DISPOSICIONES GENERALES

DEPARTAMENTO DE SEGURIDAD

2940

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.

La Sociedad actual es una sociedad interconectada muy dependiente de las tecnologías de información.

Es un hecho que las amenazas de ciberseguridad son una realidad a la que se está haciendo frente por medio de distintas estrategias y normativas. La rapidez con la que los avances tecnológicos se desarrollan hace necesario que dichas estrategias estén en continua implementación.

Las autoridades competentes en la materia son diversas por lo que resulta complicado el desarrollo común de directrices. El Gobierno Vasco viene trabajando en este ámbito con la creación, entre otras actuaciones, de Cyberzaintza-Agencia Vasca de Ciberseguridad en el ámbito de la seguridad pública.

Cuando hay una amenaza de ciberseguridad, puede llegar a verse comprometida la prestación de los servicios esenciales del territorio, con las potenciales consecuencias negativas en la población.

Del mismo modo, el artículo 26 del texto refundido de la Ley de Gestión de Emergencias aprobado por el Decreto Legislativo 1/2017, de 27 de abril, prevé que los planes de protección civil aprobados por el Gobierno Vasco podrán exigir la elaboración e implantación de planes de continuidad de la actividad en determinadas infraestructuras críticas y recursos clave que resulten esenciales para la comunidad, su estabilidad económica y social y la pronta recuperación en situaciones de grave riesgo, catástrofe o calamidad. Así se identifica en el Plan de Protección Civil de Euskadi.

También el Decreto Legislativo 1/2017, de 27 de abril, por el que se aprueba el texto refundido de la Ley de Gestión de Emergencias y su normativa de desarrollo abordan la autoprotección como medida de prevención y eslabón de unión con el sistema vasco de atención de emergencias.

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, contempla las actividades que deben disponer de planes de autoprotección y los requisitos para su elaboración.

Visto lo anterior, parece conveniente arbitrar mecanismos que posibiliten que las actividades de sectores básicos y esenciales obligados a desarrollar planes de autoprotección deban desarrollar también planes de continuidad en materia de ciberseguridad que puedan unificarse en un documento único y común.

Por todo ello,

DISPONGO:

Artículo 1.– Objeto.

Es objeto de la presente Orden regular los planes de continuidad informática para hacer frente a los eventos de la ciberseguridad en actividades, centros, establecimientos o infraestructuras prioritarias de la Comunidad Autónoma de Euskadi.

Artículo 2.– Ámbito de aplicación:

1.– Lo dispuesto en esta Orden será de aplicación a las actividades de los sectores cuya operación es 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, cuando alguno de sus establecimientos este sujeto a lo establecido 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 hace referencia el párrafo anterior de este artículo se encuentran categorizados en el Anexo I de la presente Orden, sin perjuicio que mediante orden de la persona titular del departamento competente en materia de seguridad puedan ser actualizados posteriormente en virtud de 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); así como en virtud de cualquier otra normativa relacionada con estos sectores en materia de ciberseguridad.

3.– Las administraciones públicas competentes podrán exigir la elaboración e implantación de planes de continuidad a los titulares de actividades no incluidas en el ámbito de aplicación de esta Orden, cuando presenten un especial riesgo o vulnerabilidad.

4.– Igualmente, los titulares de actividades, centros, establecimientos o infraestructuras no recogidos en los párrafos 2 y 3 del presente artículo, podrán voluntariamente elaborar un plan de continuidad en materia de ciberseguridad conforme a lo previsto en esta Orden, asumiendo de ese modo las mismas responsabilidades con respecto a ciberseguridad que los titulares para los que su realización es obligatoria, si bien, en cualquier momento y de un modo voluntario, podrán solicitar la no realización y control del plan aunque continúen con su actividad.

5.– Quedan exentos del control administrativo aquellos centros, establecimientos o instalaciones dependientes del Ministerio de Defensa, de Instituciones Penitenciarias, de las Fuerzas y Cuerpos de Seguridad, y Resguardo Aduanero, así como los de los órganos judiciales.

Artículo 3.– Criterios de aplicación

1.– Las obligaciones de ciberseguridad establecidas en la presente Orden serán exigidas como norma mínima o supletoria respecto a las normativas especificas en materia de ciberseguridad.

2.– Los planes de continuidad previstos en esta Orden y aquellos otros instrumentos de prevención y autoprotección impuestos por otra normativa aplicable, podrán fusionarse en un documento único cuando dicha unión permita evitar duplicaciones innecesarias de la información y la repetición de los trabajos realizados por el titular o la autoridad competente, siempre que se cumplan todos los requisitos esenciales de la presente Orden.

