C/2026/3712

13.7.2026

COMUNICACIÓN DE LA COMISIÓN

Directrices sobre la aplicación del artículo 13, apartado 5, de la Directiva (UE) 2022/2557 relativa a la resiliencia de las entidades críticas

(C/2026/3712)

I. INTRODUCCIÓN

1. La Directiva (UE) 2022/2557, relativa a la resiliencia de las entidades críticas (en lo sucesivo, «la Directiva») ([1]), tiene por objeto garantizar que los servicios esenciales para el mantenimiento de funciones sociales o actividades económicas vitales se presten sin obstáculos en el mercado interior. La Directiva tiene por objeto mejorar la resiliencia de las entidades críticas que prestan dichos servicios, creando un marco general para la resiliencia frente a todos los peligros (naturales y provocados por el hombre, accidentales o intencionados).

2. De conformidad con el artículo 6, apartado 1, de la Directiva, los Estados miembros deben identificar sus entidades críticas para los sectores y subsectores establecidos en el anexo de la Directiva a más tardar el 17 de julio de 2026. Para lograr un alto nivel de resiliencia, dichas entidades críticas tienen obligaciones en virtud de la Directiva, incluida la obligación establecida en el artículo 13 de adoptar medidas técnicas, organizativas y de seguridad adecuadas y proporcionadas para garantizar su resiliencia. A este respecto, el artículo 13, apartado 5, de la Directiva encargó a la Comisión que adoptara directrices no vinculantes para especificar en mayor medida las medidas técnicas, organizativas y de seguridad que pueden adoptar las entidades críticas.

3. De conformidad con las disposiciones mencionadas anteriormente, antes de la adopción de la presente Comunicación, se consultó a los Estados miembros y a las partes interesadas en un taller celebrado el 29 de septiembre de 2025. Se consultó al Grupo de Resiliencia de las Entidades Críticas sobre las líneas generales de la Comunicación en sus reuniones de los días 10 de abril, 19 de mayo y 30 de septiembre de 2025. También se le consultó sobre el proyecto de texto de la Comunicación el 14 de noviembre de 2025, y el 25 de febrero de 2026 se compartió una versión actualizada con el Grupo de Resiliencia de las Entidades Críticas. El 6 de marzo de 2026 tuvo lugar una consulta final del Grupo de Resiliencia de las Entidades Críticas sobre el proyecto de directrices.

4. La presente Comunicación no es jurídicamente vinculante ni afecta a la interpretación del Derecho de la UE por parte del Tribunal de Justicia de la Unión Europea.

II. DIRECTRICES NO VINCULANTES SOBRE MEDIDAS DE MEJORA DE LA RESILIENCIA

A. CONSIDERACIONES GENERALES

5. Estas directrices no vinculantes tienen por objeto especificar aún más las medidas técnicas, organizativas y de seguridad que pueden adoptar las entidades críticas con arreglo al artículo 13, apartado 1, letra a) a f), de la Directiva. La lista de medidas no es exhaustiva y puede complementarse con medidas adicionales.

6. De conformidad con el artículo 13, apartado 1, al aplicar estas medidas, las entidades críticas deben tener en cuenta lo siguiente.

   a) Información pertinente facilitada por los Estados miembros sobre la evaluación de riesgos del Estado miembro realizada con arreglo al artículo 5 de la Directiva. Los Estados miembros deben enviar información rápida, sucinta y personalizada a sus entidades críticas. Dicha información podrá incluir los informes a que se refiere el artículo 9, apartado 3, de la Directiva, enviados a la Comisión utilizando el modelo común de informe.

   b) Información pertinente sobre los resultados de la evaluación de riesgos de la entidad crítica realizada con arreglo al artículo 12 de la Directiva. Se anima a las entidades críticas a aplicar un enfoque holístico pasando de una mera protección de las infraestructuras críticas a garantizar la continuidad de los servicios esenciales que prestan y a vincular los resultados de la evaluación de riesgos a sus medidas de mejora de la resiliencia. Con el fin de apoyar las medidas de resiliencia, las entidades críticas deben considerar la posibilidad de llevar a cabo evaluaciones de riesgos exhaustivas que vayan más allá de sus dependencias directas, teniendo en cuenta los aspectos de interdependencia transfronteriza, sectorial y sistémica.

([1]) Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo (DO L 333 de 27.12.2022, p. 164).

7. De conformidad con el artículo 13, apartado 1, de la Directiva, las medidas que deben adoptar las entidades críticas deben ser adecuadas y proporcionadas. La idoneidad y proporcionalidad de estas medidas deben evaluarse en relación con los resultados de las evaluaciones de riesgos mencionadas anteriormente.

   a) Por «adecuadas» deben entenderse medidas basadas en el riesgo o en el impacto, efectivas y apropiadas que puedan hacer que la entidad crítica sea plenamente resiliente en la prestación de servicios esenciales. La idoneidad de una medida puede diferir de una entidad crítica a otra en función de sus especificidades.

   b) Por «proporcionadas» deben entenderse las medidas necesarias y suficientes que no sean excesivas en cuanto al nivel de riesgo y la gravedad del incidente perturbador. Las medidas deben adaptarse a las especificidades de la entidad crítica en cuestión y tener en cuenta aspectos como la naturaleza de los servicios esenciales prestados, la cadena de suministro y las interdependencias, la eficiencia en costes de las medidas, el tamaño de la entidad y el impacto geográfico de los servicios prestados.

8. Las directrices tienen en cuenta todos los sectores cubiertos por el capítulo III de la Directiva ([2]). La lista no exhaustiva de ejemplos podría no aplicarse por igual a todos los sectores y a todos los tipos de infraestructuras críticas.

9. Las medidas que se adopten dependerán del resultado de la evaluación de riesgos del Estado miembro y de las evaluaciones de riesgos de las entidades críticas.

10. Las medidas de resiliencia adoptadas por las entidades críticas en virtud del artículo 13, apartado 1, letra a) a f), deben aplicarse sin perjuicio de las medidas derivadas de la legislación sectorial pertinente, como la legislación mencionada en el considerando 31 de la Directiva, así como la Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI 2) ([3]), la Legislación Europea sobre el Clima ([4]), el Reglamento sobre la preparación frente a los riesgos en el sector de la electricidad ([5]), el Reglamento sobre la seguridad del suministro de gas ([6]), la Directiva sobre la seguridad de las operaciones relativas al petróleo y al gas mar adentro ([7]), el marco de la UE sobre seguridad marítima y portuaria ([8]), el Reglamento General de Protección de Datos (RGPD) ([9]), el Reglamento para la realización del Cielo Único Europeo ([10]), el Reglamento sobre la Agencia de la Unión Europea para la Seguridad Aérea ([11]) y el Reglamento de Ejecución relativo a las funciones de la red de gestión del tráfico aéreo ([12]), y en coherencia con ellas.

([2]) Energía, transporte, salud, agua potable, aguas residuales, administración pública, espacio, producción, transformación y distribución de alimentos.

([3]) 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 (DO L 333 de 27.12.2022, p. 80).

