Dictamen del Comité de las Regiones — Estrategia de ciberseguridad

(2013/C 280/05)

EL COMITÉ DE LAS REGIONES

— acoge favorablemente la Estrategia de ciberseguridad de la Comisión y la Directiva sobre seguridad de las redes y de la información (SRI), y apoya el objetivo de la Estrategia de garantizar un ciberespacio abierto y seguro y de convertir el entorno en línea de la UE en el más seguro del mundo;

— considera que es urgente un paquete que vincule los trabajos existentes y los trabajos propuestos en este ámbito y que ayude a proporcionar una visión coordinada y estratégica para Europa. El paquete se acoge favorablemente con el fin de asegurar la coordinación, fomentar la cooperación, emprender acciones claras y decisivas, lograr un nivel común de ciberprotección, mejorar la resiliencia de las redes y sistemas informáticos contra nuevas y futuras ciberamenazas y reducir la fragmentación de los sistemas en la UE;

— recomienda la publicación de un plan de acción de la Comisión que explique el funcionamiento en la práctica de los ambiciosos objetivos establecidos en el paquete. El plan de acción también deberá tener una guía para evaluar y medir el efecto de la Estrategia, a fin de determinar si la cooperación se lleva a cabo y si se logran progresos;

— destaca que el nuevo paquete debería ayudar a mejorar la prevención, detección y respuesta a incidentes informáticos y conducir a una mejora del intercambio de información y de la coordinación entre los Estados miembros y la Comisión contra los incidentes importantes. Para conseguirlo, se necesita un verdadero trabajo en cooperación en el que participen los Estados miembros, las instituciones de la UE, los entes locales y regionales, el sector privado y la sociedad civil.

Ponente:	Robert BRIGHT (UK/PSE), Miembro del Ayuntamiento de Newport
Documentos de referencia	Comunicación conjunta Estrategia de ciberseguridad de la Unión Europea (JOIN(2013) 1 final)
	Propuesta de Directiva relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión (COM(2013) 48 final)

I. **RECOMENDACIONES POLÍTICAS**

EL COMITÉ DE LAS REGIONES

1. acoge favorablemente la Estrategia de ciberseguridad de la Comisión y la Directiva sobre seguridad de las redes y de la información (SRI), y apoya el objetivo de la estrategia de garantizar un ciberespacio abierto y seguro y de convertir el entorno en línea de la UE en el más seguro del mundo;

2. espera que el nuevo paquete de ciberseguridad (incluidas la Estrategia y la Directiva) «eleve el listón» y realice una importante contribución a la elaboración de normas de ciberseguridad en toda la UE, disminuya la inseguridad jurídica, aumente la confianza en los servicios en línea, reduzca costes innecesarios y cargas administrativas y apoye así el mercado único digital y los objetivos de la Estrategia Europa 2020;

3. considera que es urgente un paquete que vincule los trabajos existentes y los trabajos propuestos en este ámbito y que ayude a proporcionar una visión coordinada y estratégica para Europa. El paquete se acoge favorablemente con el fin de asegurar la coordinación, fomentar la cooperación, emprender acciones claras y decisivas, lograr un nivel común de ciberprotección, mejorar la resiliencia de las redes y sistemas informáticos contra nuevas ciberamenazas y reducir la fragmentación de los sistemas en la UE;

4. recomienda que las organizaciones, incluidas las autoridades públicas, reconozcan que la lucha contra la ciberdelincuencia es una batalla en curso, y se les insta a dar prioridad a la amenaza planteada por las interrupciones de servicio y los ataques cibernéticos mediante la identificación de puntos vulnerables y a desarrollar la capacidad organizativa necesaria para gestionar las violaciones de la seguridad. A medida que internet se convierte en una parte cada vez más integral de la vida de los ciudadanos, la amenaza de la ciberdelincuencia aumenta y se expande en paralelo. La ciberdelincuencia, en todas sus formas, es una nueva amenaza sofisticada en rápido desarrollo para los Estados Miembros, las organizaciones y los ciudadanos de la UE en el siglo XXI, que aumenta continuamente en frecuencia y complejidad y no conoce fronteras;

