con los diferentes órganos competentes en cada caso, con el fin de que sus servicios sean incorporados a la dinámica interna de cada entidad.

Artículo 20.–Coordinación con el Departamento de Seguridad.

1.– La Agencia establecerá diferentes mecanismos de coordinación con el Departamento de Seguridad de la Administración General de la CAE:

a) Con la Dirección competente en materia de protección civil y emergencias, con el fin de prestar apoyo técnico en caso de emergencias relacionadas con un incidente de ciberseguridad, así como a efectos de interoperabilidad con el Registro de Planes de Autoprotección.

b) Con el sistema vasco de atención a emergencias y protección civil y la Ertzaintza, prestando el apoyo técnico necesario en caso de emergencias relacionadas con ciberincidentes.

c) Con el LABI, prestando asistencia técnica en aquellas situaciones derivadas de ciberataques o incidentes de ciberseguridad que puedan dar lugar a una situación de emergencia.

d) Con la Dirección competente en materia de coordinación de seguridad, para el apoyo en materia de ciberseguridad a las entidades que forman parte del Plan para la Protección de Infraestructuras Sensibles de Euskadi.

e) Con la Dirección competente en materia de Procesos Electorales, participando en los operativos relacionados con la ciberseguridad de los procesos electorales.

f) Con la Jefatura de la Ertzaintza competente en materia de Coordinación de Ciberseguridad, para actividades en el ámbito de la innovación y medidas relacionadas con la persecución del ciberdelito.

g) Con la Oficina de la Ertzaintza competente en materia de Inteligencia, en ámbitos de investigación de la cibercriminalidad.

h) Con otras divisiones, jefaturas, secciones y unidades de la Ertzaintza cuyas funciones se encuentren relacionadas o puedan tener un componente de ciberseguridad, a fin de facilitar el intercambio de información, la valoración técnica de los incidentes y la adopción de actuaciones coordinadas cuando resulte necesario.

2.– Asimismo, la Agencia se coordinará con el resto de las direcciones del Departamento de Seguridad, así como, en su caso, con las viceconsejerías correspondientes, en el ámbito de sus respectivas competencias, a fin de asegurar una actuación coherente en materia de ciberseguridad y gestión de incidentes.

Artículo 21.–Relación con autoridades, órganos judiciales y cuerpos policiales.

La Agencia prestará apoyo técnico y facilitará la coordinación necesaria con las autoridades competentes, los órganos judiciales y los cuerpos policiales, con el objetivo de contribuir a la ciberseguridad y a la protección de los sistemas de información policiales, promoviendo el intercambio de información técnica, la investigación de actividades potencialmente ilícitas y la adopción de medidas de apoyo que resulten necesarias, siempre con respeto a los ámbitos competenciales propios de cada institución.

Artículo 22.–Relaciones con el Centro Criptológico Nacional.

1.– La Agencia actuará como punto de contacto frente al Centro Criptológico Nacional tanto de cada uno de los organismos de la Administración general de la Comunidad Autónoma de Euskadi como de aquellas organizaciones dependientes o adscritas a ella, especialmente en todo lo relativo a sus obligaciones de información relacionada con el estado de las principales variables de la seguridad en los sistemas de información, así como en todo lo relacionado con la notificación de aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información concernidos, todo ello sin perjuicio del cumplimiento de las obligaciones establecidas por los sujetos de aplicación.

2.– Por dicho motivo, tanto la Administración general de la Comunidad Autónoma de Euskadi como las organizaciones dependientes o adscritas a ella deberán notificar a la Agencia tanto el estado de las principales variables de la seguridad en sus sistemas de información como los incidentes que tengan un impacto significativo en la seguridad de dichos sistemas de información.

3.– Todas las demás organizaciones que conforman el sector público vasco, en aras de una mayor eficacia en la gestión de su ciberseguridad, podrán designar a la Agencia como punto de contacto frente al Centro Criptológico Nacional en lo relativo tanto a sus obligaciones de información relacionada con el estado de las principales variables de la seguridad en los sistemas de información como a las relacionadas con la notificación de aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información concernidos, todo ello sin perjuicio del cumplimiento de las obligaciones establecidas por los sujetos de aplicación. Para ello, cuando así se decida, esa delegación voluntaria del deber de informar habrá de formalizarse y registrarse mediante la suscripción de un acuerdo que así lo establezca.

Artículo 23.–Relaciones institucionales externas.

1.– La Agencia podrá establecer y mantener relaciones de cooperación y colaboración con entidades y organismos estatales e internacionales que desarrollen su actividad en el ámbito de la ciberseguridad.

2.– La Agencia actuará como interlocutor del sector público vasco ante foros, organismos y mecanismos de cooperación estatales e internacionales en ciberseguridad.

CAPÍTULO V
RECOGIDA DE DATOS

Artículo 24.–Requerimientos de información.

1.– La Agencia podrá requerir a los sujetos comprendidos en el artículo 2 la información que resulte necesaria para el adecuado ejercicio de sus funciones. Dichos requerimientos de información deberán estar debidamente motivados, ser proporcionales a la finalidad perseguida y limitarse a la información estrictamente necesaria para el cumplimiento de las funciones atribuidas a la Agencia.

2.– La información requerida podrá referirse a puntos de contacto específicos en materia de ciberseguridad, a las características de los sistemas, servicios y activos gestionados, al estado de su ciberseguridad, a la implantación de medidas de seguridad, a la gestión de riesgos, a la ocurrencia de incidentes de ciberseguridad, a las medidas aplicadas tras la notificación por parte de la Agencia de riesgos o amenazas, a la cadena de suministro o a otros elementos técnicos relevantes, en los términos y con el alcance que se determinen en cada caso.

