

## SEGURIDAD FÍSICA

### I. INTRODUCCIÓN

1. El presente anexo establece disposiciones para la aplicación del artículo 8. Define los requisitos mínimos para la protección física de los locales, edificios, oficinas, salas y demás zonas donde se maneje y almacene ICUE, incluidas las zonas que alberguen sistemas de información y comunicaciones.
2. Las medidas de seguridad física estarán concebidas para impedir el acceso no autorizado a ICUE para:
  - a) garantizar que la ICUE se maneje y se almacene adecuadamente;
  - b) permitir la separación del personal en su acceso a ICUE en función de su necesidad de conocer y, en su caso, de su habilitación de seguridad;
  - c) disuadir, impedir y detectar actividades no autorizadas, y
  - d) impedir o retrasar la entrada subrepticia o por la fuerza de intrusos.

### II. REQUISITOS Y MEDIDAS DE SEGURIDAD FÍSICA

3. Las medidas de seguridad física aplicables se determinarán sobre la base de una evaluación de las amenazas realizada por las autoridades competentes. La SGC y cada uno de los Estados miembros aplicarán un proceso de gestión de riesgos para proteger la ICUE en sus respectivos locales, de modo que se garantice un grado de protección física acorde con el riesgo evaluado. El proceso de gestión del riesgo tendrá en cuenta todos los factores pertinentes, en particular:
  - a) el grado de clasificación de la ICUE;
  - b) la forma y volumen de la ICUE, teniendo presente que grandes cantidades de ICUE o su recopilación podrían requerir la aplicación de medidas de protección más estrictas;
  - c) el entorno y la estructura de los edificios o zonas donde se guarde ICUE, y
  - d) la evaluación de las amenazas que representan tanto los servicios de inteligencia que tienen como objetivo la Unión y sus Estados miembros como el sabotaje, el terrorismo, la subversión u otras actividades delictivas.
4. Al aplicar el concepto de defensa en profundidad, las autoridades de seguridad competentes determinarán la combinación apropiada de las siguientes medidas de seguridad física que deben aplicarse. Estas pueden incluir una o más de las siguientes:
  - a) barreras perimetrales: se trata de barreras físicas que protegen los límites exteriores de la zona que precisa protección;
  - b) sistemas de detección de intrusiones (SDI): estos sistemas pueden emplearse para aumentar el grado de seguridad que brinda la barrera perimetral o, en determinadas salas y edificios, en sustitución o como complemento del personal de seguridad;
  - c) controles de acceso: los controles de acceso pueden aplicarse en una instalación, en un edificio o edificios de una instalación o en zonas o salas situadas dentro de un edificio; el control puede realizarse por medios electrónicos o electromecánicos, por medio de personal de seguridad, de un recepcionista o de ambos, o por cualquier otro medio físico;
  - d) personal de seguridad: puede emplearse, entre otros recursos, personal de seguridad formado, inspeccionado y, en caso necesario, con la debida habilitación de seguridad para disuadir a posibles intrusos que planeen una entrada encubierta;
  - e) sistemas de circuito cerrado de televisión (CCTV): estos sistemas pueden ser utilizados por el personal de seguridad para verificar incidentes y alarmas del SDI en emplazamientos de gran extensión o en el perímetro de una zona;
  - f) iluminación de seguridad: la iluminación de seguridad puede emplearse para disuadir a posibles intrusos, además de proporcionar la iluminación necesaria para una vigilancia eficaz, bien directamente por parte del personal de seguridad, bien de forma indirecta a través de un CCTV, y
  - g) cualquier otra medida apropiada de seguridad física destinada a disuadir o detectar entradas no autorizadas o a prevenir la pérdida o deterioro de ICUE.

5. Podrá autorizarse a la autoridad competente para llevar a cabo, en las entradas y las salidas, registros que disuadan de todo intento no autorizado de introducir material en los locales o edificios o de sacar de ellos ICUE.
6. Cuando exista el riesgo de que una ICUE sea objeto de miradas indiscretas, incluso accidentalmente, se tomarán medidas adecuadas para contrarrestar ese riesgo.
7. Para los nuevos establecimientos, los requisitos de seguridad física y sus especificaciones funcionales se definirán en el momento de la planificación y el diseño del mismo. Para los establecimientos ya existentes, los requisitos de seguridad física se aplicarán en la mayor medida posible.