Artículo 4.– Obligaciones

1.– Las obligaciones de las personas titulares de las actividades reseñadas en el artículo 2 de la presente Orden son las siguientes:

a) Elaborar un plan de continuidad de ciberseguridad de acuerdo a las directrices de la autoridad competente en materia de ciberseguridad, cuyos contenidos mínimos se recogen en el Anexo II de la presente Orden.

b) Remitir al Registro de Autoprotección de Euskadi como datos de registro los siguientes:

– La obligatoriedad de realizar el plan de continuidad en materia de ciberseguridad.

– La ficha con datos específicos para la protección en ciberseguridad recogido en el Anexo III de esta Orden.

– Declaración responsable del titular relativa al cumplimiento de toda la normativa de ciberseguridad. Como tal declaración, las autoridades competentes en materia de protección civil y emergencias no supervisaran, validaran o inspeccionaran el contenido del citado plan.

c) Desarrollar las actuaciones para la implantación y el mantenimiento de la eficacia del plan de continuidad.

d) Nombrar a las personas físicas responsables de la ciberseguridad de la actividad, en el caso de ser diferentes de la persona titular.

e) Informar y formar al personal a su servicio en los contenidos del plan.

f) Mantener los medios materiales y personales necesarios para afrontar el plan de continuidad.

g) Aplicar las medidas previstas en el plan de continuidad en ciberseguridad.

h) Realizar ejercicios o simulacros periódicos.

i) Notificar inicialmente a la Agencia Vasca de Ciberseguridad los incidentes relativos a ciberseguridad recogidos en el Anexo IV, por la que se define el contenido mínimo del plan de continuidad en materia de ciberseguridad a través del Centro de Coordinación de Emergencias de Euskadi (SOS Deiak-112), sin perjuicio de cualquier otra notificación que deban hacerse por requerimiento legal. Las notificaciones posteriores se harán directamente a la Agencia Vasca de Ciberseguridad.

2.– Las obligaciones de la autoridad competente en materia de emergencias y protección civil de la Comunidad Autónoma de Euskadi en relación a los planes de continuidad en materia de ciberseguridad son las siguientes:

a) Habilitar en el registro de autoprotección de Euskadi un apartado específico y exclusivo para las actividades sujetas a esta orden según el artículo 2 «ámbito de aplicación» en el que deban registrar la ficha con datos específicos para la protección en ciberseguridad recogido en el Anexo III de esta Orden.

b) Comprobar la obligatoriedad de realizar Plan de Continuidad en materia de Ciberseguridad por las actividades sujetas a esta Orden.

c) Remitir a la Agencia Vasca de ciberseguridad de Euskadi las notificaciones de los incidentes relativos a ciberseguridad notificados al Centro de Coordinación de Emergencias de Euskadi (SOS-Deiak).

d) Para la correcta validación de los datos del registro de autoprotección de Euskadi, comprobará exclusivamente que se cumple con lo establecido en los artículos 22 y 22 bis del 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 así como la obligatoriedad de disponer de Plan de continuidad en materia de ciberseguridad.

3.– Las obligaciones de la Agencia Vasca de Ciberseguridad son las siguientes:

a) Supervisar e inspeccionar el plan de continuidad en materia de ciberseguridad.

b) Supervisar e inspeccionar la Ficha con Datos Específicos para la protección en ciberseguridad.

DISPOSICIÓN ADICIONAL

El contenido de los anexos de la presente Orden, a excepción del Anexo I, podrá ser modificado mediante Resolución de la persona titular de la Agencia Vasca de Ciberseguridad, que se publicará en el Boletín Oficial del País Vasco.

DISPOSICIÓN TRANSITORIA

Las obligaciones recogidas en esta Orden serán exigibles a partir del día siguiente de su publicación en el Boletín Oficial del País Vasco para todas las actividades, centros, establecimientos o infraestructuras nuevas y para las ya existentes se da un periodo de carencia igual al periodo de revisión de su Plan de Autoprotección.

DISPOSICIÓN FINAL

La presente Orden entra en vigor el día siguiente al de su publicación en el Boletín Oficial del País Vasco.

En Vitoria-Gasteiz, a 7 de junio de 2024.

El Vicelehendakari Primero y Consejero de Seguridad,
JOSU IÑAKI ERKOREKA GERVASIO.

ANEXO I

CATEGORIZACIÓN DE SECTORES

Los sectores a los que hace referencia el artículo 2.1 de la Orden son los siguientes:

a) Tecnologías de la información comunicaciones.
b) Gobierno y Administración Pública.
c) Energía.
d) Cadena alimentaria.
e) Infraestructuras y medios de transporte y logística.
f) Finanzas.
g) Agua.
h) Agentes económicos relevantes.
i) Sanidad.
j) Residuos urbanos e industriales.
k) Sectores industriales de riesgo.
l) Investigación.

ANEXO II

CONTENIDO MÍNIMO DEL PLAN DE CONTINUIDAD EN MATERIA DE CIBERSEGURIDAD

1.– Una planificación y un control operacional: se deben planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos propios de la actividad e implementar las acciones destinadas a abordar los riesgos y oportunidades.