3.– Los requerimientos de información no tendrán carácter sancionador ni implicarán, por sí mismos, la asunción por parte de la Agencia de funciones de control, inspección o supervisión que correspondan a otros órganos o autoridades, sin perjuicio de las obligaciones de colaboración que resulten aplicables conforme al ordenamiento jurídico.

4.– La información facilitada a la Agencia será utilizada exclusivamente para el ejercicio de sus funciones y tratada con carácter confidencial, adoptándose las medidas técnicas y organizativas necesarias para garantizar su adecuada protección, conservación y, en su caso, anonimización o agregación.

5.– Los requerimientos de información se atenderán en los plazos y formas que se establezcan, preferentemente por medios electrónicos, sin perjuicio de que puedan articularse mecanismos de colaboración y canales específicos para facilitar su remisión de forma segura.

Artículo 25.–Confidencialidad de la información facilitada.

1.– Las entidades que accedan a los servicios prestados por la Agencia deberán garantizar la confidencialidad de la información que reciban de ésta en el marco de dichos servicios, cuando dicha información tenga carácter sensible o su divulgación pueda comprometer la seguridad de los sistemas, servicios o activos afectados o de terceros afectados.

2.– La información facilitada por la Agencia se utilizará exclusivamente para las finalidades para las que haya sido proporcionada y no podrá ser comunicada a terceros ni difundida sin la autorización expresa de la Agencia, salvo en los supuestos previstos en la normativa aplicable.

3.– Las entidades destinatarias adoptarán las medidas técnicas y organizativas necesarias para proteger adecuadamente la información recibida, de conformidad con la normativa de seguridad de la información que les resulte aplicable.

4.– Lo dispuesto en este artículo se entenderá sin perjuicio de las obligaciones de colaboración, comunicación o puesta a disposición de la información que correspondan conforme al ordenamiento jurídico.

Artículo 26.–Obligación de secreto

1.– El personal al servicio de la Agencia, así como las personas o entidades que colaboren con esta en el ejercicio de sus funciones, estarán sujetos a la obligación de guardar secreto respecto de la información, datos, documentos, conocimientos o resultados a los que tengan acceso como consecuencia de su actividad, con independencia del soporte, formato o medio en que se encuentren.

2.– La obligación de secreto se extenderá, en particular, a la información relativa a la seguridad de los sistemas de información, a las vulnerabilidades, amenazas, incidentes de ciberseguridad, evidencias técnicas, configuraciones, medidas de protección, planes de continuidad, así como a cualesquiera otros extremos cuya divulgación pudiera comprometer la seguridad, la confidencialidad o el adecuado funcionamiento de los sistemas y servicios afectados.

3.– La obligación de secreto subsistirá aun después de finalizar la relación de servicio, contractual o de colaboración con la Agencia, sin perjuicio de las responsabilidades que pudieran derivarse de su incumplimiento conforme al ordenamiento jurídico.

CAPÍTULO VI
RÉGIMEN DE FUNCIONAMIENTO

Artículo 27.–Nivel de desarrollo necesario para el acceso a los servicios de la Agencia.

1.– La Agencia podrá determinar el nivel de desarrollo en ciberseguridad requerido a las entidades para el acceso a cada uno de los servicios que preste, de acuerdo con lo previsto en el Modelo de Ciberseguridad de Euskadi.

2.– A efectos de lo dispuesto en este artículo, el nivel de desarrollo se entenderá como el grado de implantación de las capacidades, medidas y controles de ciberseguridad definidos en el Modelo de Ciberseguridad de Euskadi, evaluado conforme a los mecanismos que se establezcan al efecto.

3.– Con carácter general, para acceder a los servicios de la Agencia será necesario que las entidades interesadas hayan realizado, al menos, una evaluación de su nivel de desarrollo en ciberseguridad, mediante un proceso de autoevaluación, en los términos que determine la Agencia.

4.– La Agencia podrá vincular cada servicio a un nivel de desarrollo, estableciendo requisitos diferenciados en función de la naturaleza del servicio, su complejidad técnica, su impacto potencial o los riesgos asociados, de conformidad con el Modelo de Ciberseguridad de Euskadi.

5.– La evaluación del nivel de desarrollo tendrá por finalidad:

a) Facilitar una prestación adecuada y eficaz de los servicios de la Agencia.
b) Garantizar una aplicación proporcionada y coherente del Modelo de Ciberseguridad de Euskadi.
c) Orientar a las entidades en la mejora progresiva de sus capacidades de ciberseguridad.

6.– Lo dispuesto en este artículo se entiende sin perjuicio de que la Agencia pueda prestar servicios de acompañamiento, apoyo o capacitación destinados a facilitar a las entidades la realización de la autoevaluación o la mejora de su nivel de desarrollo.

Artículo 28.–Organización del modelo de gestión de incidentes de ciberseguridad

1.– Corresponde a la Agencia, en materia de gestión de incidentes de ciberseguridad lo establecido en el Capítulo III.