5. reconoce los avances clave que la UE ha realizado hasta la fecha en la mejora de la protección de los ciudadanos frente a los delitos en línea, incluidas las propuestas legislativas relativas a los ataques contra los sistemas de información y la creación de una alianza mundial contra el abuso sexual de menores en línea. El paquete debe impulsar las acciones anteriores, incluidas las determinadas en la Agenda Digital para Europa 2010 ([1]), y construir una robusta política europea de ciberdefensa. En este sentido insta a los colegisladores que actualmente debaten la propuesta de Directiva de la Comisión relativa a los ataques contra los sistemas de información ([2]) a que alcancen un rápido acuerdo sobre esta propuesta;

6. apoya los ambiciosos objetivos de la Estrategia, ya que no busca solo la armonización de las capacidades de ciberseguridad de los Estados miembros y la vinculación de las distintas líneas de trabajo existentes y propuestas para establecer normas comunes y condiciones equitativas, sino también coordinar y garantizar la coherencia en tres áreas políticas: aplicación de la ley, Agenda Digital y política de defensa, seguridad y asuntos exteriores, cuyas competencias no son ejercidas por un único organismo;

7. indica que el paquete podría beneficiarse de las pruebas obtenidas por los gobiernos nacionales y debería proponer un conjunto de normas armonizadas relativas a la seguridad de las redes y la información;

8. acoge con satisfacción el enfoque de múltiples niveles que el paquete adopta al formular políticas. En el paquete se reconoce la importancia de la asociación público-privada y del logro de una verdadera cooperación que cuente con los recursos adecuados. El paquete también aspira a la realización del mercado único digital de la UE y a la creación de un entorno en línea seguro y próspero para las empresas, los gobiernos y los ciudadanos;

([1]) COM(2010) 254.
([2]) COM(2010) 517.

9. acoge con satisfacción las medidas propuestas en la Directiva, incluidas la recomendaciones de que los Estados miembros adopten una estrategia nacional de SRI, pongan en marcha equipos de respuesta a emergencias informáticas (CERT) que colaboren con la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), y creen un claro mecanismo de cooperación entre los Estados miembros y la Comisión que les permita compartir alertas tempranas sobre riesgos e incidentes mediante una infraestructura segura. Estas medidas y el enfoque normativo de la Directiva deberían contribuir en gran parte a mejorar la coherencia, establecer un nivel mínimo común de preparación a escala nacional y reforzar las ciberdefensas en la UE;

10. alienta al Parlamento Europeo y al Consejo a que adopten rápidamente la propuesta de Directiva relativa a un elevado nivel común de SRI en la Unión Europea;

11. indica que el paquete podría beneficiarse de una mayor especificación sobre el modo en que los Estados miembros informan y recopilan datos sobre la ciberdelincuencia, así como de características adicionales sobre la manera de aplicar las medidas. Será crucial establecer sistemas comunes de información y métodos claros sobre los requisitos de notificación para evitar la incertidumbre y la falta de coherencia en la forma en que una autoridad nacional con competencias en SRI define y mide los ciberincidentes que tengan una «repercusión significativa». También es imprescindible que la creación de una autoridad nacional con competencias en SRI tenga en cuenta el reparto de competencias dentro de los Estados Miembros, en particular los que tienen estructuras muy federadas o descentralizadas;

12. expresa por tanto cierta preocupación sobre algunos aspectos reglamentarios y legales del paquete, especialmente por lo que se refiere a la falta de claridad en la definición de los criterios que debe cumplir un Estado miembro para que se le autorice a participar en el sistema común de intercambio seguro de información, a una mayor especificación de los incidentes que justifican una alerta temprana y a la definición de las circunstancias que exigen la notificación de incidentes por parte de los operadores del mercado y las administraciones públicas. La ausencia de normas claramente establecidas sobre estas cuestiones obstaculiza la seguridad jurídica;

13. expresa cierta preocupación por que la Directiva pudiera colocar cargas normativas innecesarias sobre las empresas y los organismos públicos. No deben escatimarse esfuerzos para evitar duplicar la reglamentación y garantizar que cualquier norma adicional respete el principio de proporcionalidad. Esto será de especial importancia para aquellas organizaciones que ya tienen la obligación de notificar informaciones sustancialmente similares a lo previsto aquí;

