# ANEXO XVIII

## MARCO DE PRIVACIDAD DEL FORO DE COOPERACIÓN ECONÓMICA ASIA PACÍFICO (APEC)

Los flujos de información son vitales para llevar a cabo negocios en una economía global. El Marco de Privacidad de APEC promueve un acercamiento flexible a la protección de la privacidad de la información en las Economías Miembro de APEC, evitando la creación de barreras innecesarias para los flujos de información.

Traducido y reproducido con permiso de la Secretaría de APEC. Traducido del inglés, el idioma original del documento, por la Secretaría de Economía del Gobierno de México. Información tomada de "APEC Privacy Framework" ISBN981-05-4471-5, APEC#205-SO-01.2. Número de publicación de APEC asignado a la traducción: APEC#206-TC-06.2.

Publicado por
Secretariado de APEC, Terraza Heng Mui Keng 35, Singapur 119616
Tel: (65) 6775 6012 Fax: (65)6775 6013
Correo electrónico: info@apec.org Página en Internet: www.apec.org

ISBN 981-05-4471-5
APEC#205-SO-012
2005 Secretariado de APEC
MARCO DE PRIVACIDAD DE APEC

# PRÓLOGO

Las Economías Miembro del Foro de Cooperación Económica Asia Pacífico (APEC por sus siglas en inglés) se dan cuenta del enorme potencial del comercio electrónico para expandir las oportunidades empresariales, reducir costos, incrementar la eficiencia, mejorar la calidad de vida y facilitar la participación de los pequeños negocios en el comercio global. Un marco que permita la transferencia de datos regionales beneficiará a los consumidores, a las empresas y a los gobiernos. Ministros han aprobado el Marco de Privacidad de APEC, reconociendo la importancia de desarrollar protecciones efectivas para la privacidad que eviten barreras a los flujos de información, asegurar en intercambio continuo y el crecimiento económico en la región APEC.

CONTENIDO:

## Parte 1. Preámbulo

1. Las Economías Miembro del Foro de Cooperación Económica Asia Pacífico (APEC por sus siglas en inglés) reconocen la importancia de proteger la privacidad de la información y mantener los flujos de información entre Economías de la región Asia Pacífico y entre sus socios comerciales. Como lo reconocieron los Ministros de APEC al aprobar el Programa para la Acción en el Comercio Electrónico 1998, el potencial del comercio electrónico no puede llevarse a cabo sin la cooperación del gobierno y de las empresas "para desarrollar e implementar tecnologías y políticas que establezcan confianza en cuanto a comunicación, información y sistemas de entrega seguros, protegidos y fidedignos, y que traten asuntos que incluyan la privacidad...". La falta de confianza del consumidor hacia la privacidad y seguridad de transacciones en línea y redes de información es un elemento que puede impedir a las Economías Miembro, obtener todos los beneficios del comercio electrónico. Las Economías de APEC se dan cuenta que una parte de los esfuerzos clave para mejorar la confianza del consumidor y asegurar el crecimiento del comercio electrónico, debe ser la cooperación para balancear y promover la protección de la privacidad de la información y el libre flujo de información en la región Asia Pacífico.

2. Tecnologías de información y comunicación, incluyendo tecnologías móviles que se conectan a Internet y a otras rede de información, han hecho posible recopilar, almacenar y acceder a la información desde cualquier parte del mundo. Estas tecnologías ofrecen gran potencial para beneficios económicos y sociales para las empresas, los individuos y los gobiernos, incluyendo aumento en las opciones del consumidor, expansión del mercado, productividad, educación e innovación de productos. Sin embargo, mientras estas tecnologías abaratan y facilitan el recopilar, conectar y usar grandes cantidades de información, a menudo también hacen que estás actividades pasen desapercibidas para los individuos. Por consiguiente, puede ser más difícil para los individuos conservar una medida de control sobre su información personal. Como resultado de esto, los individuos se han preocupado por las dañinas consecuencias que puedan surgir del mal uso de su información. Por lo tanto, hay una necesidad de promover y hacer cumplir prácticas fidedignas de información en contextos en línea y no en línea para reforzar la confianza de los individuos y las empresas.

3. Como las operaciones comerciales y las expectativas de los consumidores continúan moviéndose debido a cambios en la tecnología y en la naturaleza de los flujos de información, empresas y otras organizaciones requieren entradas simultáneas y acceso a información 24 horas al día para satisfacer necesidades de la clientela y la sociedad, y proporcionar servicios eficientes y rentables. Sistemas reguladores que restringen innecesariamente este flujo o le imponen cargas, tienen implicaciones adversas para el comercio global y para las Economías. Por lo tanto, para promover y hacer cumplir prácticas éticas de información, existe la necesidad de desarrollar sistemas para proteger la privacidad de la información, que den cuenta de estas nuevas realidades en el ambiente global.

4. Las Economías de APEC aprueban el Marco de Privacidad de APEC basado en principios, como una herramienta importante para alentar el desarrollo de protecciones apropiadas a la privacidad de la información y para asegurar el libre flujo de información en la región Asia Pacífico.

5. Este Marco de trabajo, cuyo objetivo es promover el comercio electrónico en toda la región Asia Pacífico, concuerda con los valores básicos de los Lineamientos de Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de 1980 de la OCDE (Lineamientos de la OCDE)[1] , y reafirma el valor de la privacidad para los individuos y para la sociedad de información.

