Guías de la OCDE para la seguridad de los sistemas de información y redes

Hacia una cultura de seguridad

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT
ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS

En virtud del artículo I de la Convención firmada el 14 de diciembre de 1960, en París, y que entró en vigor el 30 de septiembre de 1961, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) tiene como.objetivo promover las políticas destinadas:

- a lograr la más fuerte expansión posible de la economía y del empleo y a aumentar el nivel de vida de los países miembros, manteniendo la estabilidad financiera y contribuyendo así al desarrollo de la economía mundial;
- a contribuir a una sana expansión económica en los países miembros y no miembros en vías de desarrollo económico;
- a contribuir a la expansión del comercio mundial sobre una base multilateral y no discriminatoria conforme a las obligaciones internacionales.

Los firmantes de la Convención constitutiva 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 adherido posteriormente a esta Convención (las fechas corresponden a las del depósito de los instrumentos de adhesión): 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 (21 de diciembre de 1995), Hungría (7 de mayo de 1996), Polonia (22 de noviembre de 1996), Corea (12 de diciembre de 1996) y la República Eslovaca (14 de diciembre de 2000). La Comisión de las Comunidades Europeas participa en los trabajos de la OCDE (artículo 13 de la Convención de la OCDE).

Traducido bajo la responsabilidad del Instituto Nacional de Estadística, Geografía e Informática (INEGI), México, a partir de las versiones originales en inglés y francés, publicadas respectivamente con los títulos:
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

PREFACIO

Desde 1992 cuando la OCDE desarrolló por primera vez las "Guías de Seguridad de los Sistemas de Información a la fecha, se ha presentado un cambio muy dramático en el ambiente general de la tecnología de la información y las comunicaciones, así como en el uso de los sistemas de información y redes. Estos cambios continuos ofrecen grandes ventajas, pero hacen necesario que los gobiernos, los negocios, otras organizaciones y los usuarios que desarrollan, poseen, proporcionan, administran estos servicios y usan sistemas de información y redes (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 propietarias, ha sido sustituido por las computadoras personales que cada vez tienen mayor capacidad de proceso, la convergencia de las tecnologías y la difusión masiva del uso del internet. Hoy en día los participantes se encuentran cada vez más interconectados y estas conexiones se extienden más allá de las fronteras nacionales. Al mismo tiempo, el internet forma parte de la infraestructura de operación de sectores estratégicos como los de energía, transporte y finanzas y desempeña un papel muy importante en la forma en cómo las compañías hacen sus negocios, cómo los gobiernos proporcionan sus servicios a los ciudadanos y a las empresas y cómo los ciudadanos se comunican e intercambian información de manera individual. La naturaleza y el tipo de tecnologías que constituyen la infraestructura de información y comunicaciones también han cambiado de manera significativa. El número y el tipo de aparatos que integran la infraestructura de acceso se ha multiplicado para incluir dispositivos de tecnología fija, inalámbrica y móvil, y una proporción creciente de los accesos 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 la creciente conectividad, los sistemas de información y las redes son más vulnerables ya que están expuestos a un número creciente así como un rango de variedad mayor de amenazas y vulnerabilidades. Esto hace que surjan nuevos retos que deben abordarse en el tema de seguridad. Por estas razones, estas guías aplican para todos los participantes de la nueva sociedad de la información y sugieren la necesidad de tener una mayor consciencia y entendimiento de los aspectos de seguridad, así como de desarrollar una "cultura de seguridad".

I. HACIA UNA CULTURA DE SEGURIDAD

Estas guías responden a un ambiente de seguridad cada vez más cambiante mediante la promoción del desarrollo de una cultura de seguridad – esto es, un enfoque hacia la seguridad en el desarrollo de sistemas de información y redes, así como la adopción de nuevas formas de pensamiento y comportamiento cuando se usan y se interactúa mediante sistemas de información y redes. Estas guías marcan un rompimiento con los tiempos en que los aspectos de seguridad al desarrollar redes y sistemas se consideraban como un elemento a posteriori. La operación de los sistemas de información, redes y servicios afines debe ser confiable y segura ya que los participantes se han vuelto 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 proveer una seguridad efectiva.

Cada participante es un actor importante para garantizar la seguridad. Cada participante de acuerdo al papel que desempeña deberá estar consciente de los riesgos de la seguridad y de las medidas preventivas correspondientes, deberá asumir la responsabilidad correspondiente y tomar las medidas que permitan fortalecer la seguridad de los sistemas de información y las redes.