([4]) Reglamento (UE) 2021/1119 del Parlamento Europeo y del Consejo, de 30 de junio de 2021, por el que se establece el marco para lograr la neutralidad climática y se modifican los Reglamentos (CE) n.º 401/2009 y (UE) 2018/1999 (DO L 243 de 9.7.2021, p. 1), en particular en lo que se refiere al artículo 5, sobre la adaptación al cambio climático.

([5]) Reglamento (UE) 2019/941 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, sobre la preparación frente a los riesgos en el sector de la electricidad y por el que se deroga la Directiva 2005/89/CE (DO L 158 de 14.6.2019, p. 1), en particular en lo que se refiere a las medidas mencionadas en los artículos 10 y 11.

([6]) Reglamento (UE) 2017/1938 del Parlamento Europeo y del Consejo, de 25 de octubre de 2017, sobre medidas para garantizar la seguridad del suministro de gas y por el que se deroga el Reglamento (UE) n.º 994/2010 (DO L 280 de 28.10.2017, p. 1), en particular en lo que se refiere a las medidas mencionadas en el artículo 8.

([7]) Directiva 2013/30/UE del Parlamento Europeo y del Consejo, de 12 de junio de 2013, sobre la seguridad de las operaciones relativas al petróleo y al gas mar adentro, y que modifica la Directiva 2004/35/CE (DO L 178 de 28.6.2013, p. 66), en particular en lo que se refiere a las medidas mencionadas en el artículo 3.

([8]) Por ejemplo, la Directiva 2005/65/CE sobre mejora de la protección portuaria y la Directiva 2002/59/CE relativa a los sistemas de seguimiento y de información sobre el tráfico marítimo.

([9]) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (DO L 119 de 4.5.2016, p. 1).

([10]) Reglamento (UE) 2024/2803 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativo a la realización del Cielo Único Europeo (DO L, 2024/2803, 11.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2803/oj), en particular el artículo 22, apartado 2, letra b).

([11]) Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo, de 4 de julio de 2018, sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de la Unión Europea para la Seguridad Aérea (DO L 212 de 22.8.2018, p. 1).

([12]) Reglamento de Ejecución (UE) 2019/123 de la Comisión, de 24 de enero de 2019, por el que se establecen disposiciones de aplicación de las funciones de la red de gestión del tránsito aéreo (ATM) (DO L 28 de 31.1.2019, p. 1).

11. Al utilizar la inteligencia artificial (IA) en sus medidas de resiliencia (por ejemplo, un sistema de IA que vigile la presión del agua en una presa o que controle una red eléctrica), las entidades críticas deben ser conscientes de que los sistemas de IA de alto riesgo deben cumplir los requisitos de seguridad del Reglamento de Inteligencia Artificial de la UE ([13]). Por «de alto riesgo» se entiende que están destinados a ser utilizados como componentes de seguridad ([14]) en la gestión y el funcionamiento de las infraestructuras digitales críticas, del tráfico rodado o en el suministro de agua, gas, calefacción o electricidad ([15]). Su fallo o mal funcionamiento puede poner en peligro la vida y la salud de las personas a gran escala y dar lugar a perturbaciones apreciables en el desarrollo ordinario de las actividades sociales y económicas.

12. En relación con el artículo 13, apartado 2, de la Directiva, el considerando 30 explica que, «[e]n aras de la eficacia y la rendición de cuentas, las entidades críticas deben describir las medidas que adopten, con un nivel de detalle que permita alcanzar de manera suficiente los objetivos de eficacia y rendición de cuentas, teniendo en cuenta los riesgos detectados, en un plan de resiliencia, o en uno o varios documentos que sean equivalentes a un plan de resiliencia, y poner ese plan en práctica. La entidad crítica que ya haya adoptado medidas técnicas, organizativas y de seguridad y elaborado documentos en virtud de otros actos jurídicos que sean pertinentes para las medidas de aumento de la resiliencia en virtud de la presente Directiva, debe poder, a fin de evitar duplicidades, utilizar dichas medidas y documentos para cumplir los requisitos en materia de medidas de resiliencia con arreglo a la presente Directiva [...]».

13. El papel del funcionario de enlace designado por la entidad crítica de conformidad con el artículo 13, apartado 3, de la Directiva es crucial para la adopción y aplicación efectivas de medidas de mejora de la resiliencia, ya que garantiza una comunicación y coordinación eficientes y eficaces entre la entidad crítica y las autoridades competentes en relación con las obligaciones de la entidad crítica y el marco general de resiliencia.

14. Al adoptar medidas de mejora de la resiliencia, se anima a las entidades críticas a identificar todos los activos, instalaciones y equipos pertinentes y a tener en cuenta los aspectos transfronterizos y de interdependencia, dada la naturaleza altamente interconectada de los sectores que abarca la Directiva, incluidos los aspectos físicos, medioambientales, cibernéticos y de la cadena de suministro. Una perturbación en un ámbito puede tener efectos en cascada en todo el mercado interior, perturbando así la prestación de servicios esenciales.

15. El mecanismo principal para considerar las interdependencias es la evaluación de riesgos de la entidad crítica y la evaluación nacional de riesgos. La evaluación de riesgos debe evaluar y tener en cuenta el grado en que otros sectores dependen del servicio esencial prestado por la entidad crítica y el grado en que esta depende de otros servicios esenciales prestados por otras entidades en otros sectores, también, cuando proceda, en Estados miembros vecinos y terceros países.

16. Al adoptar medidas de mejora de la resiliencia, las entidades críticas deben considerar la posibilidad de tener en cuenta las normas internacionales y europeas pertinentes.

17. Deben tenerse en cuenta las características específicas de las infraestructuras marítimas críticas: estas infraestructuras son más difíciles de supervisar y proteger; en el mar la detección y la localización de incidentes, así como las reparaciones, requieren más tiempo y son más costosas.

B. MEDIDAS PREVENTIVAS [artículo 13, apartado 1, letra a), de la Directiva]

18. Se anima a las entidades críticas a que adopten medidas que aumenten su resiliencia mejorando su capacidad para evitar fallos o perturbaciones. Estas medidas deben integrarse en el plan de resiliencia mencionado en el artículo 13, apartado 2, de la Directiva y considerarse parte de un sistema integrado y no componentes aislados. La efectividad de cualquier medida depende de su interacción con otras medidas, como la protección física de las instalaciones, la respuesta, la resistencia y la recuperación frente a incidentes perturbadores, y la gestión adecuada de la seguridad de los empleados.

([13]) Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial) (DO L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

([14]) Los componentes de seguridad de las infraestructuras críticas son sistemas utilizados para proteger directamente la integridad física de las infraestructuras críticas o la salud y la seguridad de las personas y los bienes, pero no son necesarios para que el sistema funcione (artículo 3, apartado 14, y considerando 55 del Reglamento de Inteligencia Artificial).

([15]) Anexo III, punto 2, del Reglamento de Inteligencia Artificial.

