GTAG

GUÍA DE AUDITORÍA DE TECNOLOGÍA GLOBAL

Gestión y auditoría de riesgos de privacidad

The Institute of Internal Auditors

Guía de Auditoría de Tecnología Global (GTAG) 5:

Gestión y auditoría de riesgos de privacidad

Autores

Ulrich Hann, Ph.D.; Suiza/Alemania

Ken Askelson, JCPenney, EE. UU.

Robert Stiles, Texas Guaranteed (TG), EE. UU.

Junio 2006

¿Por qué es importante la privacidad?

Uno de los problemas, de mayor desafío y más significativos, de la gestión de riesgos que las organizaciones deben enfrentar actualmente es la protección de la privacidad de la información personal de los clientes y empleados. Como consumidores, nos preocupa de qué manera los comercios y las organizaciones utilizan y protegen esa información. Al mismo tiempo, como propietarios o miembros de la dirección del negocio, deseamos satisfacer las necesidades y expectativas de nuestros clientes y empleados, respetar las promesas realizadas en cuanto a políticas y avisos de privacidad, y cumplir con las leyes y regulaciones de seguridad y privacidad de datos aplicables al caso específico. Los clientes, proveedores y socios de negocio de la organización desean tener la seguridad de que la información personal recogida por la organización está protegida y se utiliza solamente para los propósitos según los cuales se recogió originalmente. Cuando la privacidad se gestiona adecuadamente, las organizaciones ganan la confianza de sus clientes, empleados y demás sujetos de datos. Cuando esa gestión es deficiente, la confianza se erosiona rápidamente.

> "La información personal se ha convertido, para sus custodios, tanto en un activo importante como en una responsabilidad".
>
> *– Dr. Ann Cavoukian, Comisario de Información y Privacidad de Ontario, Canadá*

La privacidad es una cuestión global. Muchos países han adoptado legislación de privacidad en todo su territorio para regir el uso de la información personal, así como también la exportación de ella a través de las fronteras. Para que los negocios funcionen eficazmente en este entorno, se debe comprender y cumplir con esas leyes de privacidad. Algunos ejemplos de legislación de privacidad relevante son: la Ley de Protección de Documentos Electrónicos e Información Personal (PIPEDA, en inglés) de Canadá, la Directiva de Privacidad de Datos de la Unión Europea y las leyes de privacidad de Australia, Japón y Nueva Zelanda. Entre la legislación de privacidad reciente de los sectores económicos, se incluyen la Ley Gramm-Leach Bliley (GLBA, en inglés) para el sector financiero y la Ley de Responsabilidad y Portabilidad del Seguro de Salud (HIPAA, en inglés) correspondiente al sector de servicios de salud.

Los títulos de diversos artículos han demostrado que la privacidad y la protección de la información personal no son temas definitivamente resueltos. Hay numerosas historias de primera plana referentes a violaciones de seguridad que implican la pérdida o la divulgación de información personal. Y más importante aún, los consejos de administración y los comités de auditoría desean contar con el aseguramiento de los procesos de la organización que protegen la información privada.

Beneficios de los controles de privacidad eficaces

El buen gobierno implica poder identificar los riesgos significativos para la organización, como por ejemplo, potenciales usos indebidos, fugas o pérdidas de información personal, y a la vez poder asegurar que la organización tiene controles apropiados implementados para mitigar esos riesgos.

En el sector de los negocios, los beneficios de los buenos controles de privacidad son los siguientes:

- Proteger la imagen pública y la marca de la organización.
- Proteger datos valiosos de los clientes y empleados de la organización.
- Lograr una ventaja competitiva en el mercado.
- Cumplir con las leyes y regulaciones de privacidad aplicables.
- Mejorar la credibilidad y promocionar la confianza y reputación comercial.

En el sector público y las organizaciones sin fines de lucro, los beneficios de los buenos controles de privacidad son los siguientes:

- Mantener la confianza de los ciudadanos y de los extranjeros.
- Sostener las relaciones con los donantes de las organizaciones sin fines de lucro respetando la privacidad de sus actividades.

