EUSKO JAURLARITZA GOBIERNO VASCO

SEGURTASUN SAILA
Babes Zibileko Sailburuordetza
Larrialdiei Aurre Egiteko eta
Meteorologiako Zuzendaritza

DEPARTAMENTO DE SEGURIDAD
Viceconsejería de Protección Civil
Dirección de Atención de Emergencias y
Meteorología

Procedimiento de configuración del Plan de Protección Civil de Euskadi – Larrialdiei Aurre Egiteko Bidea (LABI) frente a una emergencia de ciberseguridad de gran escala

Informado favorablemente en el Pleno de la Comisión de Protección Civil de Euskadi de 16 de diciembre de 2025

Se informa en Consejo de Gobierno de 10 de febrero de 2026

ÌNCIDE

CONTEXTO Y JUSTIFICACIÓN

El incremento exponencial en la frecuencia, complejidad y consecuencias de los incidentes de ciberseguridad en todo el mundo ha generado un nuevo paradigma de riesgo. Las experiencias acumuladas tanto en el ámbito estatal como internacional, especialmente a partir de incidentes como los ataques a servicios básicos en Estonia (2007), Ucrania (2015-2017), o el caso global del ransomware WannaCry (2017), han puesto de manifiesto que este tipo de amenazas pueden alcanzar una magnitud que desborde las capacidades sectoriales provocando una emergencia que pueda poner en riesgo a la población y requiera una respuesta multidimensional, tanto desde el punto de vista técnico como organizativo, político, social y de protección civil.

Es fundamental reconocer el creciente impacto de los ciberincidentes en las sociedades avanzadas y abordarlos desde la perspectiva de la protección civil. Ello permite, sin necesidad de modificar los planes de autoprotección ya existentes, incorporar los conocimientos adquiridos en los últimos años y disponer de procedimientos específicos que refuercen la capacidad de respuesta coordinada ante un incidente de gran escala derivado de un ciberataque. En este sentido, el Plan Territorial de Protección Civil de Euskadi – *Larrialdiei Aurre Egiteko Bidea*, en adelante LABI, como marco organizativo general y plan director para emergencias de especial gravedad, constituye una referencia estratégica que puede albergar procedimientos específicos, siempre respetando su naturaleza generalista.

En este contexto, los ciberincidentes de gran magnitud presentan características que los hacen susceptibles de ser considerados como emergencias de protección civil: la posibilidad de afectar simultáneamente a sistemas sanitarios, energéticos, logísticos, de seguridad, financieros o de comunicación; la velocidad de propagación del daño; la dificultad de atribución inmediata del origen; y el impacto potencial sobre la ciudadanía, así como sobre el orden público. Por tanto, sin necesidad de configurar un nuevo marco normativo específico, resulta pertinente reflexionar sobre los aprendizajes y posibilidades que ofrece el actual LABI para garantizar una respuesta coordinada ante una eventual emergencia de este tipo.

De hecho, en las últimas décadas se ha reforzado el enfoque integral de la gestión de emergencias, incorporando el principio de "resiliencia sistémica", en consonancia con las directrices de organismos como la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el Centro Europeo de Ciberdelincuencia de Europol (EC3), el Centro Criptológico Nacional (CCN) o el Instituto Nacional de Ciberseguridad (INCIBE). La Estrategia de Ciberseguridad de la Unión Europea 2020 y el marco español de ciberseguridad recogen explícitamente la necesidad de reforzar la gobernanza en situaciones de emergencia cibernéticas, promoviendo ejercicios de simulación interinstitucionales y protocolos de colaboración público-privada. Sin embargo, en situaciones que excedan la capacidad de respuesta de los mecanismos ordinarios de

ciberseguridad y produzcan impactos generalizados, el LABI ofrece un marco de referencia para la coordinación de todas las administraciones y sectores implicados.

Cabe recordar que el LABI establece una arquitectura de respuesta articulada en torno a una dirección única y coordinada, con participación de todas las administraciones públicas vascas y la posibilidad de integrar las capacidades locales y estatales cuando así se requiera. Este modelo de gobernanza interinstitucional ha demostrado su utilidad durante la pandemia de Covid-19, permitiendo gestionar una emergencia sanitaria de carácter sistémico con impactos multisectoriales. Si bien las características de una pandemia y un ciberincidente difieren notablemente en su forma de manifestación, ambas comparten la necesidad de coordinación, adaptación rápida a escenarios cambiantes, comunicación efectiva a la población, y soporte técnico especializado para la toma de decisiones.