### III. EQUIPO PARA LA PROTECCIÓN FÍSICA DE LA ICUE

8. La autoridad de seguridad competente se asegurará de que el equipo que se adquiera para la protección física de la ICUE (armarios de seguridad, trituradoras de papel, cerraduras, sistemas electrónicos de control de acceso, sistemas de detección de intrusos, sistemas de alarma) cumpla los estándares técnicos y los requisitos mínimos aprobados.
9. Las especificaciones técnicas del equipo que vaya a emplearse para la protección física de la ICUE se establecerán en directrices de seguridad que deberán ser aprobadas por el Comité de Seguridad.
10. Los sistemas de seguridad se inspeccionarán periódicamente, y se realizará un mantenimiento del equipo con regularidad. Para las operaciones de mantenimiento se tendrá en cuenta el resultado de las inspecciones, a fin de garantizar que el equipo siga funcionando óptimamente.
11. La eficacia de cada medida de seguridad y del sistema de seguridad en su conjunto se reevaluará en cada inspección.

### IV. ZONAS FÍSICAMENTE PROTEGIDAS

12. Para la protección física de la ICUE se establecerán dos tipos de zonas físicamente protegidas, o sus equivalentes nacionales:
  - a) zonas administrativas, y
  - b) zonas de acceso restringido (incluidas las zonas de acceso restringido protegidas por medios técnicos).

En la presente Decisión, toda referencia a las zonas administrativas y a las zonas de acceso restringido, incluidas las zonas de acceso restringido protegidas por medios técnicos, se entenderá que incluye asimismo las equivalentes nacionales.

13. La autoridad de seguridad competente decidirá si una zona cumple los requisitos para ser designada zona administrativa, zona de acceso restringido o zona acceso restringido protegida por medios técnicos.
14. Para las zonas administrativas:
  - a) se establecerá un perímetro visiblemente definido que permita el control de personas y, cuando sea posible, de vehículos;
  - b) solo se permitirá el acceso sin escolta a las personas debidamente autorizadas por la autoridad competente, y
  - c) todas las demás personas deberán ser acompañadas en todo momento o ser objeto de controles equivalentes.
15. Para las zonas de acceso restringido:
  - a) se establecerá un perímetro visiblemente definido y protegido en el que se controlen todas las entradas y salidas mediante un sistema de pases o de identificación personal;
  - b) solo se permitirá el acceso sin acompañamiento a las personas que tengan una habilitación de seguridad y una autorización específica para entrar en la zona por su necesidad de conocer, y
  - c) todas las demás personas deberán ser acompañadas en todo momento o ser objeto de controles equivalentes.

16. Cuando la entrada en una zona de acceso restringido equivalga en la práctica a tener acceso directo a la información clasificada que se encuentre en la zona, se aplicarán además los siguientes requisitos:
  - a) se indicará con claridad el máximo grado de clasificación de seguridad de la información que se encuentre normalmente en dicha zona;
  - b) todos los visitantes necesitarán una autorización específica para acceder a la zona, estarán acompañados en todo momento y debidamente habilitados, salvo que se tomen medidas para que no sea posible que accedan a la ICUE.
17. Las zonas de acceso restringido protegidas contra escuchas serán designadas como zonas de acceso restringido protegidas por medios técnicos. Se aplicarán los requisitos adicionales siguientes:
  - a) estas zonas estarán equipadas con sistemas de detección de intrusos, se cerrarán con llave cuando no estén ocupadas y se vigilarán cuando estén ocupadas; todas las llaves se controlarán de acuerdo con lo dispuesto en la sección VI;
  - b) todas las personas y el material que entren en estas zonas serán objeto de control;
  - c) estas zonas serán objeto de inspecciones físicas o técnicas regularmente, según lo requiera la autoridad de seguridad competente; además, serán inspeccionadas también siempre que se haya producido o se sospeche que se ha producido una entrada no autorizada, y
  - d) no habrá en estas zonas ninguna línea de comunicaciones, teléfono ni otro equipo de comunicaciones, ni aparatos eléctricos o electrónicos, salvo los que estén autorizados.
18. No obstante lo dispuesto en el punto 17, letra d), todos los equipos de comunicaciones y todos los aparatos eléctricos o electrónicos deberán ser examinados por la autoridad de seguridad competente antes de que puedan ser utilizados en zonas donde se estén celebrando reuniones o realizando trabajos en que se maneje información clasificada de grado SECRET UE/EU SECRET y superior, y cuando la amenaza para la ICUE se considere elevada, con el fin de garantizar que ninguna información en claro pueda transmitirse de manera involuntaria o ilícita a través de dichos equipos más allá del perímetro de la zona de acceso restringido de que se trate.
19. Las zonas de acceso restringido que no estén ocupadas por personal de servicio las 24 horas del día se inspeccionarán, en su caso, al final de la jornada normal de trabajo y a intervalos aleatorios fuera de dicha jornada, a menos que se haya instalado en ellas un sistema de detección de intrusos.
20. Se podrán establecer con carácter temporal zonas de acceso restringido y zonas de acceso restringido protegidas por medios técnicos en una zona administrativa para la celebración de una reunión clasificada u otro motivo similar.
21. Para cada zona de acceso restringido se definirán procedimientos operativos de seguridad en los que se disponga lo siguiente:
  - a) el grado de la ICUE que puede manejarse o almacenarse en la zona;
  - b) las medidas de vigilancia y protección que hayan de aplicarse;
  - c) las personas autorizadas para entrar en ella sin acompañamiento en virtud de su necesidad de conocer y de su habilitación de seguridad;
  - d) si ha lugar, los procedimientos aplicables a los acompañantes o a la protección de la ICUE cuando se autorice la entrada de cualquier otra persona en la zona, y
  - e) cualquier otra medida o procedimiento pertinente.
22. Las cámaras acorazadas se ubicarán en zonas de acceso restringido. Los muros, suelos, techos, ventanas y puertas que puedan cerrarse con llave deberán haber sido aprobados por la autoridad de seguridad competente y ofrecer una protección equivalente a la de un contenedor de seguridad aprobado para el almacenamiento de ICUE del mismo grado de clasificación.