2.– Un análisis de impacto del negocio y evaluación de riesgos: se debe implementar y mantener un proceso para analizar el impacto comercial y evaluar los riesgos de interrupción que establezca el contexto, defina criterios y evalúe el impacto potencial de una interrupción.

3.– Estrategias y soluciones de continuidad del negocio: se debe identificar y seleccionar estrategias de continuidad del negocio basadas en los resultados del análisis de impacto del negocio y la evaluación de riesgos. Las estrategias de continuidad del negocio podrán estar compuestas por una o más soluciones.

4.– Planes y procedimientos de continuidad del negocio: se debe implementar y mantener una estructura que permita la advertencia y la comunicación oportunas a las partes interesadas relevantes, y proporcionar planes y procedimientos para administrar la organización durante una interrupción. Los planes y procedimientos se utilizarán cuando sea necesario para ejecutar soluciones de continuidad del negocio.

5.– 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 del negocio.

La Agencia Vasca de Ciberseguridad desarrollará una guía con la estructura del documento del plan de continuidad en materia de ciberseguridad.

ANEXO III

FICHA CON DATOS ESPECÍFICOS

La Ficha con Datos Específicos para la protección en ciberseguridad incluirá al menos el siguiente contenido:

1.– Punto de contacto para incidentes y alertas.

1.1.– Punto de contacto responsable de la notificación de incidentes y alertas de ciberseguridad de la organización (nombre, dirección electrónica y teléfono).

1.2.– Contacto secundario en caso de ausencia del punto de contacto principal (nombre, dirección electrónica y teléfono).

2.– Controles de seguridad aplicados. Se indicará si dispone de:

2.1.– Política general de seguridad de la información.

2.2.– Políticas específicas de seguridad de la información.

2.2.1.– Política específica de gestión de actualizaciones.

2.2.2.– Política específica de gestión de contraseñas.

2.2.3.– Política específica de seguridad de la información para las relaciones con proveedores.

2.3.– Gestión de las vulnerabilidades técnicas.

2.4.– Inventario de información y otros activos asociados: identificación de los activos.

2.5.– Copias de respaldo o de seguridad (backup).

2.6.– Mecanismos de protección contra programas maliciosos. (Antivirus, EDR, etc.).

2.7.– Mecanismos de protección de correo.

2.8.– Mecanismos de segmentación de red.

2.9.– Mecanismos de control de red (Firewall, IDS, IPS, NAC, etc.).

2.10.– Mecanismos de acceso remoto (VPN, escritorio remoto, etc.).

2.11.– Mecanismos de seguridad de aplicaciones (WAF, seguridad de API, etc.).

2.12.– Mecanismos de autenticación multi-factor.

2.13.– Auditorías técnicas de seguridad.

2.13.1.– Fecha de la última auditoría técnica de seguridad.

2.14.– Concienciación al personal de la organización en materia de ciberseguridad.

2.14.1.– Fecha de la última iniciativa de concienciación al personal en materia de ciberseguridad.

2.15.– Ejercicio o simulacro de gestión de incidente de ciberseguridad.

2.15.1.– Fecha del último ejercicio o simulacro de gestión de incidente de ciberseguridad.

2.16.– Un proveedor de referencia en materia de respuesta a incidentes de ciberseguridad.

ANEXO IV

INCIDENTE RELATIVO A CIBERSEGURIDAD QUE HA DE SER NOTIFICADO

Los incidentes relativos a ciberseguridad a notificar mencionados en esta Orden 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.

Notificación inicial	Notificación intermedia	Notificación final
Inmediata.	24-48 horas.	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 incluida en la siguiente tabla:

Qué notificar	Descripción
Asunto	Frase que describa de forma general el incidente. Este campo lo heredarán todas las notificaciones asociadas al incidente.
Sector de actividad	Energía, transporte, financiero, etc.
Fecha y hora del incidente	Indicar con la mayor precisión posible cuándo ha ocurrido el incidente.
Fecha y hora de detección del incidente	Indicar con la mayor precisión posible cuándo se ha detectado el incidente.
Tipo de notificación	Inicial, intermedia o final.
Fecha y hora de la notificación	Indicar cuándo se está notificando.
Descripción	Describir con detalle lo sucedido.
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…
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.
Taxonomía (clasificación)	Posible clasificación y tipo de incidente en función de la taxonomía descrita.
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.
Afectación	Indicar si el afectado es una empresa o un particular, y las afectaciones según el nivel de impacto asignado.
Impacto económico estimado (Si se conoce)	Costes asociados al incidente, tanto de carácter directo como indirecto.
Extensión geográfica (Si se conoce)	Local, autonómico, nacional, supranacional, etc.
Daños reputacionales (Si se conocen)	Afectación a la imagen corporativa del operador.
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.).
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.