19. Las medidas de reducción del riesgo de catástrofes y de adaptación al cambio climático deben basarse en proyecciones climáticas plausibles a lo largo de la vida útil de las infraestructuras críticas. Se anima a las entidades críticas a que eviten poner infraestructuras críticas (por ejemplo, centros de datos o subestaciones) en zonas de alto riesgo; a que adopten medidas para reforzar estructuralmente la infraestructura en cuestión (por ejemplo, protección contra incendios, resistencia a inundaciones, sequías y explosiones, y protección contra líquidos), así como medidas no estructurales (por ejemplo, formación y protocolos de seguridad) para evitar colisiones, explosiones, vertidos de materiales peligrosos o radiaciones; a que encuentren soluciones basadas en la naturaleza, como la integración de infraestructuras verdes (por ejemplo, humedales restaurados para absorber las marejadas o bosques urbanos para reducir el efecto de «isla de calor» en los equipos eléctricos); a que consideren los cambios inmediatos y a largo plazo en los patrones climáticos que podrían degradar la integridad del sistema a lo largo del tiempo, como el calor extremo, las inundaciones y el aumento del nivel del mar; a que elaboren un plan para la escasez de agua; a que realicen pruebas de resistencia para garantizar que la entidad pueda funcionar en un entorno significativamente más adverso (por ejemplo, en condiciones más cálidas, frías, húmedas, secas, erráticas o no estacionales).

20. Se anima a las entidades críticas a que consideren la posibilidad de crear una base de datos de incidentes, contribuyendo a las bases de datos de incidentes de la UE ([16]) y aplicando un sistema de notificación de incidentes sistemático, que proporcione un historial de acontecimientos y permita no solo la prevención de incidentes y la reducción de riesgos, sino también la recuperación de activos.

21. Para evitar errores humanos, se anima a las entidades críticas a identificar tareas propensas a errores y a aplicar contramedidas adecuadas, como la automatización, la formación continua de los empleados, la supervisión y la rendición de cuentas clara, la documentación detallada de los procesos, las auditorías e inspecciones periódicas y el desarrollo de una cultura de resiliencia y responsabilidad.

22. Para garantizar que las medidas de resiliencia se apliquen en consonancia con la Directiva SRI 2, se anima a las entidades críticas a que, al aplicar sus medidas de resiliencia, tengan en cuenta las medidas pertinentes para la seguridad de las redes y los sistemas de información, tal como se definen en la Directiva SRI 2. Las medidas establecidas en el Reglamento de Ejecución (UE) 2024/2690 de la Comisión ([17]) aplicables a determinados tipos de entidades de los sectores de la infraestructura digital, de la gestión de servicios de tecnologías de la información y de las comunicaciones (TIC) (empresa a empresa) y de los proveedores digitales, tal como se definen en la Directiva SRI 2 ([18]), así como las orientaciones de aplicación de ENISA que la acompañan ([19]), pueden servir de referencia adicional.

23. Por lo que se refiere a la tecnología operativa, las entidades críticas deben incorporar sobremandos manuales y disposiciones que prevean la participación humana en las que se definan las condiciones y los requisitos específicos para la intervención humana y el control manual en respuesta a los peligros.

C. MEDIDAS DE PROTECCIÓN FÍSICA [artículo 13, apartado 1, letra b), de la Directiva]

24. Se anima a las entidades críticas a adoptar medidas físicas contra las amenazas naturales y de origen humano (por ejemplo, amenazas híbridas, sabotaje, terrorismo, actos delictivos, ataques militares o en tiempos de guerra, espionaje) y a establecer controles procesales que sirvan para detectar, disuadir, retrasar, denegar, responder y reducir el impacto de incidentes perturbadores.

([16]) En el sector de la aviación, las bases de datos pertinentes de la UE sobre incidentes incluyen el sistema de notificación de incidentes de la Agencia de la Unión Europea para la Seguridad Aérea, los registros de incidentes del gestor de la red y el sistema de notificación de sucesos relativos a la seguridad aérea.

([17]) Reglamento de Ejecución (UE) 2024/2690 de la Comisión, de 17 de octubre de 2024, por el que se establecen las disposiciones de aplicación de la Directiva (UE) 2022/2555 en lo que respecta a los requisitos técnicos y metodológicos de las medidas para la gestión de riesgos de ciberseguridad y en el que se detallan los casos en que un incidente se considera significativo con respecto a los proveedores de servicios de DNS, los registros de nombres de dominio de primer nivel, los proveedores de servicios de computación en nube, los proveedores de servicios de centro de datos, los proveedores de redes de distribución de contenidos, los proveedores de servicios gestionados, los proveedores de servicios de seguridad gestionados, los proveedores de mercados en línea, motores de búsqueda en línea y plataformas de servicios de redes sociales, y los proveedores de servicios de confianza (DO L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

([18]) De conformidad con el artículo 8 de la Directiva REC, los Estados miembros velarán por que determinadas disposiciones de la Directiva, incluido el artículo 13, no se apliquen a las entidades críticas que hayan identificado en determinados sectores, incluida la infraestructura digital. Los Estados miembros podrán adoptar o mantener disposiciones de Derecho nacional a fin de alcanzar un mayor nivel de resiliencia de dichas entidades críticas, a condición de que tales disposiciones sean coherentes con el Derecho de la Unión aplicable. La gestión de servicios de TIC (empresa a empresa) y los proveedores digitales no figuran entre los sectores definidos en el anexo de la Directiva REC.

([19]) https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance.

25. Al planificar medidas adecuadas y proporcionadas de mejora de la resiliencia frente a las amenazas de origen humano, las entidades críticas deben tener en cuenta la pertinencia de escenarios de amenaza específicos. Concretamente, se les anima a que:

    i) tengan en cuenta la necesidad de protocolos de coordinación estrecha entre los sectores público y privado para apoyar la cooperación operativa con las autoridades competentes y garantizar un flujo adecuado y recíproco de información sobre amenazas e incidentes, en aras de un conocimiento compartido de la situación;

    ii) en el caso de posibles amenazas híbridas de agentes estatales que, en el caso de las entidades críticas, sean principalmente intentos de sabotaje para perturbar activos y equipos, o preparativos para tales intentos (incluido el espionaje o la vigilancia), consideren que los agentes estatales pueden patrocinar y dirigir a representantes vulnerables o explotables (por ejemplo, personas o grupos) para alcanzar sus objetivos, y que los agentes estatales pueden participar en ataques coordinados a través de múltiples vectores de ataque en múltiples ámbitos o utilizando múltiples representantes;

    iii) tengan en cuenta otras posibles amenazas, en particular las derivadas del terrorismo y el extremismo violento, las actividades delictivas, los ataques militares, las amenazas internas, el activismo, etc.

26. Se anima a las entidades críticas a que consideren medidas de endurecimiento del perímetro (disuasión y retraso), como vallas de alta seguridad (por ejemplo, antiascenso/anticorte), muros reforzados, puertas, mitigación de vehículos hostiles, señalización e iluminación (por ejemplo, advertencias de alta visibilidad para disuadir a los intrusos oportunistas, e iluminación de seguridad para eliminar las zonas muertas para la vigilancia).

27. El acceso de vehículos, personal y mercancías a las instalaciones pertinentes debe canalizarse a través de un número limitado de puntos de control controlables. Las vías de aproximación directa del vehículo deben limitarse con una combinación de barreras físicas (por ejemplo, bolardos fijos y retráctiles, obstáculos naturales u otras medidas de control de la velocidad), y debe respetarse la separación máxima prescrita entre las barreras vecinas para evitar la penetración del vehículo.

