ANEXO IV

PROTECCIÓN DE LA ICUE MANEJADA EN LOS SIC

I. INTRODUCCIÓN

1. El presente anexo establece disposiciones para la aplicación del artículo 10.

2. Las siguientes propiedades y conceptos relativos a la GI se consideran esenciales para la seguridad y correcto funcionamiento de las operaciones realizadas en los SIC:

Autenticidad: la garantía de que la información es verídica y procede de fuentes de buena fe;

Disponibilidad: la propiedad de ser accesible y utilizable en el momento que lo requiera una entidad autorizada;

Confidencialidad: la propiedad de la información de no ser revelada a personas, organismos o procesos no autorizados;

Integridad: la propiedad de salvaguardar la exactitud y completitud de la información y los activos;

No repudio: la capacidad de demostrar que un acto o suceso ha ocurrido efectivamente, de modo que el acto o suceso no pueda negarse posteriormente.

II. PRINCIPIOS DE LA GI

3. Las disposiciones que se establecen a continuación constituyen el punto de partida para garantizar la seguridad de todo sistema que maneje ICUE por parte de un SIC. Los requisitos detallados para dar cumplimiento a las presentes disposiciones se definirán en políticas y directrices de seguridad para la GI.

Gestión del riesgo de seguridad

4. La gestión del riesgo de seguridad será parte integrante de la definición, desarrollo, funcionamiento y mantenimiento de los SIC. La gestión del riesgo (evaluación, tratamiento, aceptación y comunicación) se llevará a cabo como un proceso iterativo y de forma conjunta por parte de los representantes de los propietarios del sistema, las autoridades del proyecto, las autoridades operativas y las autoridades responsables de la aprobación de la seguridad, recurriendo a un método de evaluación del riesgo que haya demostrado su eficacia y sea transparente y plenamente comprensible. El alcance del SIC y de sus activos estará claramente definido ya desde el comienzo del proceso de gestión del riesgo.

5. Las autoridades competentes examinarán las amenazas potenciales para el SIC y mantendrán evaluaciones de la amenaza actualizadas y exactas que reflejen el entorno operativo del momento. Actualizarán continuamente sus conocimientos de las cuestiones relativas a la vulnerabilidad y revisarán periódicamente la evaluación de la vulnerabilidad para hacer frente al entorno cambiante de las tecnologías de la información (TI).

6. El tratamiento del riesgo de seguridad tendrá por objeto aplicar un conjunto de medidas de seguridad que creen un equilibrio satisfactorio entre las necesidades de los usuarios, el coste y el riesgo de seguridad residual.

7. Los requisitos específicos, escala y grado de detalle determinados por la autoridad de acreditación de seguridad pertinente para acreditar un SIC serán proporcionales al riesgo evaluado, teniendo en cuenta todos los factores pertinentes, con inclusión del grado de clasificación de la ICUE manejada por el SIC. La acreditación incluirá una declaración formal sobre el riesgo residual y la aceptación de dicho riesgo por parte de una autoridad competente.

Seguridad a lo largo del ciclo de vida del SIC

8. Garantizar la seguridad constituirá un requisito a lo largo de todo el ciclo de vida del SIC, desde su comienzo hasta su retirada del servicio.

9. Para cada fase del ciclo de vida de un sistema, se determinará el papel y la interacción de todo participante en un SIC con respecto a su seguridad.

10. Cualquier SIC, incluidas sus medidas de seguridad de carácter técnico y no técnico, será objeto de pruebas de seguridad durante su proceso de acreditación, para asegurarse de que se obtiene el nivel adecuado de garantía y verificar que esos sistemas están correctamente aplicados, integrados y configurados.

11. Se realizarán periódicamente evaluaciones, inspecciones y exámenes de seguridad durante el funcionamiento y el mantenimiento del SIC y cuando se produzcan circunstancias excepcionales.

12. La documentación de seguridad de un SIC irá evolucionando a lo largo de su ciclo de vida como parte integrante del proceso de gestión de la configuración y del cambio.