Así, aunque el LABI no contempla expresamente los ciberincidentes como una tipología diferenciada de emergencia, su marco flexible permite dar cabida, si fuese necesario, a situaciones excepcionales provocadas por estos. La experiencia adquirida en la gestión de emergencias recientes, como la pandemia y el cero eléctrico, ha puesto de manifiesto la importancia de contar con estructuras de asesoramiento técnico-científico, foros de coordinación interinstitucional y mecanismos de comunicación social creíbles y sostenidos en el tiempo. Estas enseñanzas podrían ser valiosas también ante un ciberincidente grave que afectara a los servicios básicos o al normal funcionamiento institucional.

Es importante señalar que, en el caso de Euskadi, la Estrategia Vasca de Ciberseguridad 2024-2029 y el Plan General de Seguridad Pública de Euskadi 2020-2025 ya identifican explícitamente el riesgo derivado de ciberataques como uno de los retos principales de seguridad en la próxima década. Esta visión está en consonancia con la Ley 17/2015, del Sistema Nacional de Protección Civil, que reconoce la necesidad de integrar los riesgos emergentes y fomentar una cultura de la prevención transversal. Del mismo modo, la Directiva (UE) 2022/2555 (NIS2), vigente desde octubre de 2024, profundiza en la obligación de los Estados miembros de disponer de mecanismos adecuados de gestión de incidencias cibernéticas a nivel nacional, subrayando la necesidad de planes de respuesta y coordinación estratégica.

La interdependencia tecnológica de los sistemas actuales implica que un ciberincidente relevante puede tener efectos dominó que trasciendan el ámbito sectorial y requerirán mecanismos de coordinación sólidos en los niveles local, autonómico, estatal e internacional.

Por otra parte, se constata la necesidad de fomentar una cultura de preparación y conciencia social sobre los riesgos cibernéticos, similar a la que se ha desarrollado en otros ámbitos de la protección civil. La experiencia demuestra que, al igual que en otras emergencias, la anticipación, la preparación, la formación continua y los ejercicios de simulación son elementos clave para mitigar el impacto y reducir los tiempos de respuesta. En este sentido, el LABI podría actuar, en caso de una emergencia excepcional, como un paraguas organizativo para canalizar de forma ordenada y coordinada las capacidades disponibles, sin necesidad de alterar su configuración legal ni de establecer nuevas estructuras.

En definitiva, ante el crecimiento exponencial de los riesgos asociados a los ciberincidentes, y sin que ello implique modificar el LABI ni crear figuras normativas nuevas, resulta conveniente reflexionar sobre cómo aprovechar su marco organizativo como base de referencia para la coordinación institucional en escenarios de emergencia cibernética grave. La experiencia acumulada en los últimos años, tanto en Euskadi como a nivel europeo, demuestra que la anticipación estratégica, la coordinación entre las distintas administraciones, el asesoramiento técnico y la comunicación transparente con la ciudadanía son pilares esenciales de una respuesta eficaz ante amenazas que, aunque invisibles, pueden tener consecuencias tangibles, generalizadas y duraderas.

1.INTRODUCCIÓN

El LABI se aprobó mediante el Decreto 153/1997, de 24 de junio, por el que se aprueba el LABI y se regulan los mecanismos de integración del sistema vasco de atención de emergencias. (Corrección de errores, BOPV nº 148, 06/08/1997) (Corrección de errores, BOPV nº 17, 27/01/1998) y modificado por Decreto 1/2015, de 13 de enero, por el que se aprueba la revisión extraordinaria del Plan de Protección Civil de Euskadi, «Larrialdiei Aurregiteko Bidea-Labi». (BOPV nº 14 de 22/01/2015).

Constituye el instrumento fundamental de ordenación de la gestión de emergencias de la Comunidad Autónoma de Euskadi y, en tal sentido, establece los criterios generales a los que debe ajustarse la planificación en Euskadi, así como el marco organizativo general o multirriesgo para hacer frente a las emergencias de tipo catastrófico, no sujetas a planificación especial, que requieran de una dirección o coordinación autonómica.

El objetivo del presente Procedimiento es concretar, ante una emergencia de ciberseguridad pública por ataque o incidente, y a la luz de la experiencia adquirida, los puntos concretos de este marco organizativo general.