14. recomienda la publicación de un plan de acción de la Comisión que explique el funcionamiento en la práctica de los ambiciosos objetivos establecidos en el paquete. El plan de acción también deberá tener una guía para evaluar y medir el efecto de la Estrategia, a fin de determinar si la cooperación se lleva a cabo y si se logran progresos;

15. insta a todos los Estados miembros a que elaboren estrategias nacionales de ciberseguridad (hasta 2012, solo diez Estados miembros han desarrollado una estrategia) que complementen la nueva estrategia de la UE. Para garantizar la coherencia es importante que haya complementariedad entre las estrategias nacionales y la Estrategia de la UE. También es importante que las acciones de la UE complementen las estructuras existentes y las buenas prácticas de los Estados miembros;

16. acoge con satisfacción las próximas acciones de la Comisión para el desarrollo de las capacidades de la UE en ciberseguridad, que incluyen la puesta en marcha de un proyecto piloto para luchar contra las redes infectadas y los programas maliciosos, el compromiso de mejorar la cooperación entre los CERT nacionales, ENISA y el nuevo Centro Europeo de Ciberdelincuencia, la elaboración de una red de centros nacionales de excelencia de lucha contra la ciberdelincuencia, y el lanzamiento de una plataforma público-privada dedicada a la SRI que ofrezca incentivos para la adopción de soluciones de TIC seguras. También se acoge con satisfacción el objetivo de la Estrategia de reunir a todas las partes interesadas para evaluar el progreso tras un periodo de doce meses;

17. subraya que una estrategia de ciberseguridad eficaz debe apoyarse en una cooperación estrecha entre las autoridades competentes de SRI y los cuerpos de seguridad. Para ello tiene una importancia crucial notificar sistemáticamente los incidentes de carácter supuestamente delictivo a los cuerpos de seguridad;

Participación local y regional

18. considera que las prioridades definidas en el paquete ofrecen un buen equilibrio y son adecuadas. Las prioridades, entre las que se cuentan la protección de los derechos fundamentales, de los datos personales y de la intimidad, una eficaz gobernanza multilateral y una responsabilidad compartida que garantice la seguridad, son campos en los que las ciudades y regiones deberían desempeñar un papel clave en su calidad de titulares de la información del sector público;

19. indica que las regiones deberían ser reconocidas, junto con los Estados miembros, como los promotores principales de la estrecha cooperación entre usuarios y productores de innovaciones de las TIC en diferentes ámbitos gubernamentales y administrativos, incluidas la ciberseguridad y la protección de datos;

20. destaca que el nuevo paquete debería ayudar a mejorar la prevención, detección y respuesta a incidentes informáticos y conducir a una mejora del intercambio de información y de la coordinación entre los Estados miembros y la Comisión contra los incidentes importantes. Para conseguirlo, se necesita un verdadero trabajo en cooperación en el que participen los Estados miembros, las instituciones de la UE, los entes locales y regionales, el sector privado y la sociedad civil;

21. reconoce que la lucha contra las ciberamenazas requerirá mayores recursos, un aumento de la concienciación sobre las amenazas que plantea la delincuencia informática y una ciberseguridad eficiente y adecuada. En cuanto a la gobernanza multinivel, un enfoque sólido sobre la ciberseguridad tiene que tener en cuenta a los entes locales y regionales, que deben ser involucrados de forma plena y efectiva en la gobernanza de las iniciativas relacionadas con las TIC;

22. considera que, dado que las violaciones de seguridad son una amenaza para los servicios básicos, por ejemplo, el suministro local de agua o energía, y dado que utilizan y poseen abundante información y servicios digitales, los entes locales y regionales tienen un papel clave que desempeñar en la lucha contra la ciberdelincuencia y en la recopilación y protección de los datos informáticos. En los entes locales y regionales recae cada vez en mayor medida la responsabilidad de ofrecer, por ejemplo, servicios digitales a los ciudadanos y las comunidades y formación en SRI en las escuelas. Los gobiernos, incluidos los de nivel local y regional, son responsables de salvaguardar el acceso y apertura de las redes, respetar y proteger los derechos fundamentales en línea y mantener la fiabilidad e interoperabilidad de internet;