28. Los puntos de entrada externos (por ejemplo, puertas o portones) a las instalaciones pertinentes deben ser de construcción robusta o reforzados, y estar (retro) equipados con bisagras de seguridad y mecanismos de bloqueo. Los marcos de las instalaciones (por ejemplo, ventanas, tragaluces) también deben estar equipados con mecanismos de bloqueo y estratificación protectora (por ejemplo, barras, rejillas, vidrio resistente a los golpes, membranas protectoras). Los puntos de entrada no convencionales (por ejemplo, trampillas de techo, bocas de inspección y respiraderos) a instalaciones o activos también deben estar protegidos contra la apertura no autorizada y la manipulación.

29. Se anima a las entidades críticas a que consideren la posibilidad de supervisar y detectar perímetros para detectar infracciones en tiempo real (por ejemplo, la instalación de alarmas o sistemas de detección de intrusiones, incluidos sensores interiores y exteriores). Estos deben mantener una cobertura de zona adecuada, estar sujetos a protocolos coherentes de seguimiento y respuesta y someterse a ensayos funcionales periódicos. Deben analizarse las detecciones legítimas, los fallos del sistema y los falsos positivos, y deben aplicarse medidas correctoras para mantener la integridad.

30. Se anima a las entidades críticas a que consideren la posibilidad de velar por que los sistemas de vídeo proporcionen una cobertura clara y específica del entorno, tanto en tiempo real como grabada, de los activos, instalaciones y equipos pertinentes, así como de las rutas de aproximación y los puntos de entrada de las instalaciones. La sincronización del tiempo de vigilancia, el estado de la grabación y los períodos de conservación deben verificarse periódicamente. Las entidades deben llevar a cabo controles de reproducción rutinarios para confirmar que los rostros, las acciones y los acontecimientos son identificables para los fines forenses previstos tras posibles incidentes. Debe disponerse de componentes críticos de repuesto (por ejemplo, medios de almacenamiento, unidades de alimentación) en cantidad adecuada.

31. Se anima a las entidades críticas a garantizar que los dispositivos de iluminación proporcionen una iluminación uniforme de las entradas, los aparcamientos, las pasarelas y los campos de visión de las cámaras, evitando el deslumbramiento y la sombra profunda que podrían impedir la detección o la grabación. El alumbrado de emergencia y de reserva debe probarse periódicamente. Deben aplicarse periódicamente medidas correctoras (por ejemplo, sustitución de lámparas, ajuste de la cobertura, recorte de la vegetación).

32. La señalización debe indicar claramente las restricciones de seguridad, los avisos de control y privacidad, y las rutas para el personal, los visitantes y las entregas.

33. Se anima a las entidades críticas a que estudien medidas para controlar (denegar) el acceso utilizando zonas de seguridad estratificadas, la gestión del acceso físico (por ejemplo, lectores de tarjetas de acceso, escáneres biométricos), las trampillas y las puertas con cerraduras dependientes. Debe considerarse el uso de personal de seguridad *in situ* para patrullar y gestionar el control de acceso a las instalaciones, puntos de entrada o equipos pertinentes. El personal de seguridad también debe desempeñar una función de respuesta a incidentes. Deben mantener un contacto estrecho y regular con las autoridades policiales y los agentes de defensa pertinentes.

34. Las salas y recintos que alberguen electricidad, agua, gas, calefacción, ventilación, aire acondicionado, telecomunicaciones, seguridad, redes u otras infraestructuras o equipos sensibles deben cerrarse con llave y controlarse el acceso, y complementarse con medidas proporcionadas contra la apertura y la manipulación no autorizadas.

35. Las salas de correo y los depósitos de entrega deben estar situados lejos de los activos, las instalaciones, los equipos y las zonas de alta ocupación pertinentes, y equipados para la segregación y la inspección segura de artículos potencialmente sospechosos. El personal debe ser informado de procedimientos claros para los artículos sospechosos, como el aislamiento, la desescalada y la notificación a las partes interesadas internas y externas pertinentes. En caso necesario, debe disponerse de herramientas de apertura y equipos de protección individual. La cadena de custodia de las entregas valiosas o controladas debe documentarse desde la recepción hasta el destinatario. Los controles aleatorios deben realizarse y registrarse de forma periódica.

36. Todos los activos, instalaciones o equipos externos deben estar igualmente sujetos a medidas de protección proporcionadas. Cualquier medida de protección física adoptada por las entidades críticas requiere una inspección y un mantenimiento rutinarios de forma periódica.

37. Las medidas relativas a los controles de acceso del personal y a la seguridad física de la información sensible o clasificada no invalidan las obligaciones de gestión de riesgos de ciberseguridad establecidas en la Directiva SRI 2 ([20]).

38. Además de las orientaciones que figuran en la parte F de las presentes directrices relativas a la gestión de la seguridad de los empleados, se anima a las entidades críticas a que mantengan un registro único y autorizado de claves físicas y credenciales (electrónicas), incluidas las fechas de expedición, revocación y retorno. Las claves o credenciales perdidas o robadas deben revocarse inmediatamente y cambiar o sustituir las cerraduras cuando se sospeche que se han puesto en peligro.

39. En lo tocante a los derechos de acceso, se anima a las entidades críticas a que sigan el principio del «mínimo privilegio» y que los revisen periódicamente o a raíz de un cambio de funciones. Los espacios pertinentes deben mantener una arquitectura por zonas, controlada mediante las medidas correspondientes para personas seleccionadas (por ejemplo, distinguiendo entre zonas públicas, de trabajo, restringidas y críticas) y combinando controles físicos, técnicos y administrativos. Debe registrarse el acceso. Los visitantes deben ser canalizados a través de un punto controlado, registrados, con identificación visible y escoltados más allá de la recepción, a menos que se autorice otra cosa. Estos medios de identificación deben desactivarse inmediatamente en el momento de la salida. Los procedimientos correspondientes deben ser sencillos, estar documentados y comunicarse a todo el personal, en particular al personal de acogida y seguridad.

40. Todo activo de información sensible debe colocarse, protegerse y almacenarse de manera que se reduzcan los riesgos para la integridad de dichos activos (por ejemplo, visualización no autorizada o accidental, manipulación, robo o daños medioambientales) y se acceda a él sobre la base de la necesidad de conocer.

41. Se anima a las entidades críticas a que establezcan y mantengan un inventario o repositorio de activos de información delicada. Los activos deben clasificarse en función del nivel de sensibilidad empresarial o de seguridad. A continuación, las entidades utilizarán un sistema para documentar los activos de información (por ejemplo, restringidos, internos, públicos o equivalentes), y etiquetar y gestionar dichos activos en consecuencia. Las normas y procedimientos de clasificación y manipulación deben comunicarse a todo el personal pertinente y revisarse periódicamente. Esto incluye normas para el acceso de escritorio y pantalla a la información y la creación o copia de información.

([20]) Artículo 21.

42. Cuando proceda, las entidades críticas deben tener en cuenta las normas nacionales aplicables para la protección de la información clasificada que se considere pertinente para la seguridad nacional.

43. Si las partes interesadas externas requieren acceso a activos de información, se anima a las entidades críticas a que consideren la posibilidad de elaborar orientaciones para los usuarios y acuerdos de no divulgación, u otros mecanismos contractuales pertinentes, según proceda.