6. El Marco se dirige específicamente a estos conceptos base, así como a asuntos de particular relevancia para las Economías Miembro de APEC. Su distintivo acercamiento es para enfocar la atención en la protección práctica y consistente de la privacidad de la información dentro de este contexto. Al hacerlo, balancea la privacidad de la información con las necesidades empresariales y los intereses comerciales, y al mismo tiempo concede el debido reconocimiento a las diversidades culturales y de otro tipo que existan entre las Economías Miembro.

7. La intención del Marco es proporcionar una clara orientación y dirección a empresas dentro de las Economías de APEC, sobre asuntos comunes de privacidad y del impacto de estos asuntos en la forma en como se con-

[1] Los Lineamientos de 1980 fueron redactados a un nivel alto, lo cual los hacen relevantes en la actualidad. En muchas maneras, los Lineamientos de la OCDE representan el consenso internacional acerco de lo que constituye un tratamiento honesto y fidedigno de la información personal.

ducen negocios legítimos, y lo hace destacando las expectativas razonables del consumidor moderno de que las empresas reconocerán sus intereses de privacidad de forma consistente con los Principios explicados en este Marco.

8. Finalmente, este Marco sobre información de la protección de la privacidad fue desarrollado reconociendo la importancia de:

- Desarrollar protecciones apropiadas para la información personal, particularmente contra las dañinas consecuencias de intrusiones no deseadas y del uso incorrecto de la información personal;
- Reconocer el libre flujo de información como algo esencial para Economías de mercado desarrolladas y en desarrollo, para sustentar el crecimiento económico y social;
- Posibilitar organizaciones globales que recopilen, accedan, usen o procesen información en Economías de APEC para desarrollar e implementar acercamientos uniformes dentro de sus organizaciones para tener acceso global y uso de la información personal;
- Posibilitar agencias de seguridad para cumplir con su mandato de proteger la privacidad de la información; y,
- Presentar mecanismos internacionales para promover y hacer cumplir la privacidad de la información, y mantener la continuidad de los flujos de información entre Economías de APEC y sus socios comerciales.

## Parte ii. Alcance

El propósito de la Parte II del Marco de Privacidad de APEC es dejar en claro el alcance de la cobertura de los Principios.

### Definiciones

9. Información Personal significa cualquier información acerca de un individuo identificado o identificable.

9. Los Principios han sido redactados tomando en cuenta el antecedente en el que algunas Economías tienen leyes de privacidad y/o prácticas bien establecidas, mientras que otras pueden estar considerando el asunto. De aquellas con políticas ya establecidas, no todas tratan la información personal exactamente de la misma forma. Algunas, por ejemplo, pueden establecer distinciones entre la información que ya puede ser buscada y otro tipo de información. A pesar de estas dife-

rencias, este Marco ha sido redactado para promover un acercamiento constante entre los sistemas de privacidad de la información de las Economías de APEC.

Es Marco tiene está pensado para aplicarse a la información sobre personas naturales, no legales. El Marco de Privacidad de APEC aplica a información personal, que es información que puede usarse para identificar a un individuo. También incluye información que cumpla con este criterio por sí sola, sino que, aunada a otra información, pudiera identificar a un individuo.

10. Controlador de información personal significa una persona u organización que controla la recolección, posesión, procesamiento o uso de información personal. Incluye a una persona u organización que instruye a otra persona u organización para recolectar, guardar, procesar, usar, transferir o revelar información personal en su nombre, pero excluye a una persona u organización que desempeñe dichas funciones por instrucciones de otra persona u organización. También excluye a un individuo que recopile, guarde, procese o use información personal con respecto a asuntos personales, familiares o domésticos del individuo.

10. EL Marco de Privacidad de APEC aplica a personas u organizaciones en los sectores público y privado que controlan la recolección, posesión, procesamiento, uso, transferir o revelar información personal. Las definiciones individuales de las Economías de "controlador de información personal", pueden variar. Sin embargo, las Economías de APEC a reconocen que, para los propósitos de este Marco, cuando una persona u organización instruye a otra persona u organización a recolectar, guardar, usar, procesar, transferir o revelar información personal en su nombre, la persona u organización instructora es el controlador de información personal y es el responsable de asegurar la conformidad con los Principios.

Individuos usualmente recopilarán, guardarán y usarán información personal para fines personales, familiares o domésticos. Por ejemplo, usualmente tienen agendas de direcciones o teléfonos, o preparan boletines informativos familiares. El Marco no tiene el propósito de aplicar a ese tipo de actividades personales, familiares o domésticas.

11. Información a disposición del público significa información personal acerca de un individuo, que él mismo hace o permite que esté disponible al público, o es obtenida o accedida legalmente desde:

a) Registros del gobierno que están disponibles para el público;
b) Reportes periodísticos; o
c) Información requerida para por la ley para ser puesta a disposición del público.

11. El Marco de Privacidad de APEC tiene aplicación limitada a la información a disposición del público. Requerimientos de aviso y elección, en particular, son usualmente donde la información ya está a disposición del público, y en controlador de información personal no recopila la información directamente del individuo interesado. La información a disposición del público puede estar contenida en registros del gobierno disponibles al público, tales como: registros de personas que tiene derecho a votar, noticias transmitidas o publicadas por los noticiarios.

## Aplicación

12. En vista de las diferencias sociales, culturales, económicas y legales de cada Economía miembro, debe haber flexibilidad para implementar estos Principios.