Sostener prácticas de privacidad eficaces

La mayoría de las organizaciones reconocen la necesidad de implementar buenas prácticas de privacidad. No obstante, el desafío es sostenerlas. La proliferación de la tecnología, que permite la recolección, el uso, la divulgación, la retención y la destrucción de la información personal en grandes volúmenes, junto a la existencia de numerosas bases de datos hacen que las organizaciones tengan dificultades para identificar dónde se almacena ese cúmulo de datos, de qué manera se protege, quién tiene acceso y cómo se desecha de manera segura. Además, las responsabilidades de rendir cuentas y de mantener un programa de privacidad no siempre están claramente asignadas y, con frecuencia, se encuentran distribuidas por toda la organización. Esto puede provocar inconsistencias y falta de certeza a la hora de asegurar que se cuenta con buenas prácticas de privacidad implementadas y que estas están funcionando eficazmente.

Para implementar y gestionar un programa de privacidad efectivo, la organización debe definir claramente sus políticas de privacidad, comunicarlas y documentar los procedimientos y controles relativos a la recolección, el uso, la retención y la divulgación de información personal para garantizar el cumplimiento con las leyes, regulaciones y políticas de la organización. Se deben establecer criterios específicos que sean relevantes, objetivos, completos y medibles para evaluar la eficacia de tales elementos. Al establecer esos criterios, se proporciona un enfoque coherente para proteger la información personal de una manera que los individuos puedan comprender con facilidad y que la organización pueda implementar y evaluar con celeridad. Existen enfoques establecidos como las Guías de Privacidad de la Organización para la Cooperación y el Desarrollo Económico (OECD, en inglés), así como legislación reciente y guías profesionales que proporcionan criterios sólidos y probados con los que se pueden establecer puntos de referencia.

El rol del auditor interno en la protección de la privacidad

La privacidad y la protección de la información personal proporcionan una plataforma urgente para que los auditores sean participantes activos en ayudar a su organización a abordar inquietudes y riesgos de privacidad. Un rol clave de los auditores internos es proporcionar una evaluación independiente de los controles de privacidad de la organización. La *Figura 1.1: Beneficios de la auditoría de privacidad* describe algunos de los beneficios de llevar a cabo una auditoría de privacidad.

Figura 1.1: Beneficios de la auditoría de privacidad

- Facilita el cumplimiento de la ley.
- Mide y ayuda a mejorar el cumplimiento con el sistema de protección de datos de la organización.
- Aumenta el nivel de conciencia, en la dirección y el personal, sobre protección de datos.
- Proporciona información para una revisión del sistema de protección de datos.
- Mejora la satisfacción del cliente al reducir la posibilidad de errores que luego dan lugar a un reclamo.

El auditor interno, al desempeñar su rol y ayudar a la organización a cumplir con los objetivos de privacidad, puede contribuir a garantizar el buen gobierno y la responsabilidad de esta. Además, está posicionado como para evaluar el enfoque de privacidad de la organización e identificar los riesgos significativos, a la vez que emite recomendaciones apropiadas para mitigarlos.

Alcance de la GTAG 5

Esta Guía de Auditoría de Tecnología Global (GTAG, en inglés) tiene como propósito suministrar al director ejecutivo de auditoría (DEA), a los auditores internos y a la dirección, cierta comprensión con respecto a los riesgos de privacidad que la organización debe abordar cuando recoge, utiliza, retiene o divulga información personal. Esta guía proporciona una descripción general de enfoques de privacidad clave para ayudar a los lectores a comprender los conceptos básicos y a identificar los recursos correctos para obtener más orientación en cuanto a expectativas y a qué es lo que funciona bien en los distintos entornos. Además, aborda la manera en que los auditores internos deben realizar las evaluaciones de privacidad.

2.1 ¿Qué es la privacidad?

La privacidad puede tomar varios significados y con frecuencia se analiza en diversos contextos (vea la *Figura 2.1: Esferas de privacidad*). En la mayoría de las sociedades, desde hace largo tiempo, la privacidad ha sido considerada un derecho humano básico. Puede ser vista como elemento descriptivo o prescriptivo, como un interés moral o como un derecho legal. Implica el derecho a vivir sin la atención no deseada de los otros sobre nosotros, o el derecho a vivir sin ser observados ni supervisados. O puede significar el derecho a vivir sin intrusiones ni en estado de reclusión. Además, cubre la privacidad de las comunicaciones y de la información. En su forma más simple, la privacidad ha sido definida como "el derecho del individuo a ser dejado en paz" (Warren/Brandeis, 1890).