44. Cualesquiera instalaciones que alberguen activos de información delicada (por ejemplo, archivos, salas de servidores) u otras zonas de las que puedan extraerse activos de información delicada deben designarse y supervisarse como zonas seguras, con controles especialmente estrictos de acceso, visualización y retirada.

45. Las entidades críticas deben velar por que los derechos de acceso se examinen y revisen periódicamente. Deben definirse períodos de conservación para los activos de información delicada. Una vez que se hayan superado estos períodos o que otros acontecimientos requieran la reclasificación de los activos de información, deben adoptarse las medidas adecuadas para sanear o destruir dichos activos.

46. Por lo que se refiere a las amenazas que plantean los sistemas no tripulados ([21]) (drones), se anima a las entidades críticas a que apliquen medidas para facilitar la detección, el seguimiento y la identificación de los sistemas no tripulados (por ejemplo, radares, escáneres de radiofrecuencia, cámaras térmicas/de luz diurna, sensores acústicos). Cuando sea posible, las entidades críticas también deben cooperar con los proveedores de servicios de telecomunicaciones para obtener acceso a los datos generados por las tecnologías de detección y comunicación integradas (ISAC), con vistas a detectar actividades no autorizadas con drones dentro de su perímetro de seguridad.

47. La amenaza de espionaje o vigilancia por parte de sistemas no tripulados no cooperativos debe mitigarse obstaculizando la visibilidad (aérea, marítima o terrestre) de activos o equipos sensibles (por ejemplo, ocultándolos o cambiándolos de ubicación) y, en su caso, garantizando que se alojen en instalaciones cerradas.

48. Las entidades críticas también deben mitigar la amenaza de sabotaje por parte de sistemas no tripulados no cooperativos de instalaciones, activos o equipos. Algunos ejemplos de medidas de mitigación son las redes o mallas antidrones y otras medidas de refuerzo estructural, como las ventanas resistentes a explosiones, el refuerzo de las placas del techo o los cerramientos estructurales completos.

49. Las entidades críticas podrán considerar la posibilidad de utilizar zonas geográficas para gestionar y mitigar los riesgos relacionados con operaciones con drones no autorizadas o inseguras en las proximidades de sus instalaciones. Toda decisión de establecer dichas zonas debe estar sujeta a una evaluación de riesgos y proporcionalidad realizada caso por caso, teniendo en cuenta la posible sensibilidad de la información que podría revelarse mediante la publicación de datos geográficos relacionados con las entidades críticas. Para ello, las entidades tendrían que cooperar con las autoridades nacionales competentes para garantizar que las zonas geográficas pertinentes estén debidamente definidas y publicadas digitalmente de conformidad con el marco de aviación aplicable. Dichas zonas deben permitir, como mínimo, que los operadores de drones se beneficien de funcionalidades de geoconsciencia. A medida que evolucionen las capacidades técnicas, y cuando el marco regulador lo apoye, las entidades críticas también pueden considerar la posibilidad de utilizar progresivamente funcionalidades de geovallado. El geovallado puede servir de salvaguardia preventiva al reducir la probabilidad de incursiones involuntarias de drones conformes en zonas sensibles. Las entidades críticas deben mantener un vínculo operativo directo con el gestor de la zona geográfica. Esto permitiría la visibilidad oportuna de la actividad de drones autorizados frente a no autorizados en sus proximidades y apoyaría mejor el conocimiento de la situación y la coordinación con las autoridades competentes.

50. Es esencial reforzar las asociaciones y la comunicación con los operadores de defensa contra los drones de las autoridades policiales y de defensa locales, u otros agentes legalmente autorizados con capacidades de mitigación (por ejemplo, interferencias de radiofrecuencia, suplantación y otras medidas cinéticas o no cinéticas). A tal efecto, se anima a las entidades críticas a que faciliten el uso de sistemas de defensa contra los drones para proteger su perímetro, de conformidad con el marco jurídico pertinente.

([21]) Comunicación (COM)2026 81, de 11 de febrero de 2026, titulada «Plan de acción sobre seguridad de drones y defensa antidrones».

D. MEDIDAS DE RESPUESTA, RESISTENCIA Y MITIGACIÓN [artículo 13, apartado 1, letra c), de la Directiva]

51. Se anima a las entidades críticas a que consideren las siguientes medidas para mitigar las consecuencias de los incidentes.

a) Gestión de crisis y catástrofes fuera del emplazamiento: medidas para mitigar las consecuencias adversas fuera del emplazamiento de un incidente perturbador grave y notificar rápidamente a las autoridades de gestión de crisis y catástrofes pertinentes para permitir la aplicación de medidas de protección fuera del emplazamiento. Esto requiere una estrecha coordinación con las autoridades pertinentes, el establecimiento de canales de comunicación probados y testados, así como ejercicios periódicos de gestión de crisis y catástrofes.

b) Asistencia externa: medidas para integrar eficazmente la asistencia externa en las acciones de respuesta *in situ* (incluida la gestión de accidentes graves, las acciones paliativas y la respuesta de emergencia).

c) Diseño de infraestructuras que fallen de forma segura garantizando que cualquier perturbación no afecte a la seguridad de las personas (incluida la seguridad del personal) y que se mitiguen los efectos en cascada en otros activos. Las características de seguridad ante fallos permiten a la infraestructura mantener las funciones esenciales durante un fallo o soportar procedimientos de parada controlada que eviten daños en los equipos y garanticen la capacidad de reinicio una vez que las condiciones lo permitan. El mantenimiento de las condiciones críticas de sustento vital o de la capacidad de supervivencia pasiva puede lograrse mediante una capacidad de almacenamiento adecuada, el control de la capacidad térmica, un suministro de reserva adecuado y la seguridad de los materiales peligrosos.

52. A la hora de diseñar infraestructuras seguras ante fallos, se anima a las entidades críticas a que tengan en cuenta los siguientes elementos: la capacidad de almacenamiento necesaria en los peores escenarios de fallo para mantener las condiciones críticas de sustento vital; el suministro de reserva necesario para mantener las operaciones críticas y apoyar el apagado controlado de las operaciones de infraestructura; la seguridad de todos los materiales peligrosos almacenados o presentes en infraestructuras críticas, garantizando su inclusión en los planes de codificación y gestión de materiales peligrosos y que se protejan adecuadamente en caso de fallo de la infraestructura; y medidas de seguridad térmica para los activos de infraestructuras críticas que alberguen personal o equipos sensibles a la temperatura. Dichas medidas podrán incluir tanto la capacidad de calefacción como de refrigeración para evitar víctimas de temperaturas extremas durante perturbaciones prolongadas.

53. Se anima a las entidades críticas a que adopten medidas para garantizar la disponibilidad, el mantenimiento y las capacidades de reparación y a que definan claramente sus necesidades de suministro, diversifiquen las fuentes de suministro a través de proveedores y rutas alternativos, apliquen el refuerzo y la redundancia de las infraestructuras y establezcan sistemas de salvaguardia con especificaciones sobre la función, la duración y la prioridad de restauración.

54. Se anima a las entidades críticas a que adopten las medidas adecuadas para garantizar la integridad de las redes y los sistemas informáticos y los programas informáticos utilizados en los equipos, en particular en relación con la dependencia de proveedores de alto riesgo y la protección contra las interferencias de las señales de radiofrecuencia y los ciberataques.