2.– Corresponde a cada entidad, sin perjuicio de lo establecido en la regulación vigente en cada caso:

a) Definir su propia metodología de gestión de ciberataques e incidentes de ciberseguridad.
b) Establecer los criterios y mecanismos necesarios para que dicha metodología de gestión de incidentes de ciberseguridad y ciberataques se articule de manera adecuada.
c) Mantener los medios materiales y personales necesarios para la correcta gestión de los incidentes de ciberseguridad y ciberataques que se puedan producir.
d) Designar a una o varias personas como interlocutoras con la Agencia en relación con la gestión de ciberataques e incidentes de ciberseguridad, y establecer los puntos de contacto necesarios para ello.
e) Atender y responder diligentemente las notificaciones de alertas de ciberseguridad recibidas desde la Agencia.
f) Gestionar los incidentes de ciberseguridad y ciberataques que se produzcan.
g) Reportar diligentemente a la Agencia los incidentes de ciberseguridad y ciberataques sufridos.
h) Resolver los incidentes de ciberseguridad y ciberataques sufridos.
i) Realizar ejercicios o simulacros periódicos, con el fin de comprobar la eficacia de la metodología de gestión de ciberataques e incidentes de ciberseguridad.

3.– Cada entidad comunicará formalmente a la Agencia la identificación de la o las personas interlocutoras con ésta en materia de gestión de incidentes de ciberseguridad y notificará a la Agencia cualquier cambio en la designación de interlocutores o puntos de contacto.

Artículo 29.–Soporte a sectores esenciales

La Agencia prestará soporte específico a los sectores esenciales y a otros ámbitos especialmente sensibles de la Comunidad Autónoma de Euskadi, atendiendo a la naturaleza crítica de los servicios que prestan y a los riesgos asociados a su funcionamiento, pudiendo adaptar a sus características y necesidades las actuaciones y servicios previstos en el presente Decreto.

Artículo 30.–Salvaguardas en la ejecución de actuaciones técnicas

1.– Las actuaciones técnicas de la Agencia que puedan suponer un riesgo para los sistemas de información se llevarán a cabo con carácter planificado, controlado y proporcional.

2.– Dichas actuaciones se realizarán exclusivamente sobre sistemas, activos o entornos respecto de los cuales exista habilitación, autorización o solicitud expresa por parte de la entidad responsable, en los términos que se establezcan, y con pleno respeto a las competencias, responsabilidades y obligaciones que correspondan a dicha entidad.

3.– La Agencia no será responsable de los efectos derivados de las actuaciones técnicas que puedan suponer un riesgo para los sistemas de información realizadas conforme a lo previsto en este Decreto, sin perjuicio de las responsabilidades que pudieran derivarse del incumplimiento del marco jurídico aplicable o de las condiciones expresamente establecidas para su ejecución.

4.– En todo caso, la Agencia adoptará las medidas técnicas y organizativas necesarias para minimizar el impacto de las actuaciones realizadas y para preservar la confidencialidad, integridad y disponibilidad de la información tratada, así como para garantizar la adecuada documentación y trazabilidad de las actuaciones llevadas a cabo.

Artículo 31.–Responsabilidad de las partes

La prestación de servicios por parte de la Agencia no implicará la asunción de la gestión directa, administración, operación, mantenimiento ni responsabilidad sobre los sistemas de las entidades. Corresponderá a cada una la implantación y gestión de las medidas de seguridad necesarias en el ámbito de sus competencias.

Artículo 32.–Seguimiento de las actividades

En el marco de la prestación de sus servicios la Agencia podrá efectuar el seguimiento de las actividades y solicitar a las entidades la información necesaria sobre las medidas adoptadas, con el fin de verificar su eficacia.

TÍTULO III
PLANES DE CONTINUIDAD EN MATERIA DE CIBERSEGURIDAD EN EL MARCO DE LA AUTOPROTECCIÓN

CAPÍTULO I
FINALIDAD Y OBLIGACIONES

Artículo 33.–Objeto

Es objeto del presente título regular la obligación de elaborar y mantener planes de continuidad en materia de ciberseguridad en determinadas actividades, centros, establecimientos, espacios, instalaciones o dependencias prioritarias de la Comunidad Autónoma de Euskadi, como instrumento específico para hacer frente a eventos e incidentes de ciberseguridad susceptibles de generar situaciones de riesgo para las personas, sus bienes y el patrimonio colectivo, de manera que puedan resultar afectados de forma especialmente grave por situaciones de este carácter.

Artículo 34.–Ámbito de aplicación

1.– Las obligaciones previstas en este título serán de aplicación a las actividades, centros, establecimientos, espacios, instalaciones o dependencias de los sectores cuya operación resulte necesaria para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de la ciudadanía, así como para el eficaz funcionamiento de las Instituciones de Euskadi y de sus Administraciones Públicas, cuando alguno de sus centros, establecimientos o infraestructuras se encuentre sujeto a lo dispuesto en el Decreto 277/2010, de 2 de noviembre, modificado por el Decreto 21/2019, de 12 de febrero, por el que se regulan las obligaciones de autoprotección exigibles a determinadas actividades, centros o establecimientos para hacer frente a situaciones de emergencia.

2.– Los sectores a los que se refiere el apartado anterior se determinan en el Anexo I del presente decreto, sin perjuicio de que puedan ser actualizados, en virtud de:

a) La transposición que se efectúe de la Directiva (UE) 2022/2555, del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2).
b) La aprobación o modificación de cualquier otra regulación relacionada con estos sectores en materia de ciberseguridad.

3.– La Agencia podrá exigir la elaboración e implantación de planes de continuidad en materia de ciberseguridad a los titulares de actividades, centros, establecimientos, espacios, instalaciones o dependencias no incluidas en los apartados anteriores, cuando concurran circunstancias de especial riesgo, vulnerabilidad o impacto potencial sobre la seguridad de las personas, los servicios esenciales o el interés público.