Figura 2.1: Esferas de privacidad

- Privacidad personal: privacidad física y sicológica.
- Privacidad del espacio: derecho a vivir sin sufrir vigilancia.
- Privacidad de la comunicación: derecho a no sufrir supervisiones ni intercepciones.
- Privacidad de la información: control por parte de otros sobre la recolección, el uso y la divulgación de la información personal.

— Fuente: Instituto Canadiense de Contadores Certificados (CICA, en inglés), 2002

Las definiciones de privacidad en el entorno de negocio varían ampliamente según el país, la cultura, el entorno político y al marco legal. En muchos países, la privacidad está estrechamente vinculada con la protección de datos. Es de especial importancia para las organizaciones cómo se define la privacidad en su contexto específico. Ya sea que se utilice una de las definiciones de la *Figura 2.2: Definiciones de privacidad*, o que simplemente se defina la privacidad como la protección de la recolección, el almacenamiento, el procesamiento, la difusión y la destrucción de información personal; las diversas definiciones de privacidad son complementarias y cualquier organización las puede utilizar como guía para su programa de privacidad.

Figura 2.2: Definiciones de privacidad

"La privacidad es la protección de los datos personales y se considera un derecho humano fundamental".

— Pautas de la OECD, 1980

"Los estados miembro deben proteger los derechos fundamentales y la libertad de las personas naturales, y en particular, su derecho a la privacidad con respecto al procesamiento de datos personales".

— Directiva de la UE, 1995

"Los derechos y las obligaciones de las personas y las organizaciones en cuanto a recolección, uso, retención y divulgación de la información personal".

— Instituto Estadounidense de Contadores Públicos Certificados (AICPA, en inglés)/CICA, 2005

En el contexto de negocio actual, la privacidad con frecuencia se refiere a la privacidad de la información personal de un individuo y a su capacidad para:

- Saber cómo se maneja su información personal.
- Controlar la información recogida.
- Controlar para qué se utiliza la información.
- Controlar quién tiene acceso a la información.
- Enmendar, cambiar y eliminar la información.

La privacidad de la información, en la que se combina la privacidad de las comunicaciones y los datos, generalmente se puede describir mediante los derechos y las obligaciones de las personas y las organizaciones en cuanto a recolección, uso, retención y divulgación de la información personal de un individuo identificable, información que abarca cualquier dato fáctico o subjetivo, registrado o no, en alguna forma. En otras palabras, la privacidad de la información se mantiene asegurando un tratamiento y una protección adecuada de la información personal.

Información personal

La información personal son datos que se pueden vincular o utilizar para identificar a un individuo, directa o indirectamente. Algunos ejemplos de información personal:

- Nombre.
- Domicilio o dirección de correo electrónico.
- Identificadores, como por ejemplo, número de seguridad social, de seguro social, de pasaporte o de cuentas.
- Características físicas.
- Registros de crédito.
- Historia de compras del consumidor.
- Archivos de empleado.

Información confidencial

Determinada información personal se considera información confidencial. Ejemplos de información personal confidencial:

- Registros médicos..
- Información financiera.
- Origen racial o étnico.
- Opiniones políticas.
- Creencias religiosas o filosóficas.
- Afiliación a una organización sindical.
- Información relativa a delitos o condenas de tipo penal.

Determinada información, aunque no sea personal en sí misma, al combinarla con otra, se convierte en personal y confidencial. La información personal confidencial generalmente requiere un nivel extra de protección y debido cuidado. Implementar una metodología de clasificación de datos que incluya información personal es una manera eficaz, por parte de la organización, de abordar el nivel adecuado de protección y debido cuidado. De esa forma, se proporciona una orientación para garantizar que se implementen prácticas coherentes en toda la organización según la naturaleza de los datos.