12 Aunque no es esencial para el comercio electrónico que todas las leyes y prácticas dentro de APEC sean idénticas en todos los aspectos, incluyendo la cobertura de información personal, acercamientos compatibles a la protección de la privacidad de la información entre las Economías de APEC facilitarán mucho el comercio internacional. Estos principios reconocen ese hecho, pero también toman en cuenta las diferencias sociales, culturales y de otro tipo entre las Economías. Se concentran en esos aspectos de la protección de la privacidad que son lo más importante para el comercio internacional.

13. Excepciones a estos Principios contenidas en la Parte II de este Marco, incluyendo aquellas relacionadas a la soberanía nacional, seguridad nacional, seguridad pública y política pública deberán:

a) ser limitadas y proporcionales para cumplir los objetivos a los que se relacionan estas excepciones; y,
b) (i) ser dadas a conocer al público; o, (ii) estar de acuerdo con la ley.

13 Los Principios contenidos en la Parte II del Marco de Privacidad de APEC deberán ser interpretados como un todo en lugar de individualmente, ya que hay una relación cercana entre ellos. Por ejemplo, el Principio de Uso está íntimamente relacionado con los Principios de Aviso y Elección. Las Economías que implementen el Marco a nivel doméstico pueden adoptar excepciones adecuadas que convengan a sus circunstancias domésticas particulares.
Aunque reconozcan la importancia del respecto gubernamental a la privacidad, este Marco no pretende obstaculizar las actividades gubernamentales autorizadas por la ley cuando se usen para proteger la seguridad nacional, la seguridad pública, la soberanía nacional u otras políticas públicas. Sin embargo, las Economías deben considerar el impacto de estas actividades sobre los derechos, responsabilidades e intereses legítimos de individuos u organizaciones.

## PRINCIPIOS DE PRIVACIDAD DE LA INFORMACIÓN FORO DE COOPERACIÓN ECONÓMICA ASIA PACÍFICO (APEC)

### Parte III. Principios de privacidad de la información de APEC

### PRINCIPIO: I. Previniendo Daño

14 Reconocer los intereses del individuo para legitimar expectativas de privacidad, la protección de la información personal debe ser diseñada para prevenir el mal uso del tal información. Además, reconocer el riesgo de que puede haber daños por el mal uso de la información personal, obligaciones específicas deben tomar en cuenta tal riesgo y medidas de saneamiento deben ser proporcionales a la probabilidad y severidad del daño amenazado por la recolección, uso y transferencia de información personal.

COMENTARIO: (14) El Principio Previniendo Daño reconoce que uno de los objetivos fundamentales del Marco de Privacidad de APEC es prevenir el mal uso de la información personal y, por consiguiente, el daño a los individuos. Por lo tanto, protecciones a la privacidad, incluyendo esfuerzos autorreguladores, campañas de educación y conciencia, leyes, regulaciones y mecanismos de seguridad deben ser diseñados para prevenir daño a los individuos por la recolección ilegal y el mal uso de su información personal. Por consiguiente, remedios para violaciones a la privacidad

deben ser diseñados para prevenir daños por la recolección ilegal o el mal uso de la información personal, y deberán ser proporcionales a la probabilidad y severidad de cualquier daño amenazado por la recolección o uso de la información personal.

PRINCIPIO: II. Aviso

15 Controladores de Información Personal deben proporcionar declaraciones claras y de fácil acceso acerca de sus prácticas y políticas por lo que respecta a la información personal, que deben incluir:

I. El hecho de que información personal está siendo recopilada;
II. Los propósitos para los que se está recopilando la información personal;
III. Los tipos de personas u organizaciones a las que se les podría revelar la información personal;
IV. La identidad y ubicación del controlador/ director de información personal, incluyendo información de cómo contactarlos respecto a sus prácticas y manejo de la información personal;
V. La elección de medios que el controlador/ director de la información personal ofrece a los individuos para limitar el uso, revelación, acceso y corrección de su información.

16 Todos los pasos razonablemente viables deberán ser tomados para asegurar que se proporcione el aviso antes o al momento de recopilar la información personal. De lo contrario, dicho aviso deberá ser proporcionado tan pronto como sea factible.

17 Quizá no se apropiado que los controladores de información personal proporcionen aviso respecto a la recolección y uso de la información disponible para el público.

COMENTARIOS: (15-17) El Principio de Aviso está dirigido para asegurar que los individuos sean capaces de saber qué información se recopila acerca de ellos y con qué propósito. Al proporcionar aviso, los controladores de la información personal pueden permitirle al individuo tomar una decisión más informada acerca de interactuar con la organización. Un método común para estar en conformidad con este Principio es que los controladores de la información personal coloquen avisos en sus sitios de Internet. En

otras situaciones, por ejemplo, la colocación de avisos en sitios de Intranet o en manuales para empleados podría ser apropiada.

La necesidad en este Principio relativo a cuando debe proporcionarse aviso, se basa en un consenso entre las Economías Miembro de APEC. Las Economías Miembro de APEC acordaron que una buena práctica de privacidad es informar a los individuos al momento que o antes de que la información acerca de ellos sea recolectada. Al mismo tiempo, el Principio también reconoce que hay circunstancias en las que no será aplicable dar aviso antes de la recolección, tal como en los casos en los que tecnología electrónica recopile información automáticamente cuando un consumidor potencial inicie contacto, como es el caso con el uso de cookies.