A continuación, se expone cómo las disposiciones generales del marco organizativo del LABI, válidas en todos sus términos, pueden adaptarse a una situación de emergencia causada por incidentes de ciberseguridad.

El texto del documento del Plan de Protección Civil al que el presente Procedimiento se suma como Anexo, se encuentra disponible en la página web www.euskadi.eus/112 .

Los Títulos / Capítulos / Apartados del LABI en los que se especifica su cometido en caso de emergencia por ciberincidente:

Títulos de LABI	Capítulos/Apartados
Título Preliminar	2.- Funciones
	3.- Marco legal
	3.- De las autoridades de protección civil

Título IV - Normas generales de dirección y coordinación	3.1.- Del consejero del Interior
	3.2.- Del Lehendakari

Título V - Marco Organizativo General de la protección civil de la Comunidad Autónoma	Capítulo I - Estructura de Dirección del Plan Territorial de Protección Civil
	1.- Director
	2.- Consejo Asesor
	3.- Gabinete de información
	Capítulo II - Estructura Operativa
	2.- Grupos de acción
	2.4.- Funciones y composición
	2.4.1.- Grupos de intervención
	2.4.2- Grupo de apoyo técnico
	Capítulo III - Operatividad
	2.- Activación del plan territorial de protección civil de Euskadi
	2.1.- Concepto
	2.2.- Modalidades de aplicación conforme a la situación de emergencia
	Capítulo IV - Medidas de protección y reparadoras
	1.- Medidas de protección
	2.- Información a la población

2.TÍTULO PRELIMINAR

Lo dispuesto en el TÍTULO PRELIMINAR, apartado FUNCIONES del LABI, siendo plenamente aplicable, se concreta para el caso de incidentes de ciberseguridad de gran impacto en la población y/o servicios básicos de la comunidad autónoma vasca entre otras funciones las siguientes:

a*) FUNCIONES*

- Ofrecer una respuesta flexible y adaptada a la magnitud del incidente de ciberseguridad, de gran impacto en la sociedad, abordando de forma integral todos los ejes de actuación: contención técnica, recuperación operativa, protección jurídica, y comunicación institucional.

- Disponer de un marco de actuación que permita actuar de manera preventiva y anticipada, minimizando los efectos del incidente y garantizando la continuidad de los servicios básicos y la resiliencia del tejido socioeconómico.
- Asegurar una adecuada participación y coordinación interdepartamental e interinstitucional entre todas las Administraciones Vascas (LABI), así como con entidades públicas y privadas afectadas o responsables de infraestructuras básicos.
- Dar soporte a las estrategias de ciberseguridad vigentes, facilitando la coordinación de las actuaciones técnicas y estratégicas ante situaciones de emergencia derivadas de ciberataques o incidentes de seguridad en sistemas de información.
- Definir claramente los niveles de actuación (análisis y diagnóstico, propuesta de medidas, toma de decisiones) y las responsabilidades en cada uno de ellos, así como establecer las líneas de respuesta que deben articularse ante los distintos escenarios de riesgo.
- Prever una estructura organizativa.
- Asegurar la coordinación plena con los planes y procedimientos de ámbito superior, que pudieran activarse en respuesta a incidentes que trasciendan el ámbito autonómico.

b)MARCO LEGAL

Además de las referencias legales recogidas en el TÍTULO PRELIMINAR, apartado MARCO LEGAL del LABI, se enumeran las siguientes disposiciones aplicables en el ámbito de la ciberseguridad:

Estado

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Ley 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil (por su aplicación en emergencias de ciberseguridad que afecten a servicios ese).
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

- Directiva (UE) 2022/2555, relativa a medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión Europea (Directiva NIS2).

Euskadi

- Ley 7/1981, de 30 de junio, de Gobierno del País Vasco.
- Ley 7/2023, de 29 de junio**,** de creación de la Agencia Vasca de Ciberseguridad.

3. IDENTIFICACIÓN DE RIESGOS E INCIDENTES RELEVANTES

La identificación de riesgos en el ámbito de la ciberseguridad responde a una evaluación sistemática de amenazas y vulnerabilidades que pueden afectar a los sistemas de información, infraestructuras y servicios básicos de la Comunidad Autónoma del País Vasco.