Información y anonimato

La información anónima acerca de las personas no debe poder ser asociada con individuos específicos. Ese tipo de información se denomina *información no personal*. Este concepto incluye información personal estadística o resumida en la que no se conoce la identidad de la persona, o bien, se ha eliminado su vínculo con la persona a la que pertenece. Cuando la identidad del individuo no se puede determinar a partir de la información remanente, se considera que se la ha "desidentificado" o "pasado al anonimato".

Protección de la privacidad

La protección de la privacidad se puede considerar como el proceso de establecer un equilibrio apropiado entre la privacidad y los diversos intereses contrapuestos. Para minimizar el grado de intrusión, maximizar la imparcialidad y generar expectativas legítimas aplicables en cuanto a privacidad, durante las décadas pasadas, se produjo la evolución de un conjunto de principios que rigen sobre el procesamiento de la información personal del individuo, junto con un modelo de los roles involucrados en el concepto de privacidad (vea la *Figura 2.3: Roles de la privacidad*). Los principios incluyen una mezcla de conceptos sustantivos, como por ejemplo, calidad de los datos, integridad y limitación de su uso; hasta principios procedimentales como los conceptos de consentimiento y derechos de acceso.

Figura 2.3: Roles de la privacidad

Cuando se implementa un programa de privacidad, se deben tener en cuenta los siguientes roles principales:

- **Sujetos de datos:** personas cuyos datos personales son los que se controlan.
- **Controlador de datos:** organización o entidad que controla los datos personales.
- **Director de privacidad:** función de contacto y supervisión de la privacidad de una organización.
- **Comisario de privacidad:** autoridad de supervisión gubernamental, generalmente a nivel federal o del estado.
- **Prestadores de servicios:** se hacen presentes en aquellas circunstancias en las que participan empresas externas en el procesamiento de datos.

La forma en que una organización gestiona la información personal de clientes y empleados; la manera en que la recoge, utiliza, distribuye, almacena y protege; es el centro del tema de la privacidad en los negocios. Algunos incidentes recientes de robo de identidad, mal manejo de la información personal y violación de los principios de privacidad han incrementado la presión de las regulaciones y de los consumidores sobre las organizaciones para que desarrollen los controles apropiados en relación con la privacidad, la gestión de datos y la seguridad de la información. Las organizaciones que no abordan los problemas de privacidad adecuadamente corren el riesgo de sufrir daños a largo plazo en su marca y reputación, pérdida de la confianza del consumidor y del empleado, además de padecer multas, acciones ejecutorias y procesos penales.

Los controles adecuados minimizan o evitan los riesgos de todas las partes involucradas. La auditoría interna juega un rol importante en identificar los riesgos, evaluar los controles y mejorar las prácticas de la organización respecto de la privacidad de los empleados, clientes y ciudadanos.

2.2 Gestión de riesgos de privacidad

La privacidad es un tema de gestión de riesgos para los comercios y las organizaciones sin fines de lucro. Las encuestas siguen mostrando que los consumidores sienten preocupación sobre cómo los comercios utilizan su información personal. La imposibilidad de la gestión de abordar la protección de la información personal correctamente presenta una serie de riesgos para la organización. Estos son:

- Posibles daños a la imagen pública y marca de la organización.
- Potenciales pérdidas financieras o de inversores.
- Responsabilidad legal, sanciones reglamentarias o de la industria.
- Cargos por prácticas engañosas.
- Falta de confianza por parte de clientes, ciudadanos y empleados.
- Pérdida de clientes o ingresos.
- Daño de las relaciones comerciales.

Controles de privacidad

Un control esencial para abordar los riesgos de privacidad que debe enfrentar la organización es que los directores y la dirección proporcionen un gobierno y supervisión adecuados (es decir, la imagen de la gerencia). El DEA, junto con el comité de auditoría, debe alentar a la dirección ejecutiva para que aborde el tema de cómo la organización gestiona, controla y protege la información personal que recoge sobre clientes y empleados. Además, la organización debe evaluar el grado de cumplimiento en relación a la privacidad, las prácticas de manejo de datos y las debilidades al respecto, y compararlas con las políticas internas, leyes y regulaciones, y mejores prácticas.