Por otra parte, cuando la información personal no sea obtenida directamente del individuo sino a través de terceros, quizá no aplique dar aviso antes o al momento de la recolección de la información. Por ejemplo, cuando una compañía de seguros recopile información de los empleados por medio del patrón para proporcionar servicios de seguros médicos, quizá no sea aplicable que la compañía de seguros de aviso antes o al momento de recopilar la información personal de los empleados.

Además, hay situaciones en las que no será necesario proporcionar aviso, tales como: recolección y uso de información disponible al público, de información de contacto de las empresas y de otra información profesional que identifique a un individuo en su capacidad dentro del contexto de una empresa. Por ejemplo, si un individuo le da a otro su tarjeta de presentación en el contexto de una relación de negocios, el individuo no esperará que el aviso se proporcione respecto a la recolección y uso normal de esa información.

Aún más, si colegas que trabajan para la misma empresa que el individuo proporcionaran la información de contacto del mismo, a consumidores potenciales para la empresa, el individuo no esperará que se le proporcione aviso respecto a la trasferencia o el uso esperado de esa información.

PRINCIPIO: III. Limitación de Recolección

18. La recolección de la información personal deberá ser limitada a aquella información que sea relevante a los propósitos de recolección y dicha información deberá ser obtenida por medios legales y justos, y cuando sea apropiado, con consentimiento y dando aviso al individuo en cuestión.

COMENTARIO: (18) Este Principio limita la recolección de información haciendo alusión a los propósitos para los que es recopilada. La reco-

lección de la información deberá ser relevante a tales propósitos, y un factor podrá ser proporcional al cumplimiento de dichos propósitos para determinar lo que es relevante.

El Principio también provee que lo método de recolección deben ser lícitos y leales. Así que, por ejemplo, obtener información personal con falsas pretensiones (por ejemplo, cuando una organización usa llamadas de telemercadeo, publicidad impresa o mande correo electrónicos representándose fraudulentamente como otra compañía para engañar a los consumidores e inducirlos a revelar los números de sus tarjetas de crédito, información de cuentas bancarias u otra información personal sensible) puede ser considerado ilícito en muchas Economías. Por lo tanto, aun en esas Economías en las que no hay una ley explícita contra estos métodos, pueden ser considerados métodos desleales de recolección.

El Principio también reconoce que hay circunstancias en las que, proporcionar aviso u obtener el consentimiento de individuos, será inapropiado. Por ejemplo, en una situación en la que hay brote intoxicación por alimentos, sería apropiado para las autoridades sanitarias relevantes el recopilar información personal de patrones de restaurantes sin proporcionarles aviso o sin obtener el consentimiento de los individuos para comentarles del riesgo potencial de salud.

PRINCIPIO: IV. Usos de la Información Personal

19. La información personal recopilada sólo debe ser usada para cumplir con los propósitos de recolección y otros propósitos compatibles o relacionados, excepto:

a. Con el consentimiento del individuo cuya información personal es recopilada;
b. Cuando sea necesaria para proporcionar un servicio solicitado por el individuo; o,
c. Por la autoridad de la ley y otros instrumentos legales, proclamas y pronunciamientos de efecto legal.

COMENTARIO (19) El Principio de Uso limita el uso de información personal para cumplir con los propósitos de recolección y otros propósitos compatibles o relacionados. Para los propósitos de este Principio, "usos de información personal" incluye la transferencia o revelación de información personal.

La aplicación de este Principio requiere considerar de la naturaleza de la información, el contexto de la recolección y el uso deseado para esa información. El criterio fundamental para determinar si un propósito es compatible con o está relacionado con los propósitos indicados, es si el uso extendido proviene de o respalda tales propósitos. El uso de información personal con "propósitos compatibles o relacionados" extenderá, por ejemplo, a cuestiones como la creación o uso de una base de datos centralizada para manejar al personal de una manera efectiva y eficiente; el procesamiento por un tercero, de las nóminas de empleados; o, el uso de información recopilada por una organización con el propósito de otorgar crédito para el propósito subsiguiente de cobrar una deuda a esa organización.

PRINCIPIO: V. Elección

20. Cuando sea apropiado, se le deben proporcionar a los individuos mecanismos claros, prominentes, de fácil entendimiento, accesibles y asequibles para ejercitar la elección en relación a la recolección, uso y revelación de su información personal. Puede que no sea apropiado que los controladores de la información personal proporcionen estos mecanismos cuando recopilen información disponible para el público.

COMENTARIO (20) El propósito general del Principio de Elección es asegurar que los individuos tengan una opción con relación a la recolección, uso, transferencia y revelación de su información personal. Ya sea que la información sea transmitida electrónicamente, por escrito o por otros medios, aviso de tal elección debe ser comunicado y mostrado de manera clara y evidente. Del mismo modo, los mecanismos para ejercitar la elección deben ser accesibles y asequibles para los individuos. Facilidad de acceso y conveniencia son factores que deben ser tomados en cuenta.

Cuando una organización proporcione información sobre mecanismos disponibles para ejercitar una elección específicamente adaptada para los individuos en una Economía miembro de APEC o en un grupo nacional, se requerirá que la información sea transmitida de una manera "fácilmente entendible" o apropiada para lo miembros de ese grupo (por ejemplo, en un lenguaje en particular). Sin embargo, si la comunicación no está dirigida a ninguna Economía en particular ni a un grupo nacional distinto de aquel donde se localiza la organización, este requisito puede no aplicar.