Mejores prácticas

13. La SGC y los Estados miembros colaborarán en el desarrollo de mejores prácticas para la protección de la ICUE manejada en los SIC. Las directrices sobre las mejores prácticas establecerán medidas de seguridad técnicas, físicas, de organización y de procedimiento para los SIC, de probada eficacia para contrarrestar determinadas amenazas y vulnerabilidades.

14. La protección de la ICUE manejada en SIC se basará en las enseñanzas obtenidas por las entidades que intervienen en la GI tanto dentro de la Unión como fuera de ella.

15. La difusión y ulterior aplicación de las mejores prácticas contribuirán a lograr un nivel equivalente de garantía en los distintos SIC que manejan ICUE y que funcionan en la SGC y en los Estados miembros.

Defensa en profundidad

16. Para paliar los riesgos en los SIC, se aplicará una serie de medidas de seguridad de carácter técnico y no técnico, organizadas a modo de defensa en barreras sucesivas. Esas barreras de defensa incluirán:

    a) *disuasión:* medidas de seguridad destinadas a desalentar a los adversarios que planeen un ataque a un SIC;

    b) *prevención:* medidas de seguridad destinadas a impedir u obstaculizar un ataque a un SIC;

    c) *detección:* medidas de seguridad destinadas a descubrir que se ha producido un ataque a un SIC;

    d) *resistencia:* medidas de seguridad destinadas a limitar las consecuencias de un ataque a un bloque mínimo de información o de activos de un SIC y a impedir mayores daños, y

    e) *recuperación:* medidas de seguridad destinadas a volver al estado anterior de seguridad del SIC.

    El grado de rigor de estas medidas de seguridad se determinará mediante una evaluación del riesgo.

17. La ANS u otra autoridad competente se asegurará:

    a) de que se pongan en práctica capacidades de ciberdefensa a fin de responder a amenazas que puedan traspasar los límites de las organizaciones o las fronteras nacionales, y

    b) de que se coordinen las respuestas y de que se comparta la información sobre dichas amenazas, los incidentes y los riesgos conexos (capacidades de respuesta para urgencias informáticas).

Principio de minimalidad y privilegios mínimos

18. Únicamente se pondrán en marcha las funciones, dispositivos y servicios esenciales para cubrir las necesidades operativas, con el fin de evitar riesgos innecesarios.

19. Los usuarios de los SIC y los procesos automáticos solo obtendrán el acceso, los privilegios o los permisos que necesiten para realizar su cometido, con el fin de limitar los daños resultantes de accidentes, errores o uso no autorizado de recursos de los SIC.

20. Los procedimientos de registro que efectúa un SIC, cuando es preciso, se verificarán como parte del proceso de acreditación.

Concienciación de la GI

21. La conciencia de los riesgos y de las medidas de seguridad disponibles constituye la primera línea de defensa de la seguridad de los SIC. En particular, todas las personas que intervienen en el ciclo de vida de un SIC, incluidos sus usuarios, deben ser conscientes:

    a) de que los fallos de seguridad pueden perjudicar seriamente al SIC;

    b) de los posibles daños a terceros que pueden derivarse de la interconectividad e interdependencia, y

    c) de que son responsables de la seguridad del SIC y se les pedirán cuentas según la función que desempeñen en los sistemas y procesos.

22. Para garantizar que son conscientes de las responsabilidades que conlleva la seguridad, será obligatoria la formación y concienciación en relación con la GI para todo el personal implicado, tanto los altos directivos como los usuarios de SIC.

Evaluación y aprobación de los productos de seguridad de TI

23. El grado de confianza necesario en las medidas de seguridad, definido como nivel de garantía, se determinará con arreglo al resultado del proceso de gestión del riesgo y en consonancia con las correspondientes políticas y directrices de seguridad.

24. El nivel de garantía se verificará recurriendo a procedimientos y metodologías reconocidos internacionalmente o aprobados en el plano nacional. Aquí deben incluirse principalmente la evaluación, los controles y las auditorías.