Es esencial que la organización implemente un programa de privacidad eficaz que incluya:

- La responsabilidad y el gobierno respecto al tema de la privacidad.
- Una declaración de privacidad.
- Políticas y procedimientos escritos.
- Controles y procesos.
- Roles y responsabilidades.
- Capacitación y formación de los empleados.
- Supervisión y auditoría.
- Prácticas de seguridad de la información.
- Plan de respuesta ante incidentes.
- Leyes y regulaciones de privacidad.
- Planes de respuesta ante problemas detectados y acciones correctivas.

El auditor interno, al desempeñar su rol y ayudar a la organización a cumplir con sus objetivos de privacidad, puede contribuir a garantizar el buen gobierno y responsabilidad de esta. Las actividades específicas que los auditores internos pueden desempeñar en esta área son las siguientes:

- Trabajar con el asesor legal para determinar cuáles son las regulaciones y la legislación de privacidad aplicables a la organización.
- Trabajar con la gestión de tecnología de la información y los propietarios del proceso de negocio para evaluar si se han implementado controles de seguridad de la información y de protección de datos, y si se revisan regularmente.
- Llevar a cabo evaluaciones de riesgos de privacidad, o revisar la eficacia de las políticas de privacidad, sus prácticas y controles en toda la organización.
- Identificar los tipos de información personal recogida, la metodología de recolección utilizada y determinar si el uso de la información por parte de la organización coincide con el uso pretendido.
- Revisar las políticas, los procedimientos y las pautas que rigen sobre los flujos de datos y los procedimientos

de manejo de datos diseñados para salvaguardar la privacidad de la información personal centrando la atención en identificar las posibles oportunidades de estandarizar las prácticas de protección de datos en la organización.
- Efectuar una evaluación de las interacciones de los prestadores de servicios, como por ejemplo, la revisión de los procedimientos y controles sobre los prestadores que manejan, en nombre de la organización, información personal identificable o datos confidenciales.
- Revisar las prácticas y materiales de capacitación en curso, y realizar el inventario de los materiales disponibles y necesarios para la capacitación y conciencia de privacidad.
- Realizar un análisis de las posibles brechas en los flujos y procedimientos de manejo de datos comparándolos con políticas relevantes, leyes, regulaciones y mejores prácticas para determinar coherencia y cumplimiento. Este análisis cubre las evaluaciones de procesos manuales y automatizados para manejar la información personal que identifica a los individuos.

Riesgos y acciones de privacidad clave

Los auditores internos están posicionados como para evaluar el enfoque de privacidad de su organización e identificar los riesgos significativos, y a la vez emitir las recomendaciones apropiadas para mitigarlos. En la *Figura 2.4: Matriz de riesgos y acciones de privacidad*, se encuentran ejemplos de riesgos de privacidad clave que los auditores internos deben abordar en su tarea.