55. Los sistemas de alimentación alternativos pueden incluir generadores y baterías de alimentación ininterrumpida (SAI). Los sistemas de salvaguardia deben probarse periódicamente; la autonomía del combustible eléctrico debe mantenerse durante al menos setenta y dos horas y deben activarse los contratos de los proveedores para la asistencia urgente (suministro, intervenciones y reparaciones).

56. En cuanto a la resiliencia del suministro de agua, las entidades críticas podrán limitar el uso del agua a funciones esenciales durante las perturbaciones y utilizar fuentes alternativas, como pozos de salvaguardia, tanques de almacenamiento, unidades portátiles de tratamiento y opciones de almacenamiento flexibles. Se anima a las entidades críticas del sector del agua potable a que determinen los puntos de suministro prioritarios, con el fin de garantizar una respuesta adecuada en situaciones de contingencia o durante la interrupción del suministro. Al adoptar medidas de resiliencia, las entidades críticas deben garantizar que el agua destinada al consumo humano cumpla las normas de calidad establecidas en la Directiva (UE) 2020/2184 ([22]).

([22]) Directiva (UE) 2020/2184 del Parlamento Europeo y del Consejo, de 16 de diciembre de 2020, relativa a la calidad de las aguas destinadas al consumo humano (versión refundida) (DO L 435 de 23.12.2020, p. 1).

57. En el caso de otros servicios públicos sectoriales (por ejemplo, agua caliente, agua fría, caldera de vapor) y suministros (por ejemplo, productos químicos, materias primas, piezas de recambio), la planificación de contingencia en las cadenas de suministro debe considerar la posibilidad de pasar de modelos de inventario «justo a tiempo» a modelos de inventario «por si acaso», cuando proceda. Los sistemas alternativos deben incluir recursos y suministros de salvaguardia preestablecidos (reservas de seguridad y reservas de contingencia).

58. Se anima a las entidades críticas a que desarrollen programas de mantenimiento exhaustivos basados en las recomendaciones del fabricante, la experiencia operativa y las evaluaciones de riesgos. El mantenimiento predictivo puede llevarse a cabo utilizando tecnologías avanzadas de seguimiento con redes de sensores integradas. El mantenimiento periódico y predictivo basado en el rendimiento, que utiliza herramientas de análisis de datos e IA para supervisar el envejecimiento y los fallos de previsión, podría ser adecuado para optimizar el calendario de cualquier intervención necesaria. Deben establecerse protocolos claros para responder a las alertas del sistema de seguimiento, incluida la verificación de las alertas, la evaluación de la urgencia y la movilización de recursos de mantenimiento. Estos protocolos deben definir procedimientos de gradación ascendente para situaciones que requieran atención inmediata. Las inspecciones periódicas de las infraestructuras complementan el seguimiento automatizado.

59. Por lo que se refiere a la gobernanza, las entidades críticas deben considerar que la resiliencia debe integrarse desde los niveles más altos a los más bajos de la estructura de gobernanza. Deben establecer objetivos de resiliencia y adoptar una estrategia, una política y una planificación en materia de resiliencia, comunicarlos a las partes interesadas pertinentes sobre la base de la necesidad de conocer y llevar a cabo revisiones periódicas. Deben tenerse en cuenta las vulnerabilidades existentes y cómo ofrecer una mejor prevención, protección, respuesta, resistencia, mitigación, absorción, adaptación y recuperación en caso de un incidente.

60. Se anima a las entidades críticas a que establezcan jerarquías claras en la toma de decisiones. Debe consolidarse una competencia adecuada en materia de resiliencia en los consejos de administración y en las funciones de resiliencia o gestión de riesgos para garantizar una estrategia adecuada, una política adecuada y una planificación operativa adecuada para la resiliencia. Se anima a las entidades críticas a que consideren la posibilidad de nombrar a un responsable de resiliencia y a que garanticen una delimitación clara de las funciones y responsabilidades de coordinación para la aplicación de los objetivos de resiliencia.

61. También es pertinente en este contexto establecer y formalizar la cooperación con las autoridades públicas pertinentes, incluidos los responsables políticos, las autoridades policiales, los servicios de emergencia y los agentes de defensa. Se anima a las entidades críticas a que aclaren las funciones y los procedimientos para el intercambio de información, la notificación y coordinación de incidentes y las expectativas mutuas.

62. También puede considerarse el establecimiento y la formalización de la cooperación con los agentes pertinentes del sector privado en el propio sector de la entidad, otros sectores y otros Estados miembros.

63. Deben establecerse protocolos de comunicación de crisis para garantizar un flujo de información oportuno y preciso a las partes interesadas internas y externas (incluidos los clientes y el público) durante los incidentes. Las entidades críticas deben mantener plantillas de comunicación aprobadas previamente, rutinas de notificación a las partes interesadas y capacidades de comunicación multicanal, incluidos sistemas redundantes. Las comunicaciones deben adaptarse a distintos públicos, teniendo en cuenta la multiplicidad de lenguas y los requisitos de accesibilidad.

64. El diseño de redundancias a múltiples escalas garantiza que los servicios puedan prestarse a escala transfronteriza, nacional, regional y local con una interoperabilidad efectiva.

65. Se anima a las entidades críticas a que garanticen que los procedimientos de respuesta de emergencia abarquen sistemas de alerta multicanal con capacidades de geosegmentación, como el servicio espacial de alerta de emergencia por satélite del Programa Galileo, cadenas de mando de comunicación claras, incluidos los portavoces designados, y procedimientos operativos normalizados de riesgos específicos adaptados a los riesgos específicos de cada lugar. Las entidades críticas deben mantener equipos de emergencia, designar y formar equipos de respuesta a emergencias y garantizar que los procedimientos de evacuación sean accesibles y se practiquen con regularidad.

E. MEDIDAS DE RECUPERACIÓN [artículo 13, apartado 1, letra d), de la Directiva]

66. Para garantizar la continuidad de las operaciones, se anima a las entidades críticas a que consideren medidas de redundancia que garanticen que los servicios esenciales sigan prestándose cuando fallen los sistemas primarios. Estas medidas pueden incluir la identificación de los subservicios específicos más críticos para que sean los primeros en restablecerse (priorización del servicio), el mantenimiento de la capacidad de operar los equipos informáticos manualmente si los sistemas automatizados o basados en IA fallan o son manipulados, y la recuperación de la mano de obra en caso de incidente perturbador.

67. Los emplazamientos alternativos para la recuperación en caso de catástrofe pueden ser emplazamientos calientes (totalmente equipados para su uso inmediato), calientes (parcialmente equipados) o fríos (que requieren una configuración posterior a la perturbación). Los emplazamientos de salvaguardia deben estar suficientemente alejados de las instalaciones primarias y seguir siendo accesibles. En la medida de lo posible, deben tenerse en cuenta las instalaciones móviles (por ejemplo, los centros de mando). Las copias de seguridad deben almacenarse en lugares físicamente separados o aislados desde el punto de vista logístico.