4.– Los titulares de actividades, centros, establecimientos o infraestructuras no incluidos en los apartados anteriores podrán elaborar voluntariamente un plan de continuidad en materia de ciberseguridad conforme a lo previsto en este Decreto.

Artículo 35.–Criterios de aplicación

Las obligaciones previstas en este capítulo tendrán carácter de mínimos exigibles y serán de aplicación supletoria en aquellos aspectos no regulados por la normativa sectorial específica que resulte de aplicación.

Artículo 36.–Obligaciones

1.– Los titulares de las actividades, centros, establecimientos o infraestructuras sujetas a este título deberán cumplir las siguientes obligaciones:

a) Elaborar y mantener un Plan de Continuidad en materia de Ciberseguridad, de conformidad con las directrices de la Agencia, cuyo contenido mínimo se establece en el siguiente capítulo.
b) Inscribir en el Registro de Autoprotección de Euskadi las referencias de los Planes de Continuidad en materia de ciberseguridad vinculados en cada caso.
c) Inscribir en el Registro de Planes de continuidad en materia de ciberseguridad de Euskadi, como datos de registro, los siguientes:
   - Las referencias a los planes de autoprotección vinculados.
   - Los datos específicos para la protección en ciberseguridad.
   - Los metadatos correspondientes al Plan de continuidad en materia de ciberseguridad, conforme a lo establecido en el Anexo II del presente Decreto.
   - Una declaración responsable del titular relativa a la implantación del Plan de Continuidad en materia de ciberseguridad.
d) Desarrollar las actuaciones necesarias para la implantación, el mantenimiento y la mejora continua de la eficacia del Plan de Continuidad en materia de Ciberseguridad.
e) Designar a las personas físicas responsables de la ciberseguridad de la actividad, cuando estas sean distintas del titular.
f) Informar y formar al personal a su servicio en los contenidos del Plan de Continuidad en materia de Ciberseguridad, en función de sus responsabilidades y de su nivel de exposición al riesgo.
g) Mantener los medios materiales y personales necesarios para la correcta aplicación del Plan de Continuidad en materia de Ciberseguridad.
h) Aplicar las medidas previstas en el Plan de Continuidad en materia de Ciberseguridad ante la ocurrencia de eventos o incidentes de ciberseguridad.
i) Realizar ejercicios o simulacros periódicos, con el fin de comprobar la eficacia del plan y el grado de preparación del personal implicado.
j) Notificar a la Agencia los incidentes relativos a ciberseguridad definidos en el Anexo III del presente Decreto, directamente a la Agencia o a través del Centro de Coordinación de Emergencias de Euskadi (SOS Deiak-112), sin perjuicio de cualquier otra notificación que deba realizarse por requerimiento legal o regulatorio. Las notificaciones posteriores se realizarán directamente a la Agencia. La taxonomía de los incidentes de ciberseguridad a reportar a la Agencia, así como los canales establecidos para ello serán determinados mediante Resolución de la Dirección General de la Agencia, que se publicará en el Boletín Oficial del País Vasco.

2.– Corresponden a la autoridad competente en materia de emergencias y protección civil las siguientes obligaciones en relación con los planes de continuidad en materia de ciberseguridad:

a) Habilitar en el Registro de Autoprotección de Euskadi un apartado específico y exclusivo para las actividades, centros, establecimientos, espacios, instalaciones o dependencias sujetas a este título, en el que deba registrarse la referencia a las entradas correspondientes del Registro de Planes de Continuidad en materia de ciberseguridad de Euskadi.
b) Informar a la Agencia del sector al que pertenecen los titulares de las actividades, centros, establecimientos, espacios, instalaciones o dependencias sujetas a este título.

c) Remitir a la Agencia las notificaciones de incidentes relativos a ciberseguridad recibidas a través del Centro de Coordinación de Emergencias de Euskadi (SOS Deiak-112).

3.– Corresponden a la Agencia las siguientes obligaciones:

a) Comprobar la obligatoriedad de elaborar y disponer de un Plan de Continuidad en materia de Ciberseguridad por parte de los titulares de las actividades, centros, establecimientos, espacios, instalaciones o dependencias sujetas a este título.
b) Supervisar e inspeccionar los datos específicos para la protección en ciberseguridad registrados en el Registro de Planes de Continuidad en materia de ciberseguridad de Euskadi.
c) Supervisar e inspeccionar los metadatos del Plan de Continuidad en materia de Ciberseguridad elaborado por los titulares de las actividades, centros, establecimientos, espacios, instalaciones o dependencias sujetas a este título.

CAPÍTULO II
PLANES DE CONTINUIDAD EN MATERIA DE CIBERSEGURIDAD

Artículo 37.–El Plan de continuidad en materia de ciberseguridad

1.– El Plan de continuidad en materia de ciberseguridad es el documento que define cómo una actividad, centro, establecimiento, espacio, instalación o dependencia seguirá operando ante una interrupción significativa motivada por un incidente de ciberseguridad, con el propósito de evitar que dicho incidente paralice la actividad y asegurar que sus actividades principales se sigan desarrollando.

2.– La elaboración, implantación, mantenimiento y revisión del Plan de continuidad en materia de ciberseguridad es responsabilidad del titular de la actividad.

Artículo 38.–Estructura y contenido

1.– El Plan de continuidad en materia de ciberseguridad aborda la identificación y evaluación de los riesgos de ciberseguridad, las acciones y medidas necesarias para la prevención y control de dichos riesgos, así como las medidas de protección y otras actuaciones a adoptar en caso de que se produzca un incidente de ciberseguridad que pueda paralizar la actividad, centro, establecimiento, espacio, instalación o dependencia.