La promoción de una cultura de seguridad requiere tanto de un liderazgo fuerte como de una participación amplia para asegurar que se le otorgue un carácter de prioritario a la planeación y administración de la seguridad, así como del entendimiento de la necesidad de seguridad para todos los participantes. Los temas de seguridad deberán ser tópicos de preocupación y responsabilidad para todos los niveles de gobierno, negocios y todos los participantes. Las guías proponen adoptar y promover una cultura de seguridad para toda la sociedad. Esto permitirá que los participantes consideren la seguridad en el diseño y uso de los sistemas de información y de las redes. Las guías proponen que todos los participantes adopten y promuevan una cultura de seguridad como una manera de pensar sobre este tema, así como de evaluar y actuar en relación a los sistemas de información y redes.

II. PROPÓSITOS

Los propósitos de estos lineamientos son:

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

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

-- Promover entre todos los participantes una confianza mayor en los sistemas de información y las redes, la forma en la que operan y se usan.

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

-- Promover entre todos los participantes cuando sea apropiado, la cooperación y el intercambio de información sobre el desarrollo e implementación de políticas de seguridad, prácticas, medidas y procedimientos.

-- Promover la consideración del tema de seguridad como un objetivo importante a lograr por parte de todos los participantes involucrados en el desarrollo e implementación de estándares.

III. PRINCIPIOS

Los siguientes nueve principios son complementarios y deben ser leídos de manera integral. Éstos le competen a todos los participantes de todos los niveles, tanto los del ámbito político como operacional. De acuerdo con estos lineamientos, la responsabilidad de ellos varía de acuerdo con los papeles que desempeñen. Todos se verán beneficiados por la conscientización, educación, intercambio de información y capacitación que conlleven a la adopción de un mejor entendimiento de la seguridad y las prácticas que se requieren. Los esfuerzos para fortalecer la seguridad de los sistemas de información y de las redes 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] Además de las Guías de Seguridad, la OCDE ha desarrollado recomendaciones complementarias concernientes a los lineamientos de otros aspectos importantes de la sociedad de la información mundial. Esto se relaciona con la privacidad (en 1980 las Guías OCDE de Protección a la Privacidad y de los flujos entre fronteras de Datos Personales) y criptografía (la OCDE en 1997 Guía de las Políticas de Criptografía). Las guías de seguridad deben ser leídas de manera conjuntas con ésta.

1) Conscientización

Los participantes deben estar conscientes de la necesidad de contar con sistemas de información y redes seguros, y qué es lo que pueden hacer para promover y fortalecer la seguridad.

La conscientización de los riesgos y de los mecanismos disponibles para salvaguardarla, es el primer paso en la defensa de la seguridad de los sistemas de información y redes. Éstos pueden ser afectados tanto por riesgos internos como externos. Los participantes deben entender que las fallas de seguridad pueden repercutir en daños significativos a los sistemas y a las redes que están bajo su control. Deben estar conscientes del daño potencial que esto puede provocar a otros derivados de la interconectividad y la interdependencia. Los participantes deben estar conscientes de: las configuraciones y actualizaciones disponibles para sus sistemas, su lugar dentro de las redes, las mejores prácticas que pueden implementar para fortalecer la seguridad y las necesidades de otros participantes.

2) Responsabilidad

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

Los participantes que dependen de sistemas de información y redes interconectados de manera local y global deben comprender su responsabilidad en salvaguardar la seguridad de éstos. Deben de responder ante esta responsabilidad de una manera apropiada a su papel individual. Los participantes deben revisar sus propias políticas, prácticas, medidas y procedimientos de manera regular y evaluar si éstos son apropiados en relación a su entorno. Aquellos que desarrollan y diseñan o proveen productos o servicios deben considerar la seguridad de los sistemas y redes y distribuir a los usuarios de manera oportuna información apropiada incluyendo actualizaciones para que éstos entiendan mejor la funcionalidad de la seguridad de sus productos y servicios y la responsabilidad de ellos en relación a este tema.

3) Respuesta

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

Al reconocer la interconectividad de los sistemas de información y de las redes, así como el riesgo potencial de un daño que se extienda con rapidez y tenga una alcance amplio, los participantes deben actuar de manera oportuna y cooperativa para enfrentar los incidentes que afecten la seguridad. Cuando sea apropiado deben compartir información sobre los riesgos y vulnerabilidades e implementar procedimientos para una cooperación rápida y efectiva que permita prevenir, detectar y responder a incidentes que afecten la seguridad. Cuando sea permitido, esto puede implicar el intercambio de información y cooperación transfronteriza.

4) Ética

Los participantes deben respetar los intereses legítimos de los otros.

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

5) Democracia.