68. Sin perjuicio de lo dispuesto en la Directiva SRI 2 ([23]), las entidades críticas deben elaborar y mantener planes globales de continuidad de las actividades basados en evaluaciones del impacto sobre las actividades que identifiquen las funciones esenciales, establezcan prioridades de recuperación y definan objetivos de tiempo de recuperación y objetivos de punto de recuperación, incluido el establecimiento de Acuerdos de Nivel de Servicio (ANS). Los planes de continuidad de las actividades deben especificar criterios claros de activación, asignación de recursos, funciones y mecanismos de coordinación para las fases de respuesta, recuperación, reanudación y restauración. Deben someterse a prueba, revisarse y actualizarse a intervalos planificados y tras cualquier incidente significativo o cambio en las operaciones.

69. Los procedimientos de gestión de crisis deben incluir estructuras de mando de incidentes con una autoridad decisoria claramente definida y planes de acción para incidentes documentados. Las entidades críticas deben considerar la posibilidad de crear equipos de crisis con funciones predefinidas, protocolos de escalada, formación adecuada y canales de comunicación (primarios y alternativos) para garantizar respuestas rápidas y coordinadas a los incidentes perturbadores.

70. La planificación de la mano de obra debe abordar los requisitos de capacidad de intervención mediante el mantenimiento de una lista de intervención rápida, programas de formación y acuerdos de ayuda mutua preestablecidos con organizaciones asociadas. Las entidades críticas deben desarrollar marcos de competencias y planificación de la sucesión para garantizar una profundidad adecuada en las funciones críticas y mantener la capacidad operativa durante interrupciones prolongadas o escasez de personal.

71. Para garantizar una recuperación efectiva de los incidentes, las entidades críticas deben aplicar protocolos de reactivación gradual que den prioridad al restablecimiento de las funciones esenciales sobre la base de la evaluación de riesgos o de las conclusiones del análisis de impacto sobre las actividades. Estos protocolos deben incluir procedimientos sistemáticos de validación de los sistemas críticos, pruebas exhaustivas de la integridad y funcionalidad de los datos, medidas de control de calidad y una transición controlada de las operaciones de emergencia a las operaciones normales mediante aumentos graduales de la capacidad y la supervisión del rendimiento.

72. Las investigaciones posteriores al incidente deben utilizar metodologías estructuradas, como el análisis de las causas subyacentes, para identificar las causas sistémicas en lugar de los síntomas inmediatos. Las revisiones posteriores a la acción deben llevarse a cabo tras todos los ejercicios e incidentes reales para extraer las lecciones aprendidas, y los resultados deben recogerse e integrarse sistemáticamente en procedimientos actualizados, programas de formación y evaluaciones de riesgos para evitar que se repitan y reforzar la resiliencia organizativa.

73. En términos de cadenas de suministro, la resiliencia es esencial en el contexto de la recuperación de incidentes perturbadores. En consonancia con sus evaluaciones de riesgos, las entidades críticas deben considerar la posibilidad de cartografiar la cadena de suministro para la prestación de sus servicios esenciales, desarrollar estrategias de resiliencia de la cadena de suministro a largo plazo y revisar y actualizar periódicamente el plan de contingencia de la cadena de suministro. Se les anima a que identifiquen cadenas de suministro alternativas en caso de que sus principales proveedores se vean afectados por incidentes perturbadores.

([23]) En particular, el artículo 21, apartado 2, letra c), de la Directiva SRI 2.

74. Las entidades críticas deben considerar el almacenamiento estratégico, incluidas las existencias de seguridad, los mecanismos de resuministro rápido y el almacenamiento externo protegido frente a amenazas comunes, de modo que, si se interrumpe la cadena de suministro, no se interrumpan los servicios esenciales.

75. También merece la pena considerar la posibilidad de establecer contratos formales con otras entidades del mismo sector para compartir recursos, equipos o personal durante un esfuerzo de recuperación a gran escala.

F. MEDIDAS DE GESTIÓN DE LA SEGURIDAD DEL EMPLEADO [artículo 13, apartado 1, letra e), de la Directiva]

76. Las amenazas relacionadas con el personal deben evaluarse y abordarse de modo que se mitigue el riesgo de error humano, sabotaje, amenazas internas y el riesgo de ausencia por enfermedad, emergencia o amenazas externas. Se anima a las entidades críticas a que identifiquen y elaboren listas de categorías de personal que ejerzan funciones esenciales, incluido el personal de proveedores de servicios externos (contratistas y subcontratistas).

77. Al establecer estas listas, las entidades críticas deben tener en cuenta las particularidades de los servicios esenciales prestados y vincularlos al personal que participe en su prestación. A tal fin, las entidades críticas deben conservar documentación clara, exhaustiva y actualizada de estas categorías de personal.

78. Además de las consideraciones anteriores relacionadas con los derechos de acceso, se anima a las entidades críticas a que determinen a quién y en qué condiciones se da acceso a los locales, las infraestructuras críticas y la información delicada. Deben establecerse procesos efectivos para conceder y revocar inmediatamente el acceso físico y al sistema, y los derechos de acceso deben aplicarse estrictamente.

79. Se anima a las entidades críticas a que concedan permisos únicamente según la necesidad de conocer o de acceder; solo debe concederse el nivel mínimo de acceso necesario para que el personal desempeñe su función. Deben ponerse en marcha estrategias de aplicación como el control de acceso basado en funciones ([24]), la autenticación reforzada y la gestión de identidades ([25]), la separación de funciones ([26]), las restricciones de base temporal y el acceso justo a tiempo ([27]), junto con auditorías y revisiones periódicas.

80. En cuanto a las comprobaciones de antecedentes personales, a fin de garantizar un alto nivel de seguridad de los empleados, es importante aplicar procedimientos internos sólidos para solicitar comprobaciones de antecedentes personales de conformidad con el artículo 14 de la Directiva y designar las categorías de personas que deben someterse a dichas comprobaciones de antecedentes personales. También deben establecerse procedimientos para tratar con los empleados cuya habilitación de seguridad se haya retirado.

81. Se anima a las entidades críticas a que definan la política de comprobación de antecedentes personales, indicando qué funciones son sensibles, qué funciones tienen acceso directo o remoto a las instalaciones, la información o los sistemas de control, y los tipos de comprobaciones que deben realizarse para cada función sensible, como la verificación de la identidad, los antecedentes penales y laborales y la educación.

82. Cuando proceda, las medidas deben ser coherentes con las actividades de verificación de antecedentes con arreglo al Reglamento de Ejecución (UE) 2024/2690 de la Comisión ([28]). También debe garantizarse la coherencia con las medidas de seguridad de los recursos humanos adoptadas por la entidad en cuestión de conformidad con el artículo 21, apartado 2, letra i), de la Directiva SRI 2.

([24]) Esto podría implicar definir funciones específicas como «guardia de seguridad física», asignar un conjunto predefinido de derechos de acceso y asignar personal a las funciones pertinentes.

([25]) Esto podría significar autenticación multifactor e identificadores únicos.

([26]) Esto podría significar diseñar controles de acceso para garantizar que ninguna persona tenga acceso suficiente para completar por sí sola un proceso crítico y de alto riesgo. Por ejemplo, la persona que aprueba un cambio del sistema no debe ser la misma que la persona que aplica el cambio.

([27]) El personal solo debe tener acceso temporal cuando lo necesite activamente para tareas específicas. En ese caso, el acceso debe revocarse inmediatamente. Debe existir una política que restrinja los derechos de acceso fuera de horas de trabajo específicas, cuando proceda.