23. propone que, a fin de lograr una mejor legislación, dadas las competencias de los entes locales y regionales y el papel fundamental que están llamados a desempeñar en la planificación y puesta en práctica de medidas en el ámbito de las TIC (especialmente en los aspectos relacionados con la privacidad, la protección de datos y la ciberseguridad), estos entes deberían ser consultados sistemáticamente por las instituciones de la UE y los Estados miembros, tanto en la concepción como en la aplicación de medidas destinadas a llevar a la práctica la Agenda Digital para Europa. De hecho, es lamentable que no se haya realizado ningún esfuerzo especial para recoger las opiniones de los entes locales y regionales en la preparación de la propuesta de Directiva. El CDR ha dejado claro que está dispuesto a ayudar a la Comisión en las consultas prelegislativas, como se establece en el Protocolo de cooperación CDR-Comisión ([3]);

24. recomienda incluir medidas aplicables al nivel local y regional en el artículo 14, punto 1, de la Directiva. Estas medidas podrían incluir el establecimiento de un proceso de evaluación y gestión de riesgos, la aplicación de la política de seguridad de la información, el aumento de la percepción de las cuestiones de ciberseguridad y la mejora de la alfabetización y la capacitación digitales;

25. destaca que, en el nivel subnacional, deberían fomentarse y desarrollarse acuerdos de asociación entre todos los actores relevantes que permitieran trabajar en acciones coordinadas sobre ciberseguridad. Estas acciones podrían, a su vez, tenerse en cuenta cuando se pongan en marcha medidas de ciberseguridad en el nivel nacional y europeo con el fin de luchar contra la delincuencia y minimizar los efectos causados por el robo directo de propiedad financiera o intelectual, la perturbación de las comunicaciones o el daño causado a datos empresariales cruciales;

([3]) Protocolo de cooperación entre la Comisión Europea y el Comité de las Regiones firmado el 16 de febrero de 2012, R/CDR 39/2012 pt 7.

Subsidiariedad y proporcionalidad

26. considera que, en términos generales, parecen cumplirse las dos condiciones del principio de subsidiariedad: necesidad de acción de la UE y valor añadido de esa acción a escala de la UE. Las acciones propuestas son necesarias porque involucran aspectos transnacionales que no pueden ser regulados de forma adecuada por los Estados miembros o los entes locales y regionales por separado. También es probable que las acciones propuestas proporcionen un claro beneficio en comparación con las acciones aisladas en el nivel nacional, regional o local, ya que, por ejemplo, los datos personales se transfieren cada vez en mayor medida a través de las fronteras, tanto internas como externas. Además, está claro que las obligaciones reglamentarias a escala de la UE ayudarán a lograr condiciones uniformes y colmar las lagunas jurídicas;

27. acoge con satisfacción el respeto fundamental de la Directiva de los principios de subsidiariedad y proporcionalidad. Teniendo en cuenta los aspectos transfronterizos de los incidentes y riesgos de la SRI, los objetivos establecidos en la Directiva pueden lograrse mejor a escala de la UE, de conformidad con el principio de subsidiariedad. Las investigaciones muestran que los ciudadanos de la UE confían en instituciones como la Comisión en lo referente a la protección de datos personales ([4]). La Directiva también respeta esencialmente el principio de proporcionalidad, ya que la propuesta no excede de lo necesario para alcanzar esos objetivos. Sin embargo, el hecho de que la propuesta prevea una sola autoridad competente o CERT nacional por país plantea problemas en relación con el respeto del principio de proporcionalidad y de las estructuras de gobernanza interna de los Estados miembros de la UE;

28. considera que, si bien la base jurídica del paquete se sustenta en los artículos 26 y 114 del TFUE, las acciones propuestas exceden los presupuestos de esos artículos, ya que la propuesta abarca todos los sistemas de información de la administración pública, incluidos los sistemas de información internos como una intranet;