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

La seguridad debe ser implementada de manera consistente con 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 identifica las amenazas y vulnerabilidades y debe ser lo suficientemente amplia para incluir los factores internos y externos fundamentales como tecnología, factores físicos y humanos, políticas y servicios de terceros que tengan implicaciones en la seguridad. La evaluación del riesgo permite determinar los niveles aceptables de seguridad y ayudar en la selección de controles apropiados para administrar el riesgo de daños potenciales a los sistemas de información y redes, en relación a la naturaleza e importancia de la información que debe ser protegida. Debido a la creciente interconectividad de los sistemas de información, la evaluación del riesgo debe incluir consideraciones acerca del daño potencial que puede ser provocado por otros o que puede ocasionarse a otros.

7) Diseño e implementación de seguridad.

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

Los sistemas, las redes y las políticas deben ser diseñados, implementados y coordinados de manera apropiada para optimizar la seguridad. Un enfoque mayor pero no exclusivo de este esfuerzo está en el diseño y adopción de mecanismos y soluciones que salvaguarden o limiten el daño potencial hacia amenazas o vulnerabilidades que se hayan identificado. Las salvaguardas y mecanismos técnicos y no técnicos son

necesarios y deben ser proporcionales al valor de la información de los sistemas de información y redes de la organización. La seguridad debe 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 para sus sistemas.

8) Administración de la Seguridad.

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

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

9) Reevaluación

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

De manera constante se descubren nuevas amenazas y vulnerabilidades. Los participantes deben revisar y evaluar, modificar todos los aspectos de la seguridad de manera continua, a fin de poder enfrentar los riesgos que se encuentran en evolución permanente.

RECOMENDACIONES DEL CONSEJO DE LA OCDE

El Consejo,

Considerando que:

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) así como

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);

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);

La Recomendación del Consejo respecto a las Guías para Políticas de Criptografía del 27 de marzo de 1997 (Anexo al C (97)62/Final);

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

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

Y reconociendo:

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

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

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

Que los datos e información almacenados y transmitidos a través de los sistemas de información y redes están sujetos a amenazas de accesos, usos, apropiación y alteración no autorizados, transmisión de código dañino, caída o destrucción del servicio, y requieren de mecanismos adecuados para salvaguardarlos:

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

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

Que es del interés común promover la seguridad de los sistemas de información y redes mediante una cultura de seguridad que promueva la coordinación y cooperación internacional para enfrentar los riesgos para las economías nacionales, el comercio internacional y la vida social, cultural y política provocados por el daño potencial de fallas en la seguridad.

Reconociendo también:

Que las *Guías para la Seguridad de los Sistemas de Información y Redes: Hacia una Cultura de Seguridad* puestas en este anexo son recomendaciones de carácter voluntario y no afectan los derechos de la soberanía de las naciones;

Que estas guías por ningún motivo sugieren que exista una solución única para la seguridad o qué políticas, prácticas, medidas y procedimientos son apropiados para una situación particular, sino más bien, buscan proveer un marco de principios para promover una mejor comprensión de cómo los participantes pueden beneficiarse y contribuir al desarrollo de una cultura de seguridad;

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

Recomienda a los Países Miembros:

Establecer nuevas o modificar las políticas, prácticas, medidas y procedimientos con que cuenten para reflejar y tomar en cuenta el contenido de las *Guías para la Seguridad de los Sistemas de Información y Redes: Hacia una Cultura de Seguridad* mediante la adopción y promoción de una cultura de seguridad como proponen estas guías;

Desarrollar esfuerzos para consultar, coordinar y cooperar a nivel nacional e internacional a efecto de poder implantar estas guías;

Dar a conocer las guías al sector público y privado, incluyendo las organizaciones de los gobiernos, los negocios y otras y usuarios individuales para promover una cultura de seguridad y hacer que todas las partes involucradas respondan a este llamado, desarrollen las acciones necesarias para implementar estas guías de una manera adecuada a sus papeles individuales;

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

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

Instruye al Comité de Política de Información, Computación y Comunicaciones de la OCDE para promover la implantación de estas guías.

Esta recomendación sustituye la recomendación del Consejo concernientes a las Guías de Seguridad de los Sistemas de Información del 26 de noviembre de 1992 (C(92)188/Final).

HISTORIA DEL PROCEDIMIENTO

Las guías de seguridad se concluyeron por primera vez en 1992, y fueron revisadas en 1997. La revisión actual fue iniciada en el 2001 por el Grupo de Trabajo sobre Seguridad de la Información y Privacidad (GTSIP) en cumplimiento a un mandato del Comité de Políticas para la Información, Computación y Comunicaciones (CPICC) y acelerada por los eventos trágicos del 11 septiembre del 2002.

La redacción fue elaborada por el grupo experto de GTSIP, quienes se reunieron en:
Washington DC el 10 y 11 de diciembre de 2001,
Sydney el 12 y 13 de febrero de 2002,
París el 4 y 6 de marzo de 2002.

El GTSIP se reunió en PARIS el 5 y 6 de marzo del 2002, el 22 y 23 de abril, así como el 25 y 26 de junio de 2002.