En un contexto de alta digitalización y fuerte dependencia tecnológica, la sociedad vasca, sus instituciones y su tejido empresarial están expuestos a diversos riesgos en el ciberespacio, entre los que destacan, pero no se limitan, a:

- Ataques dirigidos contra infraestructuras y servicios básicos (energía, agua, sanidad, transporte, telecomunicaciones, etc.).
- Incidentes derivados de fallos técnicos, posibles vulnerabilidades y/o errores humanos.
- Amenazas emergentes asociadas a la evolución tecnológica, como el uso masivo de dispositivos IoT, el despliegue de inteligencia artificial o la interconexión de sistemas industriales (ICS/SCADA).
- Ciberataques persistentes y altamente sofisticados (APT).
- Ransomware y extorsión digital, donde los atacantes cifran datos sensibles y exigen pagos para su liberación.
- Acciones maliciosas como sabotajes, fraudes electrónicos, robos de información o campañas de desinformación.

No obstante, no todos estos riesgos o incidentes darán lugar a la activación del LABI. Solo aquellos incidentes de ciberseguridad que tengan un gran impacto en la normalidad de la población afecten a infraestructuras básicas, comprometan servicios básicos o generen una emergencia de protección civil, podrán suponer la activación del LABI conforme a lo previsto en este procedimiento.

4. NORMAS GENERALES DE DIRECCIÓN Y COORDINACIÓN

Corresponde a la persona titular del Departamento competente en materia de Seguridad Pública, Emergencias y Protección Civil, la dirección única y coordinación del LABI también en situaciones de emergencia cibernética, sin perjuicio de la asunción por el o la Lehendakari de tales facultades, conforme a lo dispuesto en el Decreto Legislativo 1/2017, de 27 de abril, por el que se aprueba el texto refundido de la Ley de Gestión de Emergencias.

Esta dirección queda sujeta a la activación del LABI por parte de la persona titular del mismo, a solicitud de Cyberzaintza o a la vista de la emergencia, en función de la gravedad, extensión o repercusión de un incidente cibernético que pueda comprometer servicios básicos, infraestructuras básicas o el normal funcionamiento de los sistemas públicos que afectan a la seguridad de la ciudadanía.

La activación se declarará tras la evaluación técnica realizada por Cyberzaintza, que informará a la persona titular del Departamento competente en materia de Atención de Emergencias y Protección Civil sobre la naturaleza del incidente y tras determinarse si concurren los criterios establecidos en este procedimiento para declarar la emergencia de ciberseguridad.

Sin perjuicio de lo anterior, lo dispuesto en el Título IV NORMAS GENERALES DE COORDINACIÓN Y DIRECCIÓN del LABI para hacer frente a una emergencia por ciberataque atenderá a las siguientes consideraciones.

En situaciones de ciberemergencia, y de acuerdo con lo establecido en el presente procedimiento, será también necesaria la evaluación técnica por parte de la Agencia Vasca de Ciberseguridad del Gobierno Vasco, quienes informarán sobre la naturaleza del incidente, su impacto y la progresión previsible de la emergencia. En este marco, podrá procederse a la activación del plan en su fase y situación correspondiente, garantizando así la coordinación y movilización de medios y recursos necesarios.

Durante el transcurso de la emergencia, y atendiendo a su especial complejidad, carácter sistémico o afectación interinstitucional, el o la Lehendakari podrá asumir la dirección única y coordinación estratégica de las actuaciones del LABI, sin perjuicio de las facultades que le correspondan como autoridad delegada del Estado en caso de declararse el estado de alarma. Esta atribución se ejercerá al amparo del artículo 35 de la Ley de Gestión de Emergencias, el artículo 8 de la Ley 7/1981, de 30 de junio, del Gobierno, y la normativa específica del Estado aplicable a situaciones de emergencia, como la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

5. MARCO ORGANIZATIVO GENERAL DE LA PROTECCIÓN CIVIL DE LA COMUNIDAD AUTÓNOMA

Sin perjuicio de lo dispuesto en el Título V MARCO ORGANIZATIVO GENERAL DE LA PROTECCIÓN CIVIL DE LA COMUNIDAD AUTÓNOMA del LABI, en sus capítulos I. ESTRUCTURA DE DIRECCIÓN y II. ESTRUCTURA OPERATIVA, para hacer frente a una emergencia provocada por un ciberincidente de acuerdo con lo establecido en este procedimiento.