Carta de los Derechos Fundamentales

29. acoge con satisfacción el respeto de la Directiva de la Carta de los Derechos Fundamentales de la Unión Europea. Las mismas normas, principios y valores que la Unión Europea defiende en el mundo real también deberían aplicarse al mundo virtual. Las tecnologías de la información y la comunicación (TIC) deberían incluir las necesidades de todos los miembros de la sociedad, incluidos los que sufren riesgo de exclusión social. Todos los usuarios de internet deberían contar con normas mínimas en toda una gama de necesidades, entre las que se cuentan la fiabilidad, la seguridad, la transparencia, la sencillez, la interoperabilidad y la reducción de riesgos y responsabilidad. En interés de la protección efectiva de los derechos fundamentales y la seguridad jurídica, y a fin de tener en cuenta la reserva de estudio parlamentario, se insta a que en la propia Directiva se incluya una reglamentación más concreta, en términos del Derecho sustantivo, sobre las normas de seguridad de las

([4]) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_es.pdf.

redes y de la información. En particular, se deberían establecer requisitos relativos a los derechos fundamentales y a la legislación sobre protección y seguridad de los datos aplicables a la configuración de la seguridad de las redes y la información;

30. pone de relieve que los intentos de proteger y defender en línea a los ciudadanos deben mantener un adecuado equilibrio con los derechos, libertades y principios que les son reconocidos a los ciudadanos en la Carta. Es bienvenida la importancia que se concede a la elaboración de ciberpolíticas dentro de los valores esenciales de la UE. Como se ha señalado en dictámenes anteriores ([5]), será crucial garantizar que se cumplen todos los requisitos de seguridad en todos los niveles, para así garantizar niveles óptimos de privacidad y protección de datos de carácter personal y evitar cualquier tipo de seguimiento no autorizado de la información y los perfiles personales;

31. pone de relieve que, a pesar de la creciente responsabilidad de los operadores privados por las infraestructuras críticas y los servicios en línea y la necesidad de reconocer el papel crucial del sector privado, al Estado debe incumbir, en última instancia, la responsabilidad de preservar la libertad y proteger la seguridad en línea de sus ciudadanos;

Simplificación

32. toma nota de que la introducción en toda Europa del principio de que los datos personales y los datos de objetos puedan registrarse una sola vez, sin necesidad de rellenar formularios repetidamente, contribuirá en gran medida a la supresión de trámites burocráticos innecesarios y a la reducción de los costes de la administración pública. Por tanto, deberá procurarse cumplir debidamente la legislación sobre protección de datos;

Formación

33. destaca que una ciberdefensas eficaces requieren la formación y la mejora de las competencias del personal, incluido el de los entes locales y regionales. Debería proporcionarse amplia formación a todo el personal, en particular los especialistas técnicos, el personal que trabaja directamente con los procedimientos de seguridad relacionados con las diferentes metodologías y el personal que trabaja de forma general o indirecta en tareas de innovación y modernización en ámbitos relacionados con la confianza y la seguridad. La formación continua es importante para el éxito de la administración electrónica local, mientras que los entes locales y regionales también desempeñan un papel de creciente importancia a la hora de suministrar información y orientación a los ciudadanos para que usen correctamente los sistemas y reconozcan ciberamenazas ([6]);

34. el «compromiso de la dirección» constituye un factor de éxito muy importante. Por este motivo, se necesita también una formación específica destinada a los grupos de dirección y responsables de personal para que dispongan de los conocimientos y la preparación necesarios para sentar las bases de una cultura de la seguridad en sus organizaciones respectivas;

35. toma nota de la mejora en la educación y la formación que se consigue introduciendo la formación en SRI y estableciendo un campeonato de seguridad cibernética en 2014. Esto debería tener en cuenta los actos que se celebran regularmente en los Estados miembros y propiciar el intercambio de buenas prácticas. Acoge con satisfacción la ambición de introducir, a través de la estrategia, la formación en SRI en las escuelas; sin embargo, dado que la educación es competencia de los Estados miembros, indica que se necesitarán una planificación y unos recursos significativos para alcanzar este objetivo en 2014;

