Organisation for Economic
Co-operation and Development

DIRECTRICES DE LA OCDE
PARA LA SEGURIDAD
DE SISTEMAS Y REDES DE INFORMACIÓN :
HACIA UNA CULTURA DE SEGURIDAD

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICO

En virtud del artículo 1 del Convenio firmado el 14 de diciembre de 1960 en París, entrado en vigor el 30 de septiembre de 1961, la Organización para la Cooperación y el Desarrollo Económico (OCDE) tiene por objetivo promover políticas dirigidas:

– A conseguir la mayor expansión de la economía y el empleo y una progresión del nivel de vida en los países miembros, manteniendo la estabilidad financiera, y a contribuir así al desarrollo de la economía mundial.

– A contribuir a una sana expansión económica en los países miembros, así como en los países no miembros, en vías de desarrollo económico.

– A contribuir a la expansión del comercio mundial sobre una base multilateral y no discriminatoria, conforme con las obligaciones internacionales.

Los países miembros originales de la OCDE son Alemania, Austria, Bélgica, Canadá, Dinamarca, España, Estados Unidos, Francia, Grecia, Irlanda, Islandia, Italia, Luxemburgo, Noruega, Países Bajos, Portugal, Reino Unido, Suecia, Suiza y Turquía. Los países siguientes se han convertido posteriormente en miembros mediante adhesión en las fechas indicadas: Japón (28 de abril de 1964), Finlandia (28 de enero de 1969), Australia (7 de junio de 1971), Nueva Zelanda (29 de mayo de 1973), México (18 de mayo de 1994), República Checa (12 de diciembre de 1995), Hungría (7 de mayo de 1996), Polonia (22 de noviembre de 1996), Corea (12 de diciembre de 1996) y Eslovaquia (14 de diciembre de 2000). La Comisión de las Comunidades Europeas participa en los trabajos de la OCDE (artículo 13 del Convenio de la OCDE).

Traducción en lengua española realizada de los textos en inglés y/o francés, versiones oficiales de esta publicación, titulados:

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: Vers une culture de la sécurité

Publicada con la autorización de la OCDE.

NIPO: 326-04-035-2

PRÓLOGO

Las presentes *Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información: hacia una cultura de Seguridad* se adoptaron como Recomendación del Consejo de la OCDE en su sesión 1037 de 25 de julio de 2002).

ÍNDICE

DIRECTRICES PARA LA SEGURIDAD DE SISTEMAS Y REDES DE INFORMACIÓN

HACIA UNA CULTURA DE SEGURIDAD

PREFACIO

Desde que en 1992 la OCDE desarrollara por primera vez las *Directrices de Seguridad de los Sistemas de Información*, el uso de los sistemas y redes de información, así como el entorno tecnológico de información, en su totalidad, han sufrido grandes cambios. Estos cambios continuos ofrecen grandes ventajas, pero hacen necesario que los gobiernos, las empresas, y otras organizaciones y usuarios que desarrollan, poseen, proporcionan, administran estos servicios, y usan sistemas y redes de información ("participantes") pongan mayor atención en los aspectos relacionados con la seguridad.

El ambiente que predominaba en el pasado, en el que los sistemas operaban de manera aislada o en redes privadas, ha sido sustituido por computadoras personales que cada vez tienen mayor capacidad de proceso, así como por tecnologías convergentes y por la propia difusión masiva del uso del Internet. Hoy en día los participantes se encuentran cada vez más interconectados, y esta interconexión se extiende más allá de las fronteras nacionales. Al mismo tiempo, Internet forma parte de la infraestructura operativa de sectores estratégicos como energía, transportes y finanzas, y desempeña un papel fundamental en la forma en que las compañías realizan sus transacciones comerciales, los gobiernos proporcionan sus servicios a los ciudadanos y a las empresas, y los ciudadanos se comunican e intercambian información de manera individual. La naturaleza y el tipo de tecnologías que constituyen la infraestructura de la información y comunicaciones también han cambiado de manera significativa. El número y el tipo de dispositivos que integran la infraestructura de acceso se ha multiplicado, incluyendo elementos de tecnología fija, inalámbrica y móvil, así como una proporción creciente de accesos que están conectados de manera permanente. Como consecuencia de todos estos cambios, la naturaleza, volumen y sensibilidad de la información que se intercambia a través de esta infraestructura se ha incrementado de manera muy significativa.