Además de las consideraciones señaladas, se plantea un modelo de actuación con dos niveles de actuación. El **primero**, propiamente de decisión, con la concreción de las funciones de la persona Directora y la configuración del consejo Asesor con representación de todas las instituciones Vascas y el Área de Comunicación. El **segundo**, de carácter técnico, se articula en torno a una Comisión Especializada en Ciberseguridad, encargada de evaluar la amenaza, analizar riesgos, prever escenarios y formular propuestas de medidas de respuesta al Consejo Asesor.

El Consejo Asesor estará integrado por representantes de los departamentos del Gobierno Vasco directamente implicados en la gestión de la emergencia, así como, en su caso, por representantes de otras instituciones públicas del ámbito estatal, autonómico, local, según la naturaleza y alcance del incidente.

La Comisión Técnica será nombrada por la persona Directora del Plan Territorial de Protección Civil de Euskadi y estará integrada, entre otros, por personal técnico de la Agencia Vasca de Ciberseguridad.

En el marco de este procedimiento, y de manera específica para emergencias de ciberseguridad, se prevé la figura de un/a Coordinador/a de la Comisión Técnica. Esta persona será designada por la Dirección del Plan y tendrá como cometido organizar los trabajos de la Comisión, coordinar a sus integrantes y trasladar al Consejo Asesor los informes y propuestas que se elaboren.

Asimismo, podrán incorporarse personas expertas en ciberseguridad, análisis de amenazas, continuidad operativa y respuesta ante incidentes complejos, procedentes de entidades públicas o privadas, en función de la naturaleza y características del incidente.

a) ESTRUCTURA DE DIRECCIÓN

i. DIRECTOR O DIRECTORA

Para el caso de emergencias derivadas de incidentes de ciberseguridad, corresponde a la persona Directora del Plan, además de las funciones generales previstas, asumir las siguientes responsabilidades específicas:

- Nombrar a las personas integrantes del Consejo Asesor, al Coordinador o Coordinadora de la Comisión Técnica, y a las personas expertas que la conformen.
- Convocar la Comisión Técnica total o parcialmente, en función del tipo y gravedad del ciberincidente.
- Garantizar una comunicación clara, transparente y coordinada con la ciudadanía e instituciones, tanto en cuanto al impacto del incidente como a las medidas adoptadas.
- Conformar el área de comunicación e información.
- Coordinarse con otras Comunidades Autónomas y con el Estado a través de los órganos establecidos al efecto, con objeto de adoptar las medidas más coherentes y adecuadas.
- Establecer la articulación de la respuesta para la protección de servicios e infraestructuras básicas, en relación con la vigilancia, detección y neutralización de amenazas, la recuperación operativa y la continuidad de los servicios básicos.
- Adoptar, ante una crisis grave y prolongada, una jerarquía de criterios para la toma de decisiones, priorizando la protección de la población, la continuidad institucional y el funcionamiento de los servicios básicos, buscando el equilibrio en su ponderación y valorando el impacto generado.
- Establecer la información que se va a trasladar, transparencia, indicadores, casos, en función de los ámbitos más críticos.
- Establecer la articulación de la respuesta para paliar los daños sobre la economía y la pérdida de empleo y promover la reconstrucción socioeconómica.

ii. CONSEJO ASESOR

El Consejo Asesor estará compuesto por representantes de los departamentos del Gobierno Vasco directamente implicados en la gestión de la emergencia, así como, en su caso, por representantes de otras instituciones públicas del ámbito autonómico, foral o local, en función de la naturaleza y alcance del incidente.

Su composición básica incluirá, entre otros:

- Lehendakaritza / Portavocía del Gobierno Vasco.
- Departamento con competencias en seguridad.
- Dirección de la Ertzaintza.
- Dirección de Atención de Emergencias y Meteorología.
- Dirección de Cyberzaintza.

- Representación de las tres diputaciones forales.
- Representación de la Asociación de Municipios Vascos (EUDEL).
- Representación institucional de las tres capitales de los territorios históricos.
- Persona representante de la Delegación del Gobierno en la CAE.
- Departamento con competencias en gobernanza pública y digital.
- Departamento con competencias en salud, en caso de que el incidente afecte a servicios sanitarios.
- Departamentos con competencia Economía y Hacienda, Industria y Energía, Salud, Educación y Ciencia, entre otros, que pudieran verse afectados por la naturaleza del incidente.