2.– Los contenidos mínimos del Plan de continuidad en materia de ciberseguridad serán los siguientes:

a) Planificación y un control operacional: se deben planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos propios de la actividad, centro, establecimiento, espacio, instalación o dependencia, e implementar las acciones destinadas a abordar los riesgos y oportunidades de ciberseguridad.
b) Análisis de impacto y evaluación de riesgos de ciberseguridad: se debe implementar y mantener un proceso para analizar el impacto operacional y evaluar los riesgos de interrupción que establezca el contexto, defina criterios y evalúe el impacto potencial de una interrupción motivada por un incidente de ciberseguridad.
c) Estrategias y soluciones de continuidad: se deben identificar y seleccionar estrategias de continuidad operacional basadas en los resultados del análisis de impacto y la evaluación de riesgos de ciberseguridad. Las estrategias de continuidad podrán estar compuestas por una o más soluciones.
d) Planes y procedimientos de continuidad: se debe implementar y mantener una estructura que permita la advertencia y comunicación oportunas a las partes interesadas relevantes, y proporcionar pautas de actuación para administrar la organización durante una interrupción operacional provocada por un incidente de ciberseguridad. Los planes

y procedimientos se utilizarán cuando sea necesario para ejecutar soluciones de continuidad.

e) Programa de ejercicios: se debe implementar y mantener un programa de ejercicios y pruebas para validar con el tiempo la efectividad de las estrategias y soluciones de continuidad.

3.– Con la finalidad de facilitar el desarrollo de los Planes de Continuidad en materia de ciberseguridad, la Agencia publicará y mantendrá actualizada una guía con la estructura del documento.

Artículo 39.–Criterios para la implantación del Plan

1.– La implantación del Plan de continuidad en materia de ciberseguridad comprenderá, al menos, la formación y capacitación del personal y la provisión de los medios y recursos precisa para la aplicabilidad del plan.

2.– A tal fin el Plan de continuidad en materia de ciberseguridad atenderá a los siguientes criterios:

a) Información previa: Se establecerán mecanismos de información para el personal acerca tanto de los riesgos de ciberseguridad como del propio Plan de continuidad en materia de ciberseguridad.
b) Formación teórica y práctica del personal asignado al Plan de continuidad en materia de ciberseguridad, estableciendo un adecuado programa de actividades formativas.
c) Definición, provisión y gestión de los medios y recursos económicos necesarios.

Artículo 40.–Criterios para el mantenimiento de la eficacia del Plan

1.– Se establecerá un adecuado programa de actividades formativas periódicas para asegurar el mantenimiento de la formación teórica y práctica del personal asignado al Plan de continuidad en materia de ciberseguridad, estableciendo sistemas o formas de comprobación de que dichos conocimientos han sido adquiridos.

2.– Existirá un programa de mantenimiento de los medios y recursos materiales y económicos necesarios.

3.– Para evaluar los Planes de continuidad en materia de ciberseguridad y asegurar su eficacia y operatividad en caso de incidentes de ciberseguridad se realizarán pruebas, ejercicios o simulacros, con la periodicidad mínima que fije el propio plan, y en todo caso, al menos una vez al año evaluando, sus resultados. Estas pruebas tendrán como objetivo la verificación y comprobación de:

a) La eficacia de la organización para responder ante un incidente de ciberseguridad.
b) La capacitación del personal adscrito a la organización de respuesta.
c) El entrenamiento de todo el personal en la respuesta frente a un incidente de ciberseguridad.
d) La suficiencia e idoneidad de los medios y recursos asignados.
e) La adecuación de los procedimientos de actuación.

4.– Los ejercicios o simulacros implicarán la activación total o parcial de las acciones contenidas en el Plan de continuidad en materia de ciberseguridad. En los ejercicios, simulacros y pruebas se ejercitarán, principalmente, los procedimientos de actuación internos del establecimiento.

5.– De las actividades de mantenimiento de la eficacia del Plan de continuidad en materia de ciberseguridad se conservará información sobre las mismas a disposición de la Agencia, así como de los informes de evaluación realizados.

Artículo 41.–Vigencia del plan y criterios para su actualización y revisión.

El Plan de continuidad en materia de ciberseguridad tendrá vigencia indeterminada, se mantendrá adecuadamente actualizado y se revisará siempre que la actividad o las

infraestructuras se vean modificadas respecto a la redacción inicial o como consecuencia de las conclusiones de la realización de un ejercicio, simulacro o prueba y, al menos, con una periodicidad no superior a tres años.

CAPÍTULO III
REGISTRO DE PLANES DE CONTINUIDAD EN MATERIA DE CIBERSEGURIDAD

Artículo 42.–Creación

1.– El Registro de Planes de Continuidad en materia de ciberseguridad se crea con la finalidad de inscribir los datos relevantes de los mismos, así como otras medidas de ciberseguridad que dispongan los sujetos obligados, para facilitar a la Agencia el acceso a la información necesaria para el ejercicio de sus competencias, así como para permitir el control administrativo registral y las actuaciones de supervisión e inspección en materia de ciberseguridad por los órganos competentes.

2.– El Registro se adscribe a la Agencia Vasca de Ciberseguridad, que será la encargada de gestionarlo.

Artículo 43.–Naturaleza, funciones y estructura del Registro

1.– La inscripción en el Registro será obligatoria para los titulares de las actividades, centros, establecimientos, espacios, instalaciones o dependencias sujetas a la obligación de disponer de un Plan de Continuidad en materia de Ciberseguridad conforme a este Decreto y a la normativa que resulte de aplicación.