## V. MEDIDAS DE PROTECCIÓN FÍSICA PARA EL MANEJO Y ALMACENAMIENTO DE LA ICUE

23. La ICUE de grado RESTREINT UE/EU RESTRICTED se podrá manejar:
  - a) en una zona de acceso restringido;
  - b) en una zona administrativa, siempre que se impida el acceso a la ICUE a personas no autorizadas, o
  - c) fuera de una zona de acceso restringido o de una zona administrativa, siempre que el poseedor transporte la ICUE de conformidad con los puntos 28 a 41 del anexo III y se haya comprometido a cumplir las medidas compensatorias establecidas en las instrucciones de seguridad definidas por la autoridad de seguridad competente para garantizar que la ICUE está protegida del acceso de personas no autorizadas.

24. La ICUE de grado RESTREINT UE/EU RESTRICTED se guardará en muebles de oficina adecuadamente cerrados con llave en las zonas administrativas o las zonas de acceso restringido. La ICUE de dicho grado podrá almacenarse temporalmente fuera de una zona de acceso restringido o de una zona administrativa, siempre que el poseedor se haya comprometido a cumplir las medidas compensatorias establecidas en las instrucciones de seguridad definidas por la autoridad de seguridad competente.
25. La ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL o SECRET UE/EU SECRET se podrá manejar:
- en una zona de acceso restringido;
  - en una zona administrativa, siempre que se impida el acceso a la ICUE a personas no autorizadas, o
  - fuera de una zona de acceso restringido o de una zona administrativa siempre que el poseedor:
    - transporte la ICUE de conformidad con los puntos 28 a 41 del anexo III,
    - se haya comprometido a cumplir las medidas compensatorias establecidas en las instrucciones de seguridad definidas por la autoridad de seguridad competente para garantizar que el acceso a la ICUE se impide a personas no autorizadas,
    - mantenga la ICUE en todo momento bajo su control personal, y
    - en el caso de documentos en papel, haya notificado el hecho al registro correspondiente.
26. La ICUE de grado CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET se almacenará en una zona de acceso restringido, bien dentro de un contenedor de seguridad o bien en una cámara acorazada.
27. La ICUE de grado TRÈS SECRET UE/EU TOP SECRET se manejará en una zona de acceso restringido.
28. La ICUE de grado TRÈS SECRET UE/EU TOP SECRET se almacenará en una zona de acceso restringido en una de las condiciones siguientes:
- en un contenedor de seguridad conforme a lo dispuesto en el punto 8, con al menos uno de los controles adicionales siguientes:
    - protección continua o verificación periódica por personal de seguridad o de servicio habilitado,
    - un SDI aprobado, junto con personal de seguridad para intervención en caso de incidente;
  - en una cámara acorazada con SDI, junto con personal de seguridad para intervención en caso de incidente.
29. En el anexo III se recogen las normas para el transporte de ICUE fuera de las zonas físicamente protegidas.
- VI. CONTROL DE LLAVES Y COMBINACIONES EMPLEADAS PARA LA PROTECCIÓN DE ICUE
30. La autoridad de seguridad competente definirá procedimientos de gestión de las llaves y las combinaciones de las oficinas, salas, cámaras acorazadas y contenedores de seguridad. Estos procedimientos deberán evitar accesos no autorizados.
31. Las combinaciones serán confiadas al menor número posible de personas que necesiten conocerlas. Las combinaciones de los contenedores de seguridad y cámaras acorazadas en los que se guarde ICUE se modificarán:
- al recibir un nuevo contenedor;
  - cada vez que cambie el personal que conoce la combinación;
  - cada vez que se haya producido o se sospeche que se ha producido una situación de comprometimiento;
  - cuando se hayan realizado operaciones de mantenimiento o reparación de una cerradura, y
  - al menos cada 12 meses.
-