La persona Directora del Plan podrá incorporar a otros responsables institucionales u órganos directivos, en función de la evolución y el impacto del incidente.

iii. GABINETE DE INFORMACIÓN

Las comunicaciones estarán lideradas por el Gabinete de Comunicación del Plan de Protección Civil. Será el canal oficial de información durante el tiempo que dure la emergencia, y tendrá, entre otras, estas funciones:

- Informar periódicamente a la ciudadanía e instituciones sobre la evolución del incidente y las medidas adoptadas.
- Garantizar la transparencia, claridad y accesibilidad de la información pública, combatiendo la desinformación o los bulos en colaboración con los equipos especializados.
- Difundir recomendaciones de autoprotección digital, seguridad básica y buenas prácticas para empresas, instituciones y ciudadanía.
- Promover, si se considera necesario, el uso de tecnologías y aplicaciones específicas para la difusión de información y alertas de ciberseguridad.

b) ESTRUCTURA OPERATIVA

Sin perjuicio de lo dispuesto en el capítulo II del LABI, relativo a la estructura operativa para la gestión de emergencias, en el caso de un incidente de ciberseguridad que cumpla los criterios de gravedad definidos en este procedimiento se contemplan, además, una serie de elementos organizativos específicos que refuerzan la capacidad de respuesta técnica y la coordinación institucional.

En este sentido, se establece una Comisión Técnica dependiente del Consejo Asesor, concebida como el principal órgano de apoyo técnico y especializado a la persona Directora del Plan. Su objetivo es ofrecer una aproximación transversal y multisectorial a la emergencia, garantizando la adecuada integración del conocimiento técnico, operativo e institucional. La Comisión actúa como núcleo de análisis, diagnóstico y propuesta, facilitando una comprensión global y en tiempo real de la evolución del incidente, así como la anticipación de posibles escenarios de riesgo.

La **Comisión Técnica** tiene entre sus cometidos la elaboración de informes técnicos sobre la evolución de la emergencia, basados en datos contrastados e indicadores relevantes, así como la formulación de propuestas de actuación dirigidas a la Dirección del Plan. Estas propuestas deberán responder a criterios de coordinación interinstitucional, viabilidad operativa y coherencia estratégica, y estarán enmarcadas en los ejes fundamentales de actuación ante emergencias cibernéticas: continuidad operativa de los servicios críticos, seguridad de los sistemas y redes, y protección de la ciudadanía y de las instituciones afectadas.

Este órgano se estructura en ámbitos temáticos vinculados a la naturaleza del incidente y al tipo de impacto que este pueda generar. Estará integrada por personal técnico con experiencia contrastada en ciberseguridad, gestión de riesgos tecnológicos, protección de infraestructuras básicas, análisis de datos, continuidad operativa y otros campos que se consideren relevantes para la emergencia.

Asimismo, podrán participar responsables operativos de áreas clave de la administración, en calidad de miembros técnicos, quienes podrán contar con el soporte especializado de equipos de expertos, a fin de garantizar una respuesta eficaz y coordinada.

Este diseño organizativo es flexible y se ajustará a las características concretas del ciberincidente y a su evolución en el tiempo. La persona Directora del Plan podrá designar a nuevos integrantes en función de las necesidades de la situación y convocar, cuando se estime oportuno, a profesionales o especialistas externos cuya contribución se considere relevante.

6. OPERATIVIDAD

Ante la detección de un incidente de seguridad de naturaleza cibernética con potencial impacto sobre servicios públicos básicos de los descritos en este procedimiento y en la población, la Agencia Vasca de Ciberseguridad emitirá una alerta técnica preliminar, que activará los procedimientos de valoración de riesgos establecidos. Esta alerta no implica la activación automática del Plan Territorial de Protección Civil, pero constituye el primer nivel formal de aviso institucional, a partir del cual se analizará la necesidad de activar el plan en alguno de sus fases y situaciones operativos.

Sin perjuicio de lo dispuesto en el Título V, **MARCO ORGANIZATIVO GENERAL DE LA PROTECCIÓN CIVIL DE LA COMUNIDAD AUTÓNOMA**, del LABI, en su Capítulo III, **OPERATIVIDAD**, para hacer frente a una emergencia derivada de un **ciberincidente de gran escala** se atenderá adicionalmente a las consideraciones que se exponen a continuación.