25. Los productos criptológicos de protección de la ICUE serán evaluados y aprobados por una ACC de un Estado miembro.

26. Antes de recomendarlos para su aprobación por el Consejo o el Secretario General, de conformidad con el artículo 10, apartado 6, dichos productos criptológicos deberán superar una segunda evaluación realizada por la autoridad debidamente acreditada (ADA) de un Estado miembro que no haya participado en el diseño o fabricación del equipo considerado. El grado de detalle exigido en la segunda evaluación dependerá del grado máximo de clasificación de la ICUE que se prevé proteger con dichos productos. El Consejo aprobará una política de seguridad sobre la evaluación y aprobación de los productos criptológicos.

27. Cuando ello esté justificado por motivos operativos específicos, el Consejo o el Secretario General, según proceda, podrá, previa recomendación del Comité de Seguridad, dispensar del cumplimiento de los requisitos recogidos en los puntos 25 o 26 del presente anexo y otorgar una aprobación provisional durante un período específico, de conformidad con el procedimiento establecido en el artículo 10, apartado 6.

28. El Consejo, por recomendación del Comité de Seguridad, podrá aceptar el proceso de evaluación, selección y aprobación de los productos criptológicos de un tercer Estado o de una organización internacional y considerar en consecuencia que tales productos criptológicos quedan aprobados a efectos de protección de ICUE cedida a dicho tercer Estado o dicha organización internacional.

29. Una ADA será una ACC de un Estado miembro, acreditada mediante criterios objetivos establecidos por el Consejo para realizar la segunda evaluación de los productos criptológicos de protección de la ICUE.

30. El Consejo aprobará una política de seguridad sobre la cualificación y aprobación de productos de seguridad de TI no criptológicos.

Transmisión dentro de zonas de acceso restringido y zonas administrativas

31. No obstante las disposiciones de la presente Decisión, cuando la transmisión de ICUE se limite a zonas de acceso restringido o zonas administrativas, podrá utilizarse la transmisión no cifrada, o cifrada en un nivel inferior, en base al resultado de un proceso de gestión del riesgo y previa aprobación de la AAS.

Interconexión segura de los SIC

32. A los efectos de la presente Decisión, por interconexión se entenderá la conexión directa de dos o más sistemas de TI con objeto de compartir datos y otros recursos de información (por ejemplo, comunicación) de forma unidireccional o multidireccional.

33. Todo SIC tratará como no fiable a cualquier sistema de TI interconectado y aplicará medidas protectoras para controlar el intercambio de información clasificada.

34. Con relación a todas las interconexiones de un SIC con otro sistema de TI, se observarán los siguientes requisitos básicos:

a) las autoridades competentes enunciarán y aprobarán los requisitos operacionales o de servicio de dichas interconexiones;

b) la interconexión se someterá a un proceso de gestión del riesgo y acreditación y necesitará la aprobación de las autoridades de acreditación de seguridad competentes, y

c) se pondrán en marcha servicios de protección del perímetro de todos los SIC.

35. No habrá interconexión entre un SIC acreditado y una red desprotegida o pública, salvo cuando el SIC tenga instalado a tal fin un servicio de protección de perímetro aprobado, que actúe entre el SIC y la red desprotegida o pública. Las medidas de seguridad de tales interconexiones serán examinadas por la autoridad de garantía de la información competente y aprobadas por la autoridad de acreditación de seguridad competente.

Cuando la red desprotegida o pública se utilice únicamente para el transporte y los datos estén cifrados con un producto criptológico aprobado en conformidad con el artículo 10, se considerará que la conexión no es una interconexión.

36. Quedarán prohibidas las interconexiones directas o dispuestas en cascada de un SIC acreditado para manejar información clasificada de grado TRÈS SECRET UE/EU TOP SECRET con redes públicas o desprotegidas.

Soportes de almacenamiento informático

37. Los soportes de almacenamiento informático se destruirán con arreglo a un procedimiento aprobado por la autoridad de seguridad competente.

38. La reutilización, la reducción del grado de clasificación y la desclasificación de los soportes de almacenamiento informático se efectuarán de conformidad con unas directrices de seguridad establecidas de conformidad con el artículo 6, apartado 2.

Circunstancias de emergencia

39. No obstante lo dispuesto en la presente Decisión, podrán aplicarse los procedimientos específicos que se describen a continuación en casos de emergencia, por ejemplo, en situaciones de crisis, conflicto o guerra, inminentes o reales, o en circunstancias operativas excepcionales.