Como resultado de una creciente interconexión, los sistemas y las redes de información son más vulnerables, ya que están expuestos a un número creciente, así como a una mayor variedad, de amenazas y de vulnerabilidades. Esto hace que surjan nuevos retos que deben abordarse en materia de seguridad. Por estas razones, estas Directrices se aplican para todos los participantes de la nueva sociedad de la información y sugieren la necesidad de tener una mayor conciencia y entendimiento de los aspectos de seguridad, así como de la necesidad de desarrollar una "cultura de seguridad".

I. HACIA UNA CULTURA DE SEGURIDAD

Estas Directrices pretenden dar respuesta a un ambiente de seguridad cada vez más cambiante, a través de la promoción del desarrollo de una cultura de seguridad – esto es, centrándose en la seguridad del desarrollo de sistemas y redes de información, así como en la adopción de nuevas formas de pensamiento y comportamiento en el uso e interconexión de sistemas y redes de información. Estas Directrices marcan una clara ruptura con un tiempo en el que los aspectos de seguridad y el uso de redes y sistemas se consideraban con frecuencia como elementos a posteriori. Los sistemas, redes y servicios de información afines, deben ser fiables y seguros, dado que los participantes son cada vez más dependientes de éstos. Sólo un enfoque que tome en cuenta los intereses de todos los participantes y la naturaleza de los sistemas, redes y servicios afines puede proporcionar una seguridad efectiva.

Cada participante es un actor importante en la garantía de la seguridad. Cada participante de acuerdo con el papel que desempeña deberá ser consciente de los riesgos de seguridad y de las medidas preventivas que sean oportunas, debiendo asumir la responsabilidad que les corresponde y tomar las medidas necesarias para fortalecer la seguridad de los sistemas y redes de información.

La promoción de una cultura de seguridad requerirá tanto un liderazgo fuerte como una participación amplia para asegurar que se le otorgue un carácter de prioritario a la planificación y administración de la seguridad, así como la comprensión de la necesidad de una seguridad plena entre todos los participantes. Los aspectos de seguridad deberían ser objeto de interés y responsabilidad a todos los niveles de la administración pública y empresa, así como para todos los
participantes. Estas Directrices constituyen una base de trabajo fundamental hacia una cultura de seguridad para toda la sociedad. Ello permitirá que los participantes consideren la seguridad en el diseño y uso de los sistemas y de las redes de información. Asimismo, estas Directrices proponen que todos los participantes adopten y promuevan una cultura de seguridad como modo de pensar, así como de evaluar y actuar en los sistemas y redes de información.

II. PROPÓSITOS

Los propósitos de estas Directrices son:

- Promover una cultura de seguridad entre todos los participantes como medio de proteger los sistemas y redes de información.

- Incrementar la concienciación sobre el riesgo de los sistemas y redes de información; sobre las políticas, prácticas, medidas y procedimientos disponibles para poder afrontar estos riesgos; así como sobre la necesidad de adoptarlos y ejecutarlos.

- Promover entre todos los participantes una confianza mayor en los sistemas y redes de información, sí como en la forma de operar y de uso.

- Crear un marco general de referencia que ayude a los participantes en la comprensión de los aspectos de seguridad y respeto de valores éticos en el desarrollo y ejecución de políticas coherentes, así como de prácticas, medidas y procedimientos para la seguridad de sistemas y redes de información.

- Promover entre todos los participantes cuando sea posible, la cooperación y el intercambio de información sobre el desarrollo y ejecución de políticas de seguridad, así como de prácticas, medidas y procedimientos.

- Promover el conocimiento en materia de seguridad como un objetivo importante a lograr entre todos los participantes involucrados en el desarrollo y ejecución de normas técnicas.

III. PRINCIPIOS

Los siguientes nueve principios son complementarios entre sí, y deben ser interpretados como un todo. Éstos son de interés general para todos los participantes y a todos los niveles, tanto en el ámbito político como técnico. De acuerdo con estas Directrices, la responsabilidad de los mismos varía de acuerdo con los papeles que desempeñen. Todos se verán beneficiados por la concienciación, educación, intercambio de información y capacitación que lleven a la adopción de un mejor entendimiento de la seguridad y de las prácticas requeridas. Los esfuerzos para fortalecer la seguridad de los sistemas y redes de información deben ser consistentes con los

valores de una sociedad democrática, en particular con la necesidad de contar con flujos de información libres y abiertos, y los principios básicos de protección de la privacidad personal[1].