ACTIVACIÓN DEL PLAN TERRITORIAL DE PROTECCIÓN CIVIL DE EUSKADI

La activación del Plan Territorial de Protección Civil de Euskadi para hacer frente a una situación de emergencia provocada por un ciberincidente podrá producirse cuando, en función del análisis técnico realizado por Agencia Vasca de Ciberseguridad, se estime que la continuidad de servicios básicos pudiera verse gravemente comprometida en el territorio de Euskadi, debido a un ataque deliberado, fallo sistémico o amenaza que afecte de forma significativa a sistemas tecnológicos clave.

Las modalidades de aplicación conforme a las fases y situaciones de emergencia dependerán de la naturaleza del incidente, su evolución, y la afectación territorial o sectorial concreta, conforme a lo dispuesto en el Capítulo III, **OPERATIVIDAD**, del texto del cuerpo del Plan de Protección Civil de Euskadi. Entre los elementos a valorar se encontrarán, entre otros, la pérdida de funcionalidad en servicios básicos (sanidad, energía, transporte, comunicaciones, emergencias), el riesgo para la integridad de infraestructuras básicas, y el impacto social o institucional del incidente.

La asunción de la dirección única y coordinación del LABI por parte del o de la Lehendakari implicará, en este contexto, la declaración de situación 2 o 3 de la Fase de Emergencia del Plan de Protección Civil de Euskadi.

La activación del Plan de Protección Civil ante un ciberincidente en situación 2 o 3, y en todo caso cuando su Dirección haya sido avocada para sí por parte del o de la Lehendakari, supondrá la integración de los planes sectoriales o específicos de respuesta que resulten afectados. Las organizaciones competentes en cada ámbito quedarán representadas en el Consejo Asesor del presente plan, en los términos y con las funciones ya previstas en el LABI, sin necesidad de modificación alguna del mismo.

7. MEDIDAS DE PROTECCIÓN Y REPARADORAS

Sin perjuicio de lo dispuesto en el Título V, **MARCO ORGANIZATIVO GENERAL DE LA PROTECCIÓN CIVIL DE LA COMUNIDAD AUTÓNOMA**, del LABI, en su capítulo IV, **MEDIDAS DE PROTECCIÓN Y REPARADORAS**, para hacer frente a una emergencia derivada de un **ciberincidente** de los catalogados en el documento se atenderá además a las consideraciones que se exponen a continuación.

a) ÁREAS DE GESTIÓN

Se proponen las áreas de gestión del ciberincidente en las que deben articularse las medidas de protección y reparadoras:

- Comunicación y gestión de la información pública.
- Análisis de impacto e identificación de sistemas afectados.
- Gestión técnica de la respuesta contención.
- Resolución de la emergencia.
- Restablecimiento de los servicios básicos.
- Ciberseguridad institucional y operativa.
- Respuesta organizativa interinstitucional.

Estas áreas se entienden como marcos de intervención complementarios a los ya contemplados en el LABI y deberán ser adaptadas a la naturaleza y alcance del incidente concreto, en coordinación con la Agencia Vasca de Ciberseguridad.

b) INFORMACIÓN A LA POBLACIÓN

Además de lo dispuesto en el apartado **INFORMACIÓN A LA POBLACIÓN** del LABI, para hacer frente a una emergencia por ciberincidente se atenderá a las consideraciones que se exponen a continuación:

Se informará a la población, entre otras cosas, sobre:

- Indicaciones de cómo actuar ante posibles afectaciones.
- Consejos de ciberhigiene y autoprotección digital básica.
- Canales de atención y consulta habilitados para la ciudadanía.
- Soluciones provisionales y alternativas para la población afectada por la interrupción de los servicios públicos.
- Material divulgativo orientado a reducir el impacto del incidente.

Asimismo, se promoverá la **divulgación social del plan de respuesta organizativa e institucional**, como una medida relevante para reforzar la comprensión pública de los mecanismos de resiliencia y fomentar la corresponsabilidad digital. En este sentido podrán:

- Se valorará el uso de tecnologías de la información (aplicaciones móviles, notificaciones masivas, sistemas de alerta temprana digital) como herramientas de comunicación y alerta, si se consideran oportunas.
- Se prestará atención a la diversidad de perfiles digitales de la población, analizando el nivel de comprensión de los mensajes por parte de distintos grupos (por edad, competencias digitales, vulnerabilidad social) para adaptar los contenidos de forma eficaz y accesible.