Apoyar a las empresas, la innovación y las soluciones técnicas

36. llama la atención sobre el hecho de que la garantía del respeto de la privacidad depende de determinados factores como la estructuración de las entidades del sector público (la mayoría de ellas en el ámbito local), la convergencia de la legislación de la UE, el fomento de una cultura innovadora entre los funcionarios públicos, incluido el uso de un código ético común, y entre los ciudadanos, definiendo sus derechos como consumidores digitales y contribuyendo a que tomen conciencia de ello, y la gestión de las aplicaciones basadas en las TIC;

37. sostiene que otras acciones deberían impulsar y apoyar el desarrollo y la aplicación de soluciones técnicas para combatir eficazmente los contenidos ilícitos y las conductas nocivas en línea, y que las partes interesadas se animarán a cooperar e intercambiar ejemplos de buenas prácticas a escala local, regional, europea e internacional. En este sentido, son de vital importancia las líneas de ayuda a la infancia, padres y cuidadores, las líneas directas para denunciar el abuso y la existencia de programas informáticos que permitan una mejor identificación del contenido abusivo y una forma rápida y sencilla de interponer denuncias;

38. recomienda que no se escatimen esfuerzos para aumentar el pequeño porcentaje de empresas en la UE (26 % en enero de 2012) que tienen una política de seguridad de las TIC formalmente definida ([7]). Es necesario alentar a empresas de todos los tamaños a invertir en ciberseguridad, lo que puede ser utilizado como un instrumento de mercadotecnia para clientes potenciales y, a la vez, mitigar los efectos catastróficos de la ciberdelincuencia. Las empresas deberían considerar un enfoque de negocio orientado a la ciberseguridad con el apoyo de la tecnología, dando prioridad a los activos o procesos empresariales más importantes;

([5]) CDR 104/2010 fin.

([6]) http://www.enisa.europa.eu/publications/archive/scandinavian-approaches-survey.

([7]) http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/ICT_security_in_enterprises.

El potencial económico de las TIC

39. subraya que, teniendo en cuenta el enorme potencial económico de las TIC para la economía europea (en la actualidad casi el 6 % del PIB de la UE ([8])), en la actualidad se necesitan medidas concretas para hacer frente al creciente fenómeno de la ciberdelincuencia y restaurar la confianza en la seguridad de internet tanto de los ciudadanos como de las empresas (reduciendo a la vez el número de usuarios de internet de la UE que están preocupados por la seguridad, por ejemplo, de los pagos en línea ([9]));

40. sostiene que, a fin de reducir las enormes cantidades de fondos perdidos por causa de la delincuencia informática y de aumentar la confianza de los consumidores, se necesitan esfuerzos urgentes en el nivel local, regional, nacional y europeo contra la ciberdelincuencia;

41. indica que la Estrategia se beneficiaría de una mayor especificación sobre la forma de proteger y desarrollar la computación en nube, que tiene un enorme potencial económico. El rápido crecimiento del uso de dispositivos electrónicos móviles no muestra signos de desaceleración. Gartner informa de que, para el año 2016, al menos el 50 % de los usuarios de correo electrónico empresarial utilizará un terminal móvil ([10]). Es necesario analizar los nuevos problemas y oportunidades que crean los dispositivos electrónicos móviles y la computación en nube. Por otra parte, la computación en nube tiene una arquitectura apropiada para alcanzar niveles óptimos de seguridad ([11]). En efecto, el Comité ha manifestado su preocupación por el hecho de que la reciente Comunicación de la Comisión Europea sobre la computación en nube no trate de manera adecuada el vínculo entre la estrategia propuesta y otras cuestiones como la seguridad del tratamiento de los datos, los derechos de autor o el desarrollo de la accesibilidad y la portabilidad de los datos ([12]);

Cooperación internacional

42. considera que, dada la amenaza global, interconectada y transfronteriza que plantea el delito cibernético, también se debe fomentar la cooperación internacional y el diálogo más allá de las fronteras de la UE con el fin de garantizar un enfoque verdaderamente global y coordinado de la ciberseguridad. En este sentido, hay que alentar a todos los Estados a respetar el Convenio internacional sobre la ciberdelincuencia (Convenio de Budapest) ([13]). También es importante continuar la colaboración bilateral, en particular con EE.UU., y multilateral con una serie de organizaciones internacionales,