Este Principio también reconoce, a través de las palabras introductorias "cuando sea apropiado", que hay ciertas situaciones en las que el consenti-

miento puede estar claramente implícito o cuando no sea necesario proporcionar un mecanismo para ejercitar la elección.

Como está especificado en el Principio, las Economías Miembro de APEC acuerdan que en muchas situaciones, no será necesario ni práctico proporcionar un mecanismo para ejercitar la elección cuando se recopile información públicamente disponible. Por ejemplo, no será necesario proporcionarle un mecanismo para ejercitar la elección a los individuos cuando se recopile su nombre y dirección de un registro público o de un periódico.

Además de situaciones que involucren información públicamente disponible, las Economías Miembro de APEC también acordaron que en circunstancias limitadas y específicas, no será necesario ni práctico proporcionar un mecanismo para ejercitar la elección al recopilar, usar, transferir o revelar otro tipo de información. Por ejemplo, cuando información de contacto u otro tipo de información que identifique a un individuo en su capacidad profesional esté siendo intercambiada en un contexto empresarial, generalmente no es práctico ni necesario proporcionar un mecanismo para ejercitar la elección, porque en estas circunstancias los individuos esperarían que su información fuera usada de esta manera.

Además, en ciertas situaciones, no será práctico que a los patrones se les requiera proporcionar un mecanismo para ejercitar la elección relacionada a la información personal de su empleados cuando usen esa información con propósitos de trabajo, Por ejemplo, si una organización ha decidido centralizar la información de recursos humanos, no se le requerirá proporcionar un mecanismo para ejercitar la elección a su empleados antes de dedicarse a tal actividad.

PRINCIPIO: VI. Integridad de la Información Personal

21. La información personal debe ser exacta, completa y debe estar actualizada al grado necesario para los propósitos para los que será usada

COMENTARIO (21) Este Principio reconoce que un controlador de información personal está obligado a mantener los registros completos, con cierta exactitud y actualizados. Tomar decisiones acerca de los individuos basadas en información inexacta, incompleta o no actualizada no es del interés de los individuos ni de las organizaciones. Este Principio también reconoce que estas obligaciones sólo son requeridas en el grado necesario para los propósitos de uso.

PRINCIPIOS VII. Medidas de Seguridad

22. Los controladores de información personal deben proteger la información personal que guarden con medidas de seguridad apropiadas contra riesgos, tales como pérdida o acceso desautorizado a la información personal, o destrucción desautorizada, uso, modificación o revelación de información o cualquier otro uso incorrecto. Tales medidas de seguridad deben ser proporcionales a la probabilidad y severidad del daño obtenido, a la sensibilidad de la información y al contexto en el que es guardada y quedarán sujetas a una revisión periódica y a una nueva evaluación.

COMENTARIO (22) Este Principio reconoce que los individuos que encomienden su información personal a otro, tiene derecho a esperar que su información sea protegida con medidas de seguridad razonables.

PRINCIPIOS: VIII. Acceso y Corrección

23. Los individuos deben ser capaces de:

a) Obtener confirmación del controlador de información acerca de si éste posee información personal acerca de ellos

b) Haberles comunicado, tras haber proporcionado pruebas suficientes de su identidad, información personal acerca de ellos;

i. dentro de un tiempo razonable;
ii. a un costo, si es que hay alguno, que no sea excesivo:
iii. de manera razonable;
iv. de forma entendible: y,

c) Desafiar la exactitud de la información relacionada con ellos y, si es posible y como sea adecuado, rectificar, completar, corregir o borrar la información.

24. Tal acceso y oportunidad para corrección deberá ser proporcionado, excepto cuando:

(i) La carga o el gasto de hacerlo no fuera razonable ni proporcional a los riesgos sobre la privacidad del individuo en el caso en cuestión;

(ii) La información no deberá ser revelada por razones legales o de seguridad, ni para proteger información comercial confidencial; o

(iii) La privacidad de la información de personas, y no del individuo, fuera violada.

25. Si una solicitud bajo (a) o (b), o un desafío bajo (c) es negada, se deberán proporcionar al individuo las razones del por qué, y éste será capaz de desafiar tal negación.

COMENTARIOS (23-25) La habilidad para acceder y corregir la información personal, que generalmente se considera un aspecto central de la protección a la privacidad, no es un derecho absoluto. Este Principio incluye condiciones específicas para lo que sería considerado razonable en el suministro de acceso, incluyendo condiciones relacionadas con sincronización, cuotas y con la manera y forma en la que se proporcionará el acceso. Lo que será considerado razonable en cada una de estas áreas, variará de una situación a otra, dependiendo de las circunstancias, tales como la naturaleza de la actividad que procesará la información. El acceso también será condicionado por los requerimientos de seguridad que impidan el acceso directo a la información y requerirán pruebas suficientes de identidad previas al acceso. El acceso debe ser proporcionado de forma y manera razonable. Una manera razonable debe incluir los métodos normales de interacción entre organizaciones e individuos.

Por ejemplo, si se involucró el uso de una computadora en la transacción o la solicitud, y el correo electrónico del individuo está disponible, éste será considerado "una manera razonable" para proporcionar información. Las organizaciones que negociado con un individuo deberán responder solicitudes de una forma similar a la que se usó en intercambios previos con el individuo mencionado o en la forma que sea usada y que esté disponible dentro de la organización, pero no debe entenderse que requieran traducción a otro idioma o conversión de código al texto.