2.– El Registro de Planes de Continuidad en materia de ciberseguridad no tendrá carácter público. Tendrán acceso a sus datos, exclusivamente, las personas titulares de las actividades, centros, establecimientos, espacios, instalaciones o dependencias, respecto de sus propios datos registrales, así como la Agencia en los términos que se expresan en este Decreto.

3.– El Registro tendrá las siguientes funciones:

a) Inscribir los datos relativos a los planes de continuidad en materia de ciberseguridad y asignar un número registral.
b) Archivar, custodiar y preservar electrónicamente la documentación registral.
c) Facilitar el acceso electrónico seguro a los datos del Registro a los servicios públicos competentes.
d) Facilitar a los titulares el acceso electrónico seguro a sus respectivos datos registrales.
e) Requerir la actualización periódica de los datos registrales.

4.– El Registro constará de tres secciones diferenciadas:

a) Sección de referencia a los planes de autoprotección.
b) Sección de datos específicos para la protección en ciberseguridad.
c) Sección de planes de continuidad en materia de ciberseguridad.

5.– El Registro se organizará en hojas registrales para cada titular de actividad, centro, establecimiento, espacio, instalación o dependencia en su ámbito de aplicación.

Artículo 44.–Sección de referencia a los planes de autoprotección

Esta sección reflejará los datos de referencia que permitan vincular los planes de continuidad en materia de ciberseguridad con cada una de las actividades, centros, establecimientos, espacios, instalaciones o dependencias correspondientes para las que se haya desarrollado su correspondiente Plan de Autoprotección, recogido en el Registro de Planes de Autoprotección regulado por el Decreto 277/2010, de 2 de noviembre, por el que se regulan

las obligaciones de autoprotección exigibles a determinadas actividades, centros o establecimientos para hacer frente a situaciones de emergencia.

Artículo 45.–Sección de datos específicos para la protección en ciberseguridad

1.– Esta sección, dedicada a los datos específicos para la protección en ciberseguridad, recogerá:

a) Los datos de contacto del titular en caso de ciberincidente.

b) Las medidas de seguridad y continuidad con las que cuenta el titular.

c) Las principales características de los sistemas de información.

2.– En caso de que un mismo titular de actividad, centro, establecimiento, espacio, instalación o dependencia, en su ámbito de aplicación, decida aplicar diferentes medidas de protección en ciberseguridad para distintas actividades, centros, establecimientos, espacios, instalaciones o dependencias, se creará una hoja registral para cada caso, de manera que en cada hoja registral queden vinculados los datos específicos para la protección en ciberseguridad de cada una de las actividades, centros, establecimientos, espacios, instalaciones o dependencias correspondientes para las que se haya desarrollado su respectivo Plan de Autoprotección.

Artículo 46.–Sección de planes de continuidad en materia de ciberseguridad

1.– Esta sección recogerá únicamente los metadatos necesarios para acreditar la existencia, implantación, vigencia y mantenimiento de los contenidos mínimos del Plan de Continuidad en materia de Ciberseguridad, sin incorporar su contenido técnico detallado. De forma específica, se reflejará la información detallada en el Anexo II del presente Decreto.

2.– En caso de que un mismo titular de actividad, centro, establecimiento, espacio, instalación o dependencia, en su ámbito de aplicación, decida desarrollar múltiples planes de continuidad en materia de ciberseguridad, se creará una hoja registral para cada caso, de manera que en cada hoja registral queden vinculadas cada una de las actividades, centros, establecimientos, espacios, instalaciones o dependencias correspondientes para las que se haya desarrollado su respectivo Plan de Autoprotección.

3.– Se inscribirán igualmente las comunicaciones relativas a revisiones, actualizaciones o modificaciones relevantes del plan.

Artículo 47.–Organización y funcionamiento del Registro

La Agencia establecerá los formularios normalizados, los criterios técnicos y los procedimientos necesarios para el funcionamiento del Registro de Planes de Continuidad en materia de ciberseguridad, que asegurarán tanto el acceso telemático de los sujetos interesados, como la confidencialidad, seguridad e integridad de los datos.

Artículo 48.–Procedimiento de inscripción

1.– Los titulares de cada actividad, centro, establecimiento, espacio, instalación o dependencia obligadas a disponer de un Plan de Continuidad en materia de Ciberseguridad deberán solicitar su inscripción en el Registro de Planes de Continuidad en materia de ciberseguridad, comunicando los datos inscribibles acompañados de la documentación preceptiva que se refleja en este Decreto.

2.– El procedimiento registral se tramitará únicamente en soporte electrónico, para lo que se habilitarán los mecanismos y aplicaciones dentro de la sede electrónica del Gobierno Vasco, para que se pueda presentar la solicitud por vía electrónica, adjuntando la documentación precisa en formatos admitidos, previa identificación de la persona interesada mediante sistemas basados en certificados electrónicos de firma electrónica expedidos por prestadores

incluidos en la lista de confianza de prestadores de servicios de certificación, así como sistemas de clave concertada.

3.– La inscripción producirá efectos meramente declarativos de los datos que consten en el registro, no confiere por sí misma una aprobación o validación administrativa de la exactitud, actualidad o corrección de los datos declarados por los sujetos obligados.