40. La ICUE podrá transmitirse utilizando productos criptológicos que hayan sido certificados para un grado de clasificación inferior o sin cifrar con el consentimiento de la autoridad competente, si resulta evidente que un retraso podría causar un daño superior al que acarrea la revelación del material clasificado y si:

a) el emisor y el receptor carecen de los medios de cifra requeridos o carecen de todo medio de cifra, y

b) el material clasificado no puede transmitirse a tiempo por otros medios.

41. En las circunstancias expuestas en el punto 39, la información clasificada transmitida no llevará ninguna marca ni indicación que la distinga de la información no clasificada o que pueda protegerse mediante un producto criptológico disponible. Se notificará sin demora a los receptores el grado de clasificación, recurriendo a otros medios.

42. Si hubiera que recurrir a lo expuesto en el punto 39, se presentará posteriormente un informe a la autoridad competente y al Comité de Seguridad.

III. GARANTÍA DE LA INFORMACIÓN: FUNCIONES Y AUTORIDADES

43. En los Estados miembros y en la SGC se establecerán las siguientes funciones respecto de la GI. Estas funciones no necesitan ser desempeñadas por organismos específicos y únicos. Tendrán cometidos separados. Sin embargo, dichas funciones y sus responsabilidades conexas podrán combinarse o integrarse en el mismo servicio administrativo, o dividirse entre varios de ellos, siempre que se eviten los conflictos internos de intereses o de funciones.

Autoridad de Garantía de la Información

44. Corresponderá a la Autoridad de Garantía de la Información (AGI):

a) establecer políticas y directrices de seguridad relativas a la GI y supervisar su eficacia y pertinencia;

b) salvaguardar y administrar la información técnica relacionada con los productos criptológicos;

c) garantizar que las medidas de GI seleccionadas para proteger la ICUE cumplan las normas que rigen su idoneidad y selección;

d) garantizar que los productos criptológicos se seleccionen de conformidad con las normas que rigen su idoneidad y selección;

e) coordinar la formación y la concienciación respecto de la GI;

f) consultar al proveedor del sistema, a los agentes en el ámbito de la seguridad y a los representantes de los usuarios sobre las políticas y directrices de seguridad relativas a la garantía de la información, y

g) velar por que se disponga de los conocimientos necesarios en la subsección especializada del Comité de Seguridad para cuestiones de GI.

Autoridad TEMPEST

45. Corresponderá a la autoridad TEMPEST garantizar que los SIC cumplan las políticas y directrices TEMPEST. La autoridad TEMPEST aprobará contramedidas para instalaciones y productos destinados a proteger ICUE de un determinado grado de clasificación dentro de su entorno operativo.

Autoridad de Certificación Criptológica

46. Corresponderá a la Autoridad de Certificación Criptológica (ACC) garantizar que los productos criptológicos cumplan la política criptológica nacional o la del Consejo. Dará su aprobación a los productos criptológicos para tratar ICUE de un determinado grado de clasificación dentro de su entorno operativo. Por lo que se refiere a los Estados miembros, la ACC se encargará de evaluar los productos criptológicos.

Autoridad de Distribución Criptológica

47. Corresponderá a la ADC:

a) gestionar y contabilizar el material criptológico de la UE;

b) garantizar que se apliquen los procedimientos adecuados y se establezcan los cauces pertinentes para rendir cuentas de todo el material criptográfico de la UE, así como para que su manejo, almacenamiento y distribución se hagan en condiciones de seguridad, y

c) garantizar la transferencia del material criptológico de la UE entre las personas o servicios que lo empleen.