Vínculos con los programas de financiación de la UE y el marco presupuestario

43. pone de relieve la importancia de mejorar la coordinación con los instrumentos de financiación existentes y futuros, como Horizonte 2020, el marco europeo de cooperación y el Fondo de Seguridad Interior, con el fin de garantizar un enfoque más coordinado de las inversiones en el ámbito informático;

44. se pregunta si el presupuesto asignado de 1,25 millones de euros será suficiente para proporcionar una infraestructura de SRI robusta y adecuada, y expresa su decepción por la reducción de la asignación financiera para el Mecanismo «Conectar Europa» que se recoge en el acuerdo sobre el marco financiero plurianual 2014-2020 aprobado por el Consejo el 8 de febrero. Es necesario un presupuesto sólido y ampliado para proporcionar apoyo financiero a infraestructuras clave de las TIC, enlazando las capacidades de los Estados miembros en materia de RSI y, por tanto, facilitando la cooperación en la UE.

II. RECOMENDACIONES DE ENMIENDA

Enmienda 1

Considerando (4)

Texto propuesto por la Comisión	Enmienda del CDR
Es conveniente crear a escala de la Unión un mecanismo de cooperación que propicie el intercambio de información y una detección y respuesta coordinadas en relación con la seguridad de las redes y de la información (en lo sucesivo, «SRI»). Para que dicho mecanismo sea eficaz e integrador, es esencial que todos los Estados miembros posean unas capacidades mínimas y una estrategia que aseguren un elevado nivel de SRI en su territorio. Asimismo, procede imponer a las administraciones públicas y a los operadores de infraestructuras críticas de información requisitos mínimos en materia de seguridad para fomentar una cultura de gestión de riesgos y garantizar la notificación de los incidentes más graves.	Es conveniente crear a escala de la Unión un mecanismo de cooperación que propicie el intercambio de información y una detección y respuesta coordinadas en relación con la seguridad de las redes y de la información (en lo sucesivo, «SRI»). Para que dicho mecanismo sea eficaz e integrador, es esencial que todos los Estados miembros posean unas capacidades mínimas y una estrategia que aseguren un elevado nivel de SRI en su territorio. Asimismo, procede imponer a las administraciones públicas, **incluidos los entes locales y regionales**, y a los operadores de infraestructuras críticas de información requisitos mínimos en materia de seguridad para fomentar una cultura de gestión de riesgos y garantizar la notificación de los incidentes más graves.

([8]) http://europa.eu/rapid/press-release_MEMO-13-71_en.htm.
([9]) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.
([10]) http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf.
([11]) http://www.mcafee.com/hk/resources/reports/rp-sda-cyber-security.pdf.
([12]) CDR 1673 (2012).
([13]) http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.

Enmienda 2

Considerando (9)

Texto propuesto por la Comisión	Enmienda del CDR
A fin de alcanzar y mantener un elevado nivel común de seguridad de las redes y los sistemas de información, los Estados miembros deben disponer de sendas estrategias nacionales de SRI que fijen los objetivos estratégicos y las medidas concretas que haya que aplicar. Deben elaborarse a escala nacional planes de cooperación en el ámbito de la SRI que cumplan los requisitos esenciales para así lograr niveles de capacidad de respuesta que hagan posible una cooperación efectiva y eficaz a escala nacional y de la Unión ante los incidentes que se produzcan.	A fin de alcanzar y mantener un elevado nivel común de seguridad de las redes y los sistemas de información, los Estados miembros deben disponer de sendas estrategias nacionales de SRI que fijen los objetivos estratégicos y las medidas concretas que haya que aplicar. Deben elaborarse a escala nacional, **con la plena participación de los entes locales y regionales**, planes de cooperación en el ámbito de la SRI que cumplan los requisitos esenciales para así lograr niveles de capacidad de respuesta que hagan posible una cooperación efectiva y eficaz a escala nacional y de la Unión ante los incidentes que se produzcan.