([28]) Punto 10.2 del anexo.

83. Exigir al personal que tenga las cualificaciones y la formación adecuadas, así como impartir dicha formación, forma parte de garantizar una gestión adecuada de la seguridad de los empleados, sensibilizar al personal sobre las medidas de resiliencia y apoyar las medidas de resiliencia adoptadas por la entidad crítica en cuestión. La evaluación de riesgos de la entidad crítica, el tipo de servicios esenciales que presta y las medidas previstas o adoptadas deben determinar el tipo y el alcance de la formación necesaria para su personal, a fin de garantizar que este no solo conozca en general las medidas de resiliencia, sino que también sea competente desde el punto de vista técnico y procedimental para desempeñar sus funciones de manera resiliente.

84. Los requisitos de formación y cualificación se refieren, entre otras cosas, a la evaluación de riesgos (por ejemplo, para el personal de gestión/cumplimiento de los riesgos), la continuidad de las actividades y la gestión de crisis (por ejemplo, para el personal de continuidad de las actividades), la seguridad física (por ejemplo, para el personal de seguridad y las personas con derechos de acceso), la respuesta a incidentes y la mitigación de estos (por ejemplo, para el personal de operaciones, los agentes designados para la respuesta a incidentes), el control y la verificación del acceso (recursos humanos, personal de seguridad y gestores de funciones esenciales) y la sensibilización general sobre las medidas de resiliencia (de todos los empleados).

85. Los requisitos de cualificación dependen de las especificidades de la entidad crítica en cuestión y de los servicios esenciales que presta. El objetivo de dichos requisitos debe ser garantizar que el personal sea competente para ejecutar las tareas descritas en la evaluación de riesgos y el plan de resiliencia y en los protocolos de continuidad de la actividad y respuesta a incidentes integrados en el plan de resiliencia, dentro del ámbito de aplicación de las medidas de resiliencia que adopten las entidades críticas. Los requisitos de cualificación se refieren a tareas operativas y técnicas, organizativas y de gestión, o de seguridad e investigación. Las cualificaciones requeridas deben definirse en las políticas internas de resiliencia y recursos humanos de la entidad crítica en cuestión.

G. MEDIDAS DE SENSIBILIZACIÓN [artículo 13, apartado 1, letra f)]

86. Es esencial contar con un buen programa para sensibilizar al personal sobre las medidas de resiliencia adoptadas por la entidad crítica e inculcar una cultura de seguridad; el personal es un elemento vital en todas las fases del ciclo de resiliencia, desde la prevención de incidentes perturbadores y la mitigación de las amenazas internas hasta la respuesta a ellos mediante la activación de los procedimientos pertinentes, la notificación de incidentes y la garantía de la continuidad de las actividades, así como el restablecimiento de las operaciones a su estado anterior al incidente. Sin personal bien informado, incluso las mejores medidas técnicas, organizativas y de seguridad podrían fracasar.

87. Sujeto a información delicada y sobre la base de la necesidad de conocer, la sensibilización sobre las medidas de resiliencia garantiza una cultura de resiliencia óptima que hace de la resiliencia un valor compartido entre el personal de una entidad crítica y reduce el riesgo de amenazas internas o de ingeniería social.

88. Deben adoptarse medidas de sensibilización junto con las medidas para las prácticas básicas de ciberhigiene y la formación en ciberseguridad con arreglo a la Directiva SRI 2 ([29]).

89. La formación organizada por una entidad crítica debe vincularse a los requisitos de formación de la entidad crítica mencionados en los puntos 82 y 83 anteriores. Los cursos de formación deben abarcar las medidas de resiliencia adoptadas por la entidad de conformidad con el artículo 13, apartado 1, letras a) a e), de la Directiva, abarcando así todo el ciclo de vida de la resiliencia. Esto significa comprender el panorama de amenazas, el papel de la entidad crítica en el mantenimiento de funciones sociales vitales y las graves consecuencias de la perturbación del servicio, reconocer y notificar rápidamente actividades sospechosas, vulnerabilidades o incidentes inusuales, así como responder a los incidentes y mitigarlos. Debe preverse una formación específica para el personal con funciones esenciales.

90. También se anima a las entidades críticas a que consideren la posibilidad de impartir formación sobre enfoques sensibles al género que, junto con el seguimiento de los indicadores pertinentes, puedan reforzar la resiliencia, la rendición de cuentas y la sostenibilidad a largo plazo.

([29]) Artículo 21, apartado 2, letra g), de la Directiva SRI 2.

91. El material informativo compartido con el personal debe estar directamente relacionado con la evaluación de riesgos de la entidad y las medidas de resiliencia adoptadas. Estos materiales informativos deben ser claros y fáciles de digerir y deben explicar el papel fundamental de la entidad y el impacto de las perturbaciones en la sociedad y la economía, la cobertura de todos los riesgos, los principios básicos de seguridad, como «ver algo, decir algo», y el principio de «mínimo privilegio» para el acceso a información delicada.

92. Los materiales informativos podrían incluir materiales visuales de referencia rápida sobre, por ejemplo, violaciones de la seguridad física, pérdida de energía/conectividad, descubrimiento de paquetes sospechosos, diagramas de flujo de notificación de incidentes y recordatorios de continuidad de las actividades extraídos del plan de continuidad de las actividades, directrices de protección física y políticas de control de acceso. Para maximizar la sensibilización, estos materiales deben entregarse en múltiples formatos, como digital ([30]) y físico ([31]), y ser interactivos ([32]).

93. Los ejercicios son cruciales para validar el plan de resiliencia de una entidad crítica y garantizar que su personal pueda desempeñar de forma efectiva sus funciones durante un incidente real. En un enfoque que contemple todos los peligros, las entidades podrían organizar ejercicios basados en debates, como simulaciones teóricas ([33]), y ejercicios basados en operaciones, como simulacros ([34]).

94. Al organizar ejercicios, las entidades críticas deben centrarse en el resultado de su evaluación de riesgos, poner a prueba todo el ciclo de resiliencia y garantizar una buena coordinación intersectorial con otras entidades críticas, cuando proceda, para poner a prueba las dependencias intersectoriales. Deben garantizar la cooperación con las autoridades públicas pertinentes, como las fuerzas y cuerpos de seguridad, los bomberos, otros servicios de emergencia y los primeros intervinientes en general en caso de incidentes perturbadores, e implicar a estas autoridades públicas en los ejercicios.

([30]) Por ejemplo, intranet, módulos obligatorios de aprendizaje electrónico con cuestionarios, vídeos breves, salvapantallas con recordatorios de seguridad clave.

([31]) Por ejemplo, carteles, folletos o fichas de referencia rápida.

([32]) Por ejemplo, preguntas frecuentes.

([33]) Poner a prueba los procesos de coordinación, de toma de decisiones y de comunicación durante un incidente simulado (por ejemplo, fallo grave de la infraestructura, interrupción prolongada del suministro eléctrico, violación de la seguridad interior).

([34]) Poner a prueba un procedimiento específico y urgente, como la activación del generador de emergencia, la evacuación de una zona crítica o el aislamiento de un panel de control comprometido.