Artículo 49.–Obligaciones de los titulares inscritos

1.– Los titulares de las actividades, centros, establecimientos, espacios, instalaciones o dependencias inscritas deben mantener permanentemente actualizados los datos incorporados al registro. Para ello deberán notificar a la Agencia las modificaciones sobrevenidas, aportando la información correspondiente, o bien podrán acceder telemáticamente previa identificación electrónica a sus datos registrales con el fin de comprobarlos y, en su caso, actualizarlos.

2.– Cuando una actividad, centro, establecimiento, espacio, instalación o dependencia presente un especial riesgo o vulnerabilidad, por sí misma o por hallarse en entornos de especial riesgo o vulnerabilidad, la Agencia, como órgano encargado del Registro, podrá requerir de los titulares de la actividad que presenten la documentación y la información adicional que se considere necesaria, adecuada y proporcionada a las finalidades del Registro, pudiendo llegar a solicitarse, si fuese necesario, el contenido íntegro del Plan de Continuidad en materia de ciberseguridad.

Artículo 50.–Cancelación de la inscripción registral

Finalizada la actividad que se desarrolla en el centro, establecimiento, espacio, instalación o dependencia cuyo Plan de Continuidad en materia de Ciberseguridad haya sido inscrito en el Registro, el titular estará obligado a solicitar la cancelación de la anotación en el plazo máximo de un mes desde el cese de la actividad.

DISPOSICIONES ADICIONALES

Disposición adicional primera. Catálogo de servicios de la Agencia.

La Agencia desarrollará y actualizará su Catálogo de Servicios, como instrumento de carácter operativo destinado a concretar y ordenar los servicios que se prestan en el ejercicio de las funciones atribuidas a la Agencia.

Disposición adicional segunda. Creación del Registro de Planes de Continuidad en materia de ciberseguridad.

En el plazo de doce meses desde la entrada en vigor del presente Decreto, la Agencia creará el Registro de Planes de Continuidad en materia de ciberseguridad de Euskadi.

DISPOSICIONES TRANSITORIAS

Disposición transitoria. Plazos de adaptación.

Las entidades que integran el sector público vasco dispondrán de un plazo máximo de veinticuatro meses, contados desde la entrada en vigor del presente decreto, para adecuar progresivamente su marco interno de ciberseguridad al Modelo de Ciberseguridad de Euskadi.

DISPOSICIÓN DEROGATORIA

Disposición derogatoria única.

Queda derogada la Orden de 7 de junio de 2024, del Vicelehendakari Primero y Consejero de Seguridad, por la que se regula la elaboración de planes de continuidad en materia de ciberseguridad para ciertas actividades sujetas a la norma vasca de autoprotección y cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en este decreto.

DISPOSICIONES FINALES

Disposición final. Entrada en vigor.

El presente Decreto entrará en vigor el día siguiente al de su publicación en el Boletín Oficial del País Vasco.

ANEXO I CATEGORIZACIÓN DE SECTORES

Los sectores a los que hace referencia el artículo 34 del presente Decreto son los siguientes:

1. Energía
    a) Electricidad
    b) Sistemas urbanos de calefacción y de refrigeración
    c) Crudo
    d) Gas
    e) Hidrógeno
2. Transporte y logística
    a) Transporte aéreo
    b) Transporte por ferrocarril
    c) Transporte marítimo y fluvial
    d) Transporte por carretera
3. Finanzas, banca e infraestructuras de los mercados financieros
4. Sector sanitario
5. Agua potable
6. Aguas residuales
7. Residuos urbanos e industriales
8. Infraestructura digital
9. Gestión de servicios de TIC y proveedores de servicios digitales
10. Administración pública
11. Espacio
12. Servicios postales y de mensajería
13. Fabricación, producción y distribución de sustancias y mezclas químicas
14. Producción, transformación y distribución de alimentos (cadena alimentaria)
15. Fabricación
    a) Fabricación de productos sanitarios
    b) Fabricación de productos informáticos, electrónicos y ópticos
    c) Fabricación de material eléctrico
    d) Fabricación de maquinaria y equipo
    e) Fabricación de vehículos de motor, remolques y semirremolques
    f) Fabricación de otro material de transporte
16. Investigación
17. Agentes económicos relevantes

ANEXO II DATOS ESPECÍFICOS PARA LA PROTECCIÓN EN CIBERSEGURIDAD

Los metadatos correspondientes a los Planes de Continuidad en materia de ciberseguridad deberán contener la siguiente información:

a) Identificación general del Plan:
   - Identificación del titular de la actividad.
   - Identificación de las actividades, centros, establecimientos, espacios, instalaciones o dependencias asociadas.
   - Sector de actividad conforme al Anexo I.
   - Identificación de la persona responsable del Plan de Continuidad en materia de Ciberseguridad.
   - Fecha de elaboración del plan.
   - Fecha de implantación efectiva.
   - Fecha de la última revisión.
   - Periodicidad prevista de revisión.

b) Planificación y control operacional
   - Declaración de existencia de una planificación y control operacional del Plan de Continuidad en materia de Ciberseguridad.
   - Alcance general del plan en relación con los servicios, procesos o sistemas cubiertos.
   - Existencia de procedimientos documentados de seguimiento y control.
   - Fecha de la última verificación interna del control operacional.

c) Análisis de impacto del negocio y evaluación de riesgos
   - Declaración de existencia de un análisis de impacto
   - Declaración de existencia de una evaluación de riesgos de ciberseguridad.
   - Fecha de realización o de la última actualización del análisis y de la evaluación.
   - Referencia a la metodología empleada.
   - Identificación agregada de los procesos, servicios o sistemas críticos.