Tanto la copia de la información personal suministrada por una organización en respuesta a una solicitud de acceso, como cualquier explicación de códigos usados por la organización, siempre deberán ser entendibles. Esta obligación no se extiende a la conversión de lenguaje computacional (por ejemplo, instrucciones que leen máquinas, códigos de fuente o códigos de objeto) al texto. Sin embargo, cuando un código represente en un significado en particular, el controlador de información personal deberá explicar el significado del código al individuo. Por ejemplo, si la información personal guardada por la organización incluye el rango de edad del individuo, y está representado por un código en particular (por ejemplo, "1" significa

18-25 años de edad, "2" significa 26-35 años de edad, etc.), entonces cuando se proporcione tal código al individuo, la organización debe explicarle qué rango de edad representa ese código.

Cuando un individuo solicite acceso a su información, ésta deberá ser proporcionada en el idioma en el que esté guardada. Cuando la información esté guardada en un idioma distinto al de la recolección original, y si el individuo solicita que se le proporcione en ese idioma original, una organización debe suministrar la información en el idioma original si el individuo paga el costo de la traducción.

Los detalles de los procedimientos por los que se proporcione la habilidad para acceder y corregir información, puede diferir dependiendo de la naturaleza de la información y de otros intereses. Por esta razón, en ciertas circunstancias, puede ser imposible, impracticable o innecesario cambiar, suprimir o borrar registros.

Consistente con la naturaleza fundamental del acceso, las organizaciones siempre deberán hacer esfuerzos de buena voluntad para proporcionar el acceso. Por ejemplo, cuando cierta información necesite ser protegida y siempre pueda ser separada de otra información sujeta a una solicitud de acceso, la organización deberá redactar la información protegida y poner a disposición la otra información. Sin embargo, en ciertas situaciones podrá ser necesario que las organizaciones nieguen demandas de acceso y corrección, y este Principio expone las condiciones que deberán ser cumplidas para que tales negaciones sean consideradas como aceptables, las cuales incluyen: situaciones en las que las demandas constituyan un gasto o carga innecesaria para el controlador de la información personal, cuando las demandas de acceso sean repetitivas o irritantes por naturaleza; en casos en los que proporcionar la información constituya una violación a las leyes o cuando eso comprometa la seguridad; o, incidencias donde fuera necesario, para proteger información comercial confidencial que una organización haya protegido para no ser revelada, cuando revelarla beneficiaría a la competencia dentro del mercado, tal como un programa computacional o un programa modelador en particular.

"Información comercial confidencial" es información que una organización protege de ser revelada, cuando dicha revelación le facilitaría a un competidor dentro del mercado, el usar o explotar la información contra el interés empresarial de la organización, causando significativas pérdidas financieras. El programa computacional en particular o el proceso empresarial que une una organización, tal como un programa modelador o los detalles de ese programa o el proceso empresarial, pueden ser información comercial confidencial.

Cuando la información comercial confidencial siempre esté separada de otra información sujeta a una solicitud de acceso, la organización deberá redactar la información comercial confidencial y deberá hacer disponible la información no confidencial, al grado de que tal información constituya la información personal del individuo en cuestión. Las organizaciones pueden negar o limitar el acceso al grado de que no sea viable separar la información personal de la información comercial confidencial y cuando otorgar el acceso revele la propia información comercial confidencial de la organización tal como se definió arriba, o cuando revele la información comercial confidencial de otra organización que sea susceptible a una obligación de confidencialidad.

Cuando una organización niegue una solicitud de acceso por las razones especificadas arriba, tal organización deberá proporcionar al individuo una explicación del por qué tomó esa determinación e información de cómo desafiar esa negación. Una organización no tendrá que proporcionar una explicación, sin embargo, en casos en los que tal revelación viole una ley o una orden judicial.

PRINCIPIO IX. Responsabilidad

26. Un controlador de información personal deberá ser responsable de cumplir con medidas que causen efecto al Principio estipulado arriba. Cuando la información personal vaya a ser transferida a otra persona u organización, nacional o internacional, el controlador de la información personal deberá obtener consentimiento del individuo o actuar con la debida diligencia y tomar las medidas razonables para asegurar que la persona u organización receptora, protegerá la información consistentemente con estos Principios.

COMENTARIO (26) Modelos eficientes y rentables a menudo requieren transferencias de información entre distintos tipos de organizaciones en lugares distintos, con relaciones variadas. Al transferir información, los controladores de información personal deberán ser responsables de asegurar que el receptor protegerá la información consecuentemente con estos Principios, cuando no obtengan consentimiento. De este modo, los controladores de información deberán tomar las medidas razonables para asegurar que la información sea protegida, en conformidad con estos Principios, después de haber sido transferida. Sin embargo, hay ciertas situaciones en las que tal diligencia no sea práctica o sea imposible, por ejemplo, cuando no haya una relación en curso entre el controlador de información personal

y la persona a la que se le revela la información. En este tipo de circunstancias, los controladores de información personal pueden elegir utilizar otros medios, tales como obtener consentimiento para asegurar que la información sea protegida consecuentemente con estos Principios. Sin embargo, en casos en los que la revelación sea requerida por la ley nacional, el controlador de la información personal será eximido de cualquier diligencia u obligaciones de consentimiento.

## Parte iv. Implementación

27 La Parte IV proporciona orientación a las Economías Miembro sobre la implementación del Marco de Privacidad de APEC. La Sección A se enfoca en aquellas medidas que las Economías Miembro deben considerar para implementar el Marco dentro de su país, mientras que la Sección B expone las amplias disposiciones de APEC para la implementación de los elementos transfronterizos de Marco.