Enmienda 3

Considerando (35)

Texto propuesto por la Comisión	Enmienda del CDR
Reviste primordial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos. Al preparar y elaborar actos delegados, la Comisión debe garantizar que los documentos pertinentes se transmitan al Parlamento Europeo y al Consejo de manera simultánea, oportuna y adecuada.	Reviste primordial importancia que la Comisión lleve a cabo las consultas oportunas durante la fase preparatoria, en particular con expertos. Al preparar y elaborar actos delegados, la Comisión, **a fin de complementar o modificar determinados elementos no esenciales de la ley básica**, debe garantizar que los documentos pertinentes se transmitan al Parlamento Europeo y al Consejo de manera simultánea, oportuna y adecuada.

Enmienda 4

Capítulo 4

Artículo 14(1)

Texto propuesto por la Comisión	Enmienda del CDR
Requisitos en materia de seguridad y notificación de incidentes 1. Los Estados miembros velarán por que las administraciones públicas y los operadores del mercado tomen las medidas técnicas y de organización apropiadas para gestionar los riesgos existentes para la seguridad de las redes y los sistemas de información que controlan y utilizan en sus operaciones. Habida cuenta del estado de la técnica, dichas medidas garantizarán un nivel de seguridad adecuado en relación con el riesgo existente. En particular, adoptarán medidas para prevenir y reducir al mínimo los efectos de los incidentes que afecten a sus redes y sistemas de información en los servicios básicos que prestan, garantizando de este modo la continuidad de los servicios que dependen de tales redes y sistemas de información.	Requisitos en materia de seguridad y notificación de incidentes 1. Los Estados miembros velarán por que las administraciones públicas y los operadores del mercado tomen las medidas técnicas y de organización apropiadas para gestionar los riesgos existentes para la seguridad de las redes y los sistemas de información que controlan y utilizan en sus operaciones. **A nivel local y regional estas medidas podrían consistir en establecer un proceso de evaluación y gestión de riesgos, velar por la aplicación de la política de seguridad de la información, aumentar la percepción de las cuestiones relativas a la ciberseguridad y fomentar la alfabetización y las competencias digitales.** Habida cuenta del estado de la técnica, dichas medidas garantizarán un nivel de seguridad adecuado en relación con el riesgo existente. En particular, adoptarán medidas para prevenir y reducir al mínimo los efectos de los incidentes que afecten a sus redes y sistemas de información en los servicios básicos que prestan, garantizando de este modo la continuidad de los servicios que dependen de tales redes y sistemas de información.

Exposición de motivos

Como en la lucha contra la ciberdelincuencia, el papel de los entes locales y regionales es crucial y debe ser plenamente reconocido.

Enmienda 5

Capítulo 4

Artículo 16

Texto propuesto por la Comisión	Enmienda del CDR
Artículo 16	*Artículo 16*
Normalización	Normalización
1. A fin de garantizar una aplicación convergente de lo dispuesto en el artículo 14, apartado 1, los Estados miembros fomentarán la utilización de las normas y especificaciones pertinentes en materia de seguridad de las redes y la información.	1. A fin de garantizar una aplicación convergente de lo dispuesto en el artículo 14, apartado 1, los Estados miembros fomentarán la utilización de las normas y especificaciones **armonizadas** pertinentes en materia de seguridad de las redes y la información.
2. La Comisión elaborará mediante actos de ejecución una lista de las normas mencionadas en el apartado 1. Dicha lista se publicará en el *Diario Oficial de la Unión Europea*.	2. La Comisión elaborará mediante actos de ejecución una lista de las normas mencionadas en el apartado 1. Dicha lista se publicará en el *Diario Oficial de la Unión Europea*.

Exposición de motivos

La Comisión Europea reconoce que la aplicación de normas divergentes por los distintos Estados miembros constituye un importante problema. Por lo tanto, la armonización de las normas es esencial para garantizar un nivel común de seguridad de las redes y la información en toda la UE.

Bruselas, 3 de julio de 2013.

El Presidente
del Comité de las Regiones
Ramón Luis VALCÁRCEL SISO