d) Estrategias y soluciones de continuidad del negocio
   - Declaración de existencia de estrategias de continuidad del negocio definidas.
   - Tipología general de las estrategias adoptadas.
   - Declaración de alineación de las estrategias con los resultados del análisis de impacto del negocio.
   - Fecha de aprobación o de la última actualización de las estrategias.

e) Planes y procedimientos de continuidad del negocio
   - Declaración de existencia de planes y procedimientos de continuidad del negocio.
   - Existencia de un plan de comunicación ante incidentes o situaciones de crisis.
   - Existencia de procedimientos de activación del plan.
   - Existencia de procedimientos de recuperación.
   - Identificación de las personas responsables de la activación y coordinación.

f) Programa de ejercicios y pruebas
   - Declaración de existencia de un programa de ejercicios, simulacros y pruebas del Plan de Continuidad en materia de Ciberseguridad.
   - Periodicidad prevista de los ejercicios, simulacros o pruebas.
   - Fecha de realización del último ejercicio, simulacro o prueba.
   - Tipología del último ejercicio, simulacro o prueba realizado.
   - Declaración de revisión del plan tras la realización del ejercicio, simulacro o prueba.

ANEXO III INCIDENTES DE CIBERSEGURIDAD QUE DEBEN SER NOTIFICADOS

Los incidentes relativos a ciberseguridad a notificar mencionados en este Decreto deben entenderse así definidos:

1.– Se notificarán los incidentes que puedan tener efectos perturbadores significativos en los servicios, considerándose a tales efectos los clasificados dentro de la siguiente taxonomía:

a) Contenido dañino: infección de algún sistema con malware.

b) Intrusión: compromiso de un sistema en el que el atacante ha conseguido acceso.

c) Disponibilidad: incidente en el que la prestación del servicio se vea afectada.

d) Compromiso de la información: incidente en el que se haya tenido acceso no autorizado a la información de la organización.

e) Fraude: incidente que mediante el uso de medios electrónicos desemboque en un daño económico, material o de cualquier otra naturaleza.

2.– La entidad remitirá, en tiempo y forma, aquellas notificaciones inicial, intermedia y final requeridas de acuerdo con la siguiente ventana temporal de reporte.

a) La notificación inicial es una comunicación consistente en poner en conocimiento y alertar de la existencia de un incidente.

b) La notificación intermedia es una comunicación mediante la que se actualizarán los datos disponibles en ese momento relativos al incidente comunicado.

c) La notificación final es una comunicación final mediante la que se amplían y confirman los datos definitivos relativos al incidente comunicado.

i. Notificación inicial: Inmediata.

ii. Notificación intermedia: 24-48 horas.

iii. Notificación final: 20 días.

3.– Los tiempos reflejados en la tabla para la «notificación intermedia» y la «notificación final» tienen como referencia el momento de remisión de la «notificación inicial». La «notificación inicial» tiene como referencia de tiempo el momento de tener conocimiento del incidente.

4.– La entidad comunicará, en la notificación inicial, toda la información relativa al incidente de la que tenga conocimiento en ese momento, datos que se irán actualizando en las notificaciones intermedias y siendo posteriormente preceptiva una notificación final del incidente. En todas las notificaciones se proporcionará al menos toda la información aquí indicada:

a) Asunto: Frase que describa de forma general el incidente. Este campo lo heredarán todas las notificaciones asociadas al incidente.

b) Sector de actividad: Energía, transporte, financiero, etc. (conforme al Anexo I).

c) Fecha y hora del incidente: Indicar con la mayor precisión posible cuándo ha ocurrido el incidente.

d) Fecha y hora de detección del incidente: Indicar con la mayor precisión posible cuándo se ha detectado el incidente.

e) Tipo de notificación: Inicial, intermedia o final.

f) Fecha y hora de la notificación: Indicar cuándo se está notificando.

g) Descripción: Describir con detalle lo sucedido.

h) Recursos tecnológicos afectados: Indicar la información técnica sobre el número y tipo de activos afectados por el incidente, incluyendo direcciones IP, sistemas operativos, aplicaciones, versiones…

i) Origen del incidente: Indicar la causa del incidente si se conoce. Apertura de un fichero sospechoso, conexión de un dispositivo USB, acceso a una página web maliciosa, etc.

j) Taxonomía (clasificación): Posible clasificación y tipo de incidente en función de la taxonomía descrita.

k) Plan de acción y contramedidas: Actuaciones realizadas hasta el momento en relación con el incidente. Indicar el Plan de acción seguido junto con las contramedidas implantadas.

l) Afectación: Indicar si el afectado es una empresa o un particular, y las afectaciones según el nivel de impacto asignado.

m) Impacto económico estimado (Si se conoce): Costes asociados al incidente, tanto de carácter directo como indirecto.

n) Extensión geográfica (Si se conoce): Local, autonómico, nacional, supranacional, etc.

o) Daños reputacionales (Si se conocen): Afectación a la imagen corporativa del operador.

p) Adjuntos: Indicar la relación de documentos adjuntos que se aportan para ayudar a conocer la causa del problema o a su resolución (capturas de pantalla, ficheros de registro de información, correos electrónicos, etc.).

q) Regulación afectada: ENS / RGPD / Otros.

5.– La notificación de un incidente de ciberseguridad no excluye ni sustituye la notificación que de los mismos hechos deba realizarse a otros organismos conforme a su normativa específica.

6.– Asimismo, la Agencia Vasca de Ciberseguridad podrá proporcionar información que contribuya a la prevención, detección y respuesta de incidentes de ciberseguridad.