### A. ORIENTACIÓN PARA LA IMPLEMENTACION INTERNA

#### I. Maximizando Beneficios de Protección a la Privacidad y Flujos de Información

28. Las Economías deberán respetar el siguiente concepto básico al considerar la adopción de medidas diseñadas para la implementación interna del Marco de Privacidad de APEC:

29. Reconociendo el interés de la Economías para maximizar los beneficios económicos y sociales disponibles para sus ciudadanos y empresa, la información personal deberá ser recopilada, guardada, procesada, usada, transferida y revelada de tal manera que se proteja la privacidad de la información individual y que les permita darse cuenta de los beneficios de los flujos de información dentro y fuera de las fronteras.

30. Por consiguiente, como parte de establecer o revisar sus protecciones a la privacidad, las Economías Miembro, en concordancia con el Marco de Privacidad de APEC y con cualquier protección interna a la privacidad ya existente, deberán tomar todas las medidas razonables y apropiadas para identificar y remover barreas innecesarias a los flujos de información y evitar la creación de tales barreras.

II. Haciendo efectivo el Marco de Privacidad de APEC

31. Hay varias opciones para hacer efectivo el Marco de Privacidad y asegurar la protección de la privacidad de los individuos, incluyendo métodos legislativos, administrativos, autorreguladores de la industria, o la combinación de estos, sobre qué derechos pueden ser ejercitados bajo el Marco. Además, las Economías Miembro deben considerar tomar medidas para establecer punto(s) de acceso o mecanismos para proporcionar información, por lo general acerca de protecciones a la privacidad dentro de su jurisdicción. En la práctica, se supone que el Marco debe ser implementado, incluyendo a través de las autoridades centrales, cuerpos conformados por varias agencias de seguridad, una red de cuerpos industriales designados, o una combinación de los anteriores, tal como las Economías Miembro lo consideren apropiado.

32. Como se estableció en el Párrafo 31, los medios para hacer efectivo el Marco puede diferir entre las Economías Miembro, y puede ser apropiado para las Economías individuales, el determinar que diferentes Principios de Privacidad de APEC pueden requerir diferentes medios de implementación. Cualquier acercamiento que sea adoptado en una circunstancia en particular, la meta general deberá ser adoptar compatibilidad en los acercamientos en la protección a la privacidad en la región de APEC, que es respetuosa de los requerimientos de las Economías individuales.

33. Las Economías de APEC son estimuladas para adoptar prácticas no discriminatorias para proteger a los individuos de violaciones a la protección de la privacidad que ocurran en la jurisdicción de esa Economía Miembro.

34. Discusiones con agencias de seguridad internas, seguridad, salud pública y otras agencias son importantes para identificar maneras para fortalecer la privacidad sin crear obstáculos para la seguridad nacional, seguridad pública y otras misiones de políticas públicas.

III. Educando y divulgando protecciones internas a la privacidad

35. Para todas las Economías Miembro, en particular aquellas en las etapas iniciales del desarrollo de sus acercamientos internos a las protecciones a la privacidad, el Marco tiene la intención de proporcionar orientación para desarrollar sus acercamientos.

36. Para que el Marco tenga efectos prácticos, debe ser conocido y accesible. En consecuencia, las Economías Miembro deben:

a) divulgar las protecciones a la privacidad que proporcionen a los individuos;

b) educar a los controladores de información personal acerca de las protecciones a la privacidad de la Economía Miembro; y,

c) educar a los individuos acerca de cómo pueden reportar violaciones y cómo pueden buscarse remedios.

IV. Cooperación entre los Sectores Público y Privado

37. La participación activa de entidades no gubernamentales ayudará a asegurar que puedan realizarse todos los beneficios del Marco de Privacidad de APEC. En consecuencia, las Economías Miembro deben dialogar con grupos relevantes del sector privado, incluyendo grupos de privacidad y aquellos representando a consumidores y a la industria, para obtener aportes en asuntos de protección a la privacidad y cooperación para fomentar los objetivos del Marco. Además, en especial en las Economías en las que no se han establecido regímenes de protección a la privacidad en su jurisdicción interna, las Economías Miembro deben poner mucha atención al hecho de que las opiniones del sector privado sean reflejadas al desarrollar protecciones a la privacidad. En particular, las Economías Miembro deben buscar cooperación de entidades no gubernamentales en la educación pública y fomentar el envío de quejas a las agencias de seguridad de la privacidad, al igual que su continua cooperación en la investigación de esas quejas.

V. Proporcionando remedios apropiados in situaciones en las que sean violadas las protecciones a la privacidad

38. El sistema de protección a la privacidad de una Economía Miembro debe incluir una apropiada selección de remedios para las violaciones a la protección de la privacidad, tales como: reparación, la habilidad de detener una violación cuando esté en proceso, y otros remedios. Para determinar el rango de los remedios para las violaciones a la protección a la privacidad, un número de factores deben ser tomados en cuenta por una Economía Miembro, incluyendo:

d) El sistema particular en esa Economía Miembro para proporcionar protecciones a la privacidad (por ejemplo, poderes legislativos para hacer cumplir las leyes, que pueden incluir derechos de los

individuos para ejercer acción legal, autorregulación de la industria, o una combinación de sistemas); y

e) La importancia de tener un rango de remedios acorde con la extensión actual o potencial del daño a los individuos que resulte de tales violaciones.