1) Concienciación

Los participantes deberán ser conscientes de la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.

El conocimiento de los riesgos y de los mecanismos disponibles de salvaguardia, es el primer paso en la defensa de la seguridad de los sistemas y redes de información. Estos sistemas y redes de información pueden verse afectados tanto por riesgos internos como externos. Los participantes deben comprender que los fallos en la seguridad pueden dañar significativamente los sistemas y redes que están bajo su control. Deben asimismo ser conscientes del daño potencial que esto puede provocar a otros derivados de la interconexión y la interdependencia. Los participantes deben tener conocimiento de las configuraciones y actualizaciones disponibles para sus sistemas, así como su lugar que ocupan dentro de las redes, las prácticas a ejecutar para ampliar la seguridad, y las necesidades del resto de los participantes.

2) Responsabilidad

Todos los participantes son responsables de la seguridad de los sistemas y redes de información.

Los participantes dependen de los sistemas y redes de información locales y globales, y deben comprender su responsabilidad en la salvaguarda de la seguridad de los sistemas y redes de información. Asimismo deben responder ante esta responsabilidad de una manera apropiada a su papel individual. Los participantes deben igualmente revisar sus propias políticas, prácticas, medidas y procedimientos de manera regular, y evaluar si éstos son apropiados en relación con su propio entorno. Aquellos que desarrollan y diseñan o suministran productos o servicios deberán elevar la seguridad de los sistemas y redes, y distribuir a los usuarios de manera apropiada información adecuada en materia de seguridad, incluyendo actualizaciones, para que éstos entiendan mejor la funcionalidad de la seguridad de sus productos y servicios, así como la responsabilidad que les corresponde en materia de seguridad.

3) Respuesta

Los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.

Al reconocer la interconexión de los sistemas y de las redes de información, así como el riesgo potencial de un daño que se extienda con rapidez y tenga una alcance amplio, los participantes deben actuar de manera adecuada y conjunta para enfrentarse a los incidentes que afecten la seguridad. Asimismo han de compartir información sobre los riesgos y vulnerabilidades y ejecutar procedimientos para una cooperación rápida y efectiva que permita prevenir, detectar y responder a incidentes que afecten a la seguridad. Cuando sea posible, estas actuaciones habrán de suponer un intercambio de información y una cooperación transfronteriza.

4) Ética

Los participantes deben respetar los intereses legítimos de terceros.

Debido a la permeabilidad de los sistemas y de las redes de información en nuestras sociedades, los participantes necesitan reconocer que sus acciones o la falta de éstas, pueden comportar daños a terceros. Es crucial mantener una conducta ética, debiendo los participantes hacer esfuerzos por desarrollar y adoptar buenas prácticas y promover conductas que reconozcan la necesidad de salvaguardar la seguridad y respetar los intereses legítimos de terceros.

[1] Además de las Directrices sobre Seguridad, la OCDE ha desarrollado Recomendaciones complementarias relativas a las directrices a seguir en otros aspectos importantes de la sociedad de la información mundial. Tales se refieren a la privacidad (Directrices de la OCDE en materia de Protección de la Privacidad y de los flujos transfronterizos de Datos Personales) y a la criptografía (Directrices de la OCDE en materia de Políticas de Criptografía de 1997). Las Directrices sobre Seguridad habrán de ser interpretadas en virtud de éstas otras Directrices.

5) Democracia.

La seguridad de los sistemas y redes de información debe ser compatible con los valores esenciales de una sociedad democrática.

La seguridad debe lograrse de manera consistente con garantía de los valores reconocidos por las sociedades democráticas, incluyendo la libertad de intercambio de pensamiento e ideas, así como el libre flujo de información, la confidencialidad de la información y la comunicación y la protección apropiada de información personal, apertura y transparencia.

6) ***Evaluación del riesgo***

Los participantes deben llevar a cabo evaluaciones de riesgo.

La evaluación del riesgo identificará las amenazas y vulnerabilidades, y debe ser lo suficientemente amplia para incluir factores internos y externos fundamentales como tecnología, factores físicos y humanos, y políticas y servicios de terceros que tengan repercusiones en la seguridad. La evaluación del riesgo permitirá determinar los niveles aceptables de seguridad y ayudar en la selección de controles apropiados para administrar el riesgo de daños potenciales a los sistemas y redes de información, en relación a la naturaleza e importancia de la información que debe ser protegida. Debido a la creciente interconexión de los sistemas de información, la evaluación del riesgo debe incluir asimismo consideraciones acerca del daño potencial que se puede causarse a terceros o que pueden tener su origen en terceras personas.