Autoridad de Acreditación de Seguridad

48. Corresponderá a la Autoridad de Acreditación de Seguridad (AAS) de cada sistema:

a) velar por que los SIC cumplan las políticas y directrices de seguridad pertinentes, expedir una declaración de aprobación a los SIC para manejar ICUE de un determinado grado de clasificación en su entorno operativo, en la que se declaren las condiciones de la acreditación y los criterios aplicables para exigir una nueva aprobación;

b) establecer un proceso de acreditación de seguridad, de conformidad con las políticas pertinentes, que enuncie claramente las condiciones de aprobación de los SIC bajo su autoridad;

c) definir una estrategia de acreditación de seguridad que indique el grado de detalle para el proceso de acreditación según el nivel de garantía requerido;

d) examinar y aprobar la documentación de seguridad, incluidas las declaraciones de gestión del riesgo y de riesgo residual, las declaraciones de requisitos específicos de seguridad del sistema, la documentación relativa a la verificación de la aplicación de la seguridad y los procedimientos operativos de seguridad y asegurarse de que se cumplan las normas y políticas de seguridad del Consejo;

e) comprobar la aplicación de las medidas de seguridad en relación con los SIC realizando o patrocinando evaluaciones de seguridad, inspecciones o exámenes;

f) aprobar los criterios de seguridad (por ejemplo, los grados de habilitación del personal) para puestos sensibles en relación con los SIC;

g) refrendar la selección de productos criptológicos y TEMPEST aprobados para dotar de seguridad a los SIC;

h) aprobar la interconexión de un SIC a otros SIC o, cuando proceda, participar en la aprobación conjunta de dicha interconexión, y

i) consultar al proveedor del sistema, a los actores en el ámbito de la seguridad y a los representantes de los usuarios respecto de la gestión del riesgo, en particular el riesgo residual, así como sobre las condiciones de la declaración de aprobación.

49. Corresponderá a la AAS de la SGC la acreditación de todos los SIC que funcionen en el marco del mandato de la SGC.

50. Corresponderá a la AAS competente de un Estado miembro acreditar los SIC y los componentes de estos que operen dentro de su jurisdicción.

51. Un Panel de Acreditación de Seguridad se encargará de la acreditación de los SIC que entren dentro de la competencia tanto de la AAS de la SGC como de las AAS de los Estados miembros. Estará integrado por un representante de la AAS de cada Estado miembro, y asistirá a él un representante de la AAS de la Comisión. Se invitará a asistir a otras entidades conectadas a un SIC, cuando dicho sistema se someta a debate.

El Panel de Acreditación de Seguridad estará presidido por un representante de la AAS de la SGC. Se pronunciará por consenso de los representantes de las AAS de las instituciones, de los Estados miembros y de otras entidades conectados al SIC de que se trate. Elaborará informes periódicos sobre sus actividades, destinados al Comité de Seguridad y le comunicará todas las declaraciones de acreditación.

Autoridad Operacional de Garantía de la Información

52. Corresponderá a la Autoridad Operacional de Garantía de la Información (AOGI) de cada sistema:

a) elaborar documentación de seguridad en consonancia con las políticas y directrices de seguridad, en particular con los requisitos específicos de seguridad del sistema, incluida la declaración sobre el riesgo residual, los procedimientos operativos de seguridad y el plan criptológico en el proceso de acreditación de SIC;

b) participar en la selección y ensayo de las medidas técnicas de seguridad específicas para el sistema, de los dispositivos y los programas informáticos; supervisar su aplicación y garantizar que su instalación, configuración y mantenimiento sean seguros, de conformidad con la correspondiente documentación de seguridad;

c) participar en la selección de medidas de seguridad y dispositivos TEMPEST si lo requiere la enunciación de requisitos específicos de seguridad del sistema y garantizar que su instalación y mantenimiento sean seguros, en colaboración con la autoridad TEMPEST;

d) supervisar el cumplimiento y aplicación de los procedimientos operativos de seguridad y, cuando proceda, delegar las competencias sobre la seguridad operativa en el propietario del sistema;

e) gestionar y manejar productos criptológicos, garantizando la custodia de los artículos criptológicos y controlados y, si es preciso, garantizar la generación de variables criptológicas;

f) realizar análisis, exámenes y ensayos en materia de seguridad, en particular para elaborar los correspondientes informes sobre el riesgo, cuando lo requiera la Autoridad de Acreditación de Seguridad (AAS);

g) proporcionar formación sobre la GI específica para SIC, y

h) aplicar y ejecutar medidas de seguridad específicas para SIC.