VI. Mecanismo para Implementación de la Cobertura Interna del Marco de Privacidad de APEC

39. Las Economías Miembro deben dar a conocer a APEC, la implementación interna del Marco a través de la finalización de y actualizaciones periódicas del Plan de Acción Individual (IAP) sobre Privacidad de la Información.

B. ORIENTACIÓN PARA LA IMPLEMENTACIÓN INTERNACIONAL

Para tratar la implementación internacional del Marco de Privacidad de APEC y de acuerdo con las provisiones de la Parte A, las Economías Miembro deben considerar los siguientes puntos relacionados con la protección a la privacidad de la información personal:

I. Información compartida por las Economías Miembro

40. Las Economías Miembro son alentadas para compartir e intercambiar información, sondeos e investigación con respecto a cuestiones que tengan impacto significativo sobre la protección de la privacidad.

41. Para fomentar los objetivos de los párrafos 35 y 36, las Economías Miembro son alentadas a educarse unas a otras en asuntos relacionados con la protección de la privacidad y a compartir e intercambiar información sobre programas promocionales, educacionales y de entrenamiento, con el propósito de despertar la conciencia pública y mejorar el entendimiento de la importancia de la protección a la privacidad y la conformidad con leyes y normas relevantes.

42. Las Economías Miembro son alentadas a compartir experiencias sobre varias técnicas para investigar violaciones a protecciones a la privacidad y estrategias reguladoras para resolver disputas que involucren tales violaciones incluyendo, por ejemplo, manejo de quejas y mecanismos para la resolución alternativa de disputas.

43. Las Economías Miembro deben designar y dar a conocer a las otras Economías Miembro, las autoridades públicas dentro de sus jurisdicciones,

que serán responsables de facilitar la cooperación transfronteriza y de compartir información acerca de la protección a la privacidad entre las Economías.

II. Cooperación Transfronteriza en Investigación y Aplicación de la Ley

44. Desarrollar compromisos de colaboración: Tomando en consideración compromisos internacionales ya existentes y acercamientos autorreguladores en desarrollo o ya existentes (incluyendo aquellos a los que se hace alusión en la Parte B. III, abajo) y al alcance permitido por la ley y la política interna, las Economías Miembro deben considerar desarrollar compromisos de colaboración y procedimientos para facilitar la cooperación transfronteriza para hacer cumplir las leyes de privacidad. Dichos compromisos de colaboración pueden tomar la forma de compromisos bilaterales o multilaterales. Este párrafo puede ser interpretado pensando en el derecho de las Economías Miembro a declinar o limitar la cooperación sobre investigaciones particulares acerca de cuestiones por motivos de que la conformidad con la solicitud de cooperación fuera inconsistente con leyes internas, políticas o prioridades, o por motivos de restricciones de recursos o basado en la ausencia de interés mutuo en la investigación en cuestión.

45. En el cumplimiento de leyes civiles de privacidad, los compromisos de colaboración transfronteriza puede incluir los siguientes aspectos:

f) mecanismos para notificar puntual, eficiente y sistemáticamente a las autoridades públicas designadas en otras Economías Miembro, de la investigación o de casos de privacidad en los que deba hacerse cumplir la ley, que sean objeto de conductas ilícitas o que provoquen daños a individuos de esas Economías;

g) mecanismos para compartir información necesaria de manera eficiente, para la exitosa cooperación en investigaciones de privacidad transfroterizas y en casos en los que debe hacerse cumplir la ley;

h) mecanismos para investigar asistencia en casos de privacidad en los que deba hacerse cumplir la ley;

i) mecanismos para dar prioridad a casos para cooperación con autoridades públicas en otras Economías, basada en la severidad de las violaciones a la privacidad de la información personal, el daño actual o potencial involucrado, así como otras consideraciones relevantes;

j) pasos para mantener el nivel apropiado de confidencialidad con respecto a la información intercambiada bajo compromisos de colaboración.

### III. Colaboración en el Desarrollo de Reglas de Privacidad Transfronterizas

46. Las Economías Miembro se esforzarán para apoyar el desarrollo y reconocimiento o aceptación de reglas de privacidad transfronterizas en la región de APEC, reconociendo que las organizaciones seguirán siendo responsables de cumplir con los requerimientos locales de protección de datos, así como con todas las leyes aplicables. Tales reglas de privacidad transfronterizas deben adherirse a los Principios de Privacidad de APEC.

47. Para hacer efectivas las reglas de privacidad transfronterizas, las Economías Miembro se esforzarán para trabajar con depositarios apropiados para desarrollar marcos o mecanismos para el mutuo reconocimiento o aceptación de dichas reglas de privacidad transfronterizas entre las Economías.

48. Las Economías Miembro deberán esforzarse para asegurar que dichas reglas de privacidad transfronterizas y el reconocimiento o aceptación de mecanismos, faciliten transferencias transfronterizas responsables de datos y protecciones efectivas a la privacidad sin crear barreras innecesarias a los flujos transfronterizos de información, incluyendo cargas administrativas y burocráticas innecesarias para las empresas y los consumidores.

Publicado por Secretariado de APEC,
Terraza Heng Mui Keng 35, Singapur 119616
Tel: (65) 6775 6012 Fax: (65)6775 6013
Correo electrónico: info@apec.org
Página en Internet: www.apec.org

ISBN 981-05-4471-5
APEC#205-SO-012 2005
Secretariado de APEC