7) Diseño y realización de la seguridad.

Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.

Los sistemas, las redes y las políticas deberán ser diseñados, ejecutados y coordinados de manera apropiada para optimizar la seguridad. Un enfoque mayor pero no exclusivo de este esfuerzo ha de encontrarse en el diseño y adopción de mecanismos y soluciones que salvaguarden o limiten el daño potencial de amenazas o vulnerabilidades identificadas. Tanto las salvaguardas técnicas como las no técnicas así como las soluciones a adoptar se hacen imprescindibles, debiendo ser proporcionales al valor de la información de los sistemas y redes de información. La seguridad ha de ser un elemento fundamental de todos los productos, servicios, sistemas y redes; y una parte integral del diseño y arquitectura de los sistemas. Para los usuarios finales el diseño e implementación de la seguridad radica fundamentalmente en la selección y configuración de los productos y servicios de sus sistemas.

8) Gestión de la Seguridad.

Los participantes deben adoptar una visión integral de la administración de la seguridad.

La gestión de la seguridad debe estar basada en la evaluación del riesgo y ser dinámica, debiendo comprender todos los niveles de las actividades de los participantes y todos los aspectos de sus operaciones. Asimismo ha de incluir posibles respuestas anticipadas a riesgos emergentes y considerar la prevención, detección y respuesta a incidentes que afecten a la seguridad, recuperación de sistemas, mantenimiento permanente, revisión y auditoría. Las políticas de seguridad de los sistemas y redes de información, así como las prácticas, medidas y procedimientos deben estar coordinadas e integradas para crear un sistema coherente de seguridad. Las exigencias en materia de gestión de seguridad dependerán de los niveles de participación, del papel que desempeñan los participantes, del riesgo de que se trate y de los requerimientos del sistema.

9) Reevaluación

Los participantes deben revisar y reevaluar la seguridad de sus sistemas y redes de información, y realizar las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad.

De manera constante se descubren nuevas amenazas y vulnerabilidades. Los participantes deberán, en este sentido, revisar y evaluar, y modificar todos los aspectos de la seguridad de manera continuada, a fin de poder enfrentarse a riesgos siempre en evolución permanente.

RECOMENDACIÓN DEL CONSEJO RELATIVA A LAS DIRECTRICES PARA LA SEGURIDAD DE SISTEMAS Y REDES DE INFORMACIÓN

HACIA UNA CULTURA DE SEGURIDAD

EL CONSEJO,

Considerando la Convención de la Organización de la Cooperación y Desarrollo Económicos del 14 de diciembre de 1960, y en particular de los artículos 1 b), 1 c), 3 a) y 5 b) ;

Considerando la Recomendación del Consejo en relación con las Guías que Regulan la Protección de la Privacidad y los Flujos Transfronterizos de Datos Personales del 23 de septiembre de 1980 (C(80)58/Final);

Considerando la Declaración sobre Flujos Transfronterizos de Información adoptada por los Países miembros de la OCDE el 11 de abril de 1985 (Anexo al C (85)139);

Considerando la Recomendación del Consejo en materia de Directrices para Políticas de Criptografía del 27 de marzo de 1997 (Anexo al C (97)62/Final);

Considerando la Declaración Ministerial sobre Protección de la Privacidad en las Redes Globales del 7-9 de diciembre de 1998 (Anexo al C (98)177/Final);

Considerando la Declaración Ministerial sobre la Autentificación del Comercio Electrónico del 7-9 de diciembre de 1998 (Anexo al C (98)177/Final);

Reconociendo que los sistemas y redes de información son cada vez más usados y gozan de un valor creciente para los gobiernos, las empresas y otras organizaciones, así como para los usuarios individuales;

Reconociendo que la creciente importancia del papel de los sistemas y redes de información, y la creciente dependencia de ellos para asegurar la estabilidad y eficiencia de las economías nacionales y del comercio internacional, y de la vida social, cultural y política, se hace evidente la necesidad de desarrollar esfuerzos especiales para proteger y promover la confianza en tales medios;

Reconociendo que los sistemas y redes de información, y su proliferación en todo el mundo han estado acompañados de nuevos y crecientes riesgos;

