

Bruselas, 29 de marzo de 2022
(OR. en)

**Expediente interinstitucional:
2022/0084(COD)**

**7670/22
ADD 3**

**CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34**

PROPUESTA

De:	Por la secretaria general de la Comisión Europea, D. ^a Martine DEPREZ, directora
Fecha de recepción:	22 de marzo de 2022
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.º doc. Ción.:	COM(2022) 119 final - Annex 3
Asunto:	ANEXO 3 de la Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO sobre la seguridad de la información en las instituciones, órganos y organismos de la Unión

Adjunto se remite a las Delegaciones el documento – COM(2022) 119 final - Annex 3.

Adj.: COM(2022) 119 final - Annex 3

Bruselas, 22.3.2022
COM(2022) 119 final

ANNEX 3

ANEXOS

de la

**Propuesta de REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO
sobre la seguridad de la información en las instituciones, órganos y organismos de la
Unión**

{SWD(2022) 65 final} - {SWD(2022) 66 final}

ANEXO III

Medidas para la protección física de la información clasificada de la Unión Europea (ICUE)

Equipos y medidas organizativas para la protección física de la ICUE

1. Las zonas administrativas deberán cumplir los siguientes requisitos:
 - a) contar con un perímetro visiblemente definido que permita el control de las personas y, cuando sea posible, de los vehículos;
 - b) garantizar que las ventanas que puedan permitir un acceso visual no autorizado a ICUE en la zona sean opacas o estén equipadas con persianas, cortinas u otros tipos de protección;
 - c) el acceso no acompañado solo se concederá a las personas debidamente autorizadas por la autoridad de seguridad de la institución u órgano de la Unión de que se trate;
 - d) todas las demás personas deberán ser acompañadas en todo momento o ser objeto de controles equivalentes.
2. Además de los requisitos establecidos en el punto 1, las zonas de acceso restringido deberán cumplir los siguientes requisitos:
 - a) tener un perímetro claramente definido y protegido a través del cual se controle en todo momento la entrada y la salida;
 - b) no disponer de ninguna línea de comunicación, teléfono ni otro equipo de comunicaciones, ni aparatos eléctricos o electrónicos, salvo los que estén autorizados;
 - c) estar equipadas con un sistema de control de acceso y un sistema de detección instantánea de intrusiones, combinado con personal de seguridad;
 - d) ser inspeccionadas al final del horario normal de trabajo y a intervalos aleatorios fuera del horario normal de trabajo, cuando el personal de servicio no lo ocupe 24 horas y no exista un sistema de detección instantánea de intrusiones;
 - e) estar gestionadas por personal de seguridad formado, supervisado y debidamente habilitado;
 - f) contar con procedimientos operativos de seguridad que incluyan los siguientes elementos:
 - i) el grado de ICUE que puede tratarse o almacenarse en la zona;
 - ii) las medidas de vigilancia y protección que hayan de aplicarse;
 - iii) las personas autorizadas para entrar en ella sin acompañamiento en virtud de su habilitación de seguridad para tratar ICUE y de su necesidad de conocer;
 - iv) si ha lugar, los procedimientos aplicables a los acompañantes o a la protección de la ICUE cuando se autorice la entrada de otras personas en la zona;
 - v) cualquier otra medida o procedimiento pertinente.

3. Cuando la entrada en una zona de acceso restringido constituya un acceso directo a la información clasificada que contiene, la zona deberá considerarse como zona de clase I y, cuando no sea así, como zona de clase II.

Para ambas clases de zonas de acceso restringido y además de los requisitos establecidos en el punto 2, el servicio o responsable de seguridad de la institución u órgano de la Unión de que se trate deberá indicar claramente el grado de clasificación de seguridad más alto de la información que se conserve normalmente en la zona y deberá definir claramente un perímetro que permita el control de las personas y, en la medida de lo posible, de los vehículos.

Las instituciones y órganos de la Unión deben garantizar que las personas que accedan a una zona de acceso restringido cumplan los siguientes criterios:

- a) contar con una autorización específica para entrar en la zona;
 - b) estar acompañadas en todo momento;
 - c) estar debidamente habilitadas, a menos que se adopten medidas para garantizar que no sea posible acceder a ICUE.
4. Las zonas de acceso restringido protegidas contra las escuchas pasivas y activas deberán ser designadas zonas de acceso restringido protegidas por medios técnicos y, además de los requisitos aplicables a las zonas de acceso restringido, se les aplicarán los siguientes requisitos:
- a) deberán estar equipadas con un sistema de detección instantánea de intrusiones, estar cerradas con llave cuando no estén ocupadas y ser vigiladas cuando estén ocupadas. Las llaves deberán utilizarse con arreglo al artículo 29, apartado 3;
 - b) la autoridad de seguridad de la institución u órgano de la Unión de que se trate deberá inspeccionar la zona periódicamente, de forma física o técnica, o de ambas formas. Estas inspecciones también se efectuarán siempre que se haya producido o se sospeche que se ha producido una entrada no autorizada;
 - c) deberá tener la adecuada protección acústica y TEMPEST.
5. Todas las personas que entren en zonas de acceso restringido protegidas por medios técnicos deberán cumplir los requisitos establecidos en el punto 3.
6. 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.
7. En las zonas de acceso restringido se instalarán cámaras acorazadas. Una cámara acorazada es una sala de construcción reforzada en la que la autoridad de seguridad de la institución u órgano de la Unión de que se trate apruebe los muros, suelos, techos, ventanas y puertas que puedan cerrarse con llave. Dichas salas deberán ofrecer una protección equivalente a un contenedor de seguridad aprobado para el almacenamiento de ICUE del mismo grado de clasificación.

Medidas de protección física para el tratamiento y almacenamiento de ICUE

8. La ICUE de grado RESTREINT UE/EU RESTRICTED deberá tratarse y almacenarse en cualquiera de los siguientes lugares:
- 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;

- c) fuera de una zona de acceso restringido o de una zona administrativa, siempre que el poseedor se haya comprometido a cumplir las medidas decididas por la autoridad de seguridad de cada institución y órgano de la Unión.
9. 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. Podrá almacenarse temporalmente fuera de una zona administrativa o de una zona de acceso restringido siempre que la persona que la trate se haya comprometido a almacenar los documentos en cuestión en muebles de oficina apropiados cerrados con llave cuando no se estén leyendo o discutiendo.
 10. Las instituciones y órganos de la Unión podrán manejar y almacenar información RESTREINT UE/EU RESTRICTED fuera de sus sitios web, siempre que la información pertinente esté adecuadamente protegida. A tal fin, las instituciones y órganos de la Unión deberán cumplir las medidas previstas en el punto 8, letra c).
 11. La ICUE de grado RESTREINT UE/EU RESTRICTED deberá tratarse y almacenarse en cualquiera de los siguientes lugares:
 - 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;
 - c) fuera de una zona de acceso restringido o de una zona administrativa, siempre que la persona que la trate se haya comprometido a cumplir las medidas compensatorias decididas por la autoridad de seguridad de cada institución y órgano de la Unión. Además, el poseedor de ICUE deberá adoptar las siguientes medidas:
 - i) notificar al registro pertinente el hecho de que los documentos clasificados se estén tratando fuera de las zonas protegidas;
 - ii) mantener el documento bajo su control en todo momento.
 12. La información CONFIDENTIEL UE/EU CONFIDENTIAL y SECRET UE/EU SECRET deberá almacenarse en una zona de acceso restringido acreditada a ese grado por la autoridad competente de acreditación de seguridad de la institución u órgano de la Unión de que se trate, ya sea dentro de un contenedor de seguridad o dentro de una cámara acorazada.
 13. Los documentos clasificados CONFIDENTIEL UE/EU CONFIDENTIAL o superior solo podrán ser copiados por el registro correspondiente.
 14. La información TRES SECRET UE/EU TOP SECRET deberá tratarse y almacenarse en una zona de acceso restringido acreditada a ese grado. A tal fin, las instituciones y órganos de la Unión podrán celebrar las disposiciones necesarias para utilizar una zona de acceso restringido alojada y acreditada al grado adecuado por la autoridad de acreditación de seguridad de otra institución u órgano de la Unión.
 15. La información TRES SECRET UE/EU SECRET deberá almacenarse en una zona de acceso restringido acreditada a ese grado por la autoridad competente de acreditación de seguridad de la institución u órgano de la Unión de que se trate, respetando las siguientes condiciones:
 - a) se almacenará en un contenedor de seguridad aprobado por la autoridad de seguridad de cada institución y órgano de la Unión, aplicando una de las medidas adicionales siguientes:

- i) protección continua o verificación periódica por personal de seguridad o de servicio habilitado;
 - ii) un sistema de detección instantánea de intrusiones aprobado, junto con personal de seguridad que pueda intervenir en caso de incidente;
- b) una cámara acorazada dotada de un sistema de detección instantánea de intrusiones, junto con personal de seguridad que pueda intervenir en caso de incidente.