Reconociendo que los datos e información almacenados y transmitidos a través de los sistemas y redes de información están sujetos a las amenazas provenientes de accesos, usos, apropiación y alteración no autorizados, transmisiones fraudulentas de código, caída o destrucción del servicio, y requieren de mecanismos adecuados para salvaguardarlos;

Reconociendo que existe la necesidad de incrementar el conocimiento de los riesgos de los sistemas y redes de información, y de las políticas, prácticas, medidas y procedimientos disponibles para responder a éstos, se hace necesario promover un comportamiento adecuado como paso esencial para el desarrollo de una cultura de seguridad;

Reconociendo que hay una necesidad de revisar las políticas, prácticas, medidas y procedimientos existentes en la actualidad, para asegurar que sean capaces de responder a los retos cambiantes y a las amenazas a los que se enfrentan los sistemas y redes de información;

Reconociendo que es de interés común promover la seguridad de los sistemas y redes de información, mediante una cultura de seguridad que amplíe la coordinación y cooperación internacional para afrontar los riesgos provocados por el daño potencial de fallos en la seguridad de las economías nacionales, el comercio internacional y la vida social, cultural y política;

Y reconociendo también que las *Directrices para la Seguridad de Sistemas y Redes de Información: Hacia una Cultura de Seguridad* establecidas en el Anexo de esta Recomendación son de carácter voluntario y no afectan a los derechos de soberanía de las naciones;

Y reconociendo también que estas Directrices por ningún motivo sugieren que exista una solución única para la seguridad ni políticas, prácticas, medidas o procedimientos apropiados para una situación particular, sino que, más bien, pretenden proporcionar un marco de principios para promover una mejor información por parte de los usuarios a fin de que puedan beneficiarse y contribuir al desarrollo de una cultura de seguridad;

RECOMIENDA estas *Directrices para la Seguridad de Sistemas y Redes de Información: Hacia una Cultura de Seguridad* a los gobiernos, empresas, otras organizaciones y usuarios individuales que desarrollen, posean, provean, administren o proporcionen servicio y usen sistemas y redes de información.

Y RECOMIENDA a los Países Miembros:

Establecer nuevas políticas, prácticas, medidas y procedimientos, o modificar los existentes, para reflejar y tomar en consideración el contenido de las *Directrices para la Seguridad de Sistemas y Redes de Información: Hacia una Cultura de Seguridad*, mediante la adopción y promoción de una cultura de seguridad, tal y como se establece en dichas Directrices;

Desarrollar esfuerzos para consultar, coordinar y cooperar a nivel nacional e internacional, a los efectos de poder implantar estas Directrices;

Dar a conocer dichas Directrices al sector público y privado, incluyendo gobiernos y empresas, y otras organizaciones y usuarios individuales, para promover una cultura de seguridad, y hacer que todas las partes involucradas asuman su responsabilidad en la materia, y adopten las medidas oportunas para ejecutar estas Directrices en la medida de sus posibilidades;

Poner a disposición de países no miembros estas Directrices en el tiempo y forma adecuados;

Revisar estas Directrices cada cinco años para promover la cooperación internacional en aspectos relacionados con la seguridad de los sistemas y redes de información;

INSTA al Comité de Política de Información, Informática y Comunicaciones de la OCDE para promover la implantación de estas Directrices.

Esta Recomendación viene a reemplazar a la Recomendación del Consejo concerniente a las Directrices de Seguridad de los Sistemas de Información del 26 de noviembre de 1992 [C(92)188/Final].

HISTORIA DEL PROCEDIMIENTO

Las Directrices de Seguridad se completaron en 1992 y se revisaron en 1997. La presente revisión se acometió en el año 2001 por el Grupo de expertos de Seguridad de la Información y Protección de la Privacidad (WPISP), de conformidad con el mandato del Comité de Política de la información, Informática y Comunicaciones (ICCP), y acelerada tras la tragedia del 11 de septiembre.

El Proyecto lo emprendió el Grupo de expertos del WPISP, que se reunió en Washington DC, el 10 y 11 de diciembre de 2001, Sydney el 12 y 13 de febrero de 2002 y París del 4 al 6 de marzo de 2002. el WPISP se reunió en París el 5 y 6 de marzo de 2002, el 22 y 23 de abril de 2002, y el 25 y 26 de junio de 2002.

Las presentes *Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad* se adoptaron como Recomendación del Consejo de la OCDE en su 1037 sesión de 25 de julio de 2002.