Figura 2.4: Matriz de riesgos y acciones de privacidad

Riesgos de privacidad	Acciones
La organización no tiene una política de privacidad ni elementos de enfoque de control al respecto.	Converse con la alta dirección sobre la necesidad de elaborar una política de privacidad documentada y sobre el desarrollo de un programa de privacidad eficaz.
La organización no está cumpliendo con su política de privacidad.	Realice una revisión de las prácticas de privacidad de la organización para asegurarse de que esta respeta los compromisos asumidos con los clientes en sus avisos de privacidad.
La organización no protege adecuadamente la información personal que recoge, utiliza, retiene y divulga.	Realice una revisión de las prácticas de seguridad de la información de la organización en cuanto a controles administrativos, físicos y técnicos para asegurar que la información personal está protegida adecuadamente.
La organización no ha identificado los tipos de información personal que recoge, quién tiene acceso a ella o dónde se la almacena.	Realice un mapa de los flujos de datos de la información personal recogida, quién tiene acceso a ella y cuál es la necesidad de negocio para tal acceso.
La organización no tiene una estructura de gobierno formal relacionada con el cumplimiento de privacidad.	Analice con la alta dirección o con el comité de auditoría, de ser necesario, la necesidad de una estructura de gobierno para el cumplimiento de privacidad.
La organización no tiene políticas internas que fortalezcan la protección de la información personal.	Revise las políticas vigentes, las normas y los procedimientos relativos a la privacidad de la información personal para asegurarse de que la organización aborda áreas tales como clasificación, gestión de registros, retención y destrucción de datos.
La organización no ha establecido una auditoría de cumplimiento o un enfoque de supervisión.	Incluya el cumplimiento de privacidad en el inventario auditable basado en el riesgo. Solicite al departamento legal que le suministre un inventario de las leyes y regulaciones que se aplican a la organización. Realice una auditoría de cumplimiento de privacidad.
La organización no tiene implementado un plan de respuesta ante incidentes.	Analice con la alta dirección, incluidos los departamentos legales y de tecnología de la información, la necesidad de desarrollar un plan de respuesta ante incidentes para el caso que ocurra una violación de información personal.
La organización no ha realizado una capacitación formal sobre conciencia de privacidad, manejo de datos o seguridad de la información.	Revise la capacitación de privacidad y el material de concientización para verificar si cumple con las necesidades de la organización. Revise los registros de capacitación para asegurarse de que los empleados que manejan o tienen acceso a la información personal han realizado la capacitación requerida.
La organización no ha implementado un programa de gestión de privacidad y seguridad de proveedores independientes como para crear un enfoque de aplicación coherente para contratar, evaluar y supervisar las prácticas de privacidad de sus prestadores.	Revise los contratos de los proveedores independientes para asegurarse de que contienen elementos clave, tales como, requerimientos de protección de la información personal, cláusulas de extinción del contrato, destrucción de registros que contienen información personal y cláusula de derecho a auditar. Realice las auditorías periódicas para garantizar que los proveedores independientes están cumpliendo con los términos del contrato.

El deseo de privacidad proviene de necesidades divergentes y depende del tiempo, el lugar, la situación y el interés de la persona o de una organización. Indudablemente con la propagación de las redes de procesamiento de datos computarizados y de comunicación global, tuvo lugar un cambio de paradigma: los ciudadanos y los consumidores se volvieron totalmente transparentes y esto generó oportunidades apasionantes y experiencias sorprendentes, pero también significó una amenaza para los cimientos de la sociedad y los negocios.

Las organizaciones de hoy en día tienen la ventaja de contar con varias décadas de experiencia en conceptos de privacidad en un mundo computarizado y conectado por redes. Los auditores internos juegan un rol en cuanto a asegurar que hay controles adecuados implementados y que estos funcionan de manera confiable, pero también deben asegurar que las organizaciones utilizan la información de manera eficiente y eficaz para lograr sus objetivos.

Se han desarrollado numerosos enfoques al respecto. Algunos son de cumplimiento obligatorio y otros proporcionan pautas discrecionales para el procesamiento de la información personal. Esta sección analizará los enfoques principales disponibles.

3.1 Principios de privacidad

El foco de los principios de privacidad varía entre los regímenes transnacionales que tienen una perspectiva más centrada en los derechos humanos, tal como lo presenta la Organización de Naciones Unidas (ONU) y el Consejo de Europa (CE), o una lógica más orientada hacia el libre comercio, como la de la Organización para la Cooperación y el Desarrollo Económico (OECD, en inglés) y el Foro de Cooperación Económica Asia-Pacífico (APEC, en inglés). Las leyes nacionales de tipo "ómnibus" usualmente apuntan a balancear las relaciones del gobierno y los ciudadanos, así como las de los negocios y los consumidores.

Los problemas de privacidad se hicieron visibles con el advenimiento de la informatización. La Asamblea General de la ONU asumió la existencia del tema en 1968 cuando encomendó la investigación del asunto para comprender las amenazas a la privacidad y emitir posibles contramedidas. A continuación de esa toma de conciencia global, se implementaron en Suecia, en 1973, las primeras leyes federales amplias sobre privacidad. Al año siguiente, Alemania siguió tal ejemplo y Francia estableció sus leyes de privacidad en 1978.

En 1980, los estados miembros de la OECD llegaron a un acuerdo sobre prácticas honestas de información e impusieron restricciones respecto de la recolección, uso y divulgación de la información personal. Estas prácticas son:

- Limitar la recolección y el uso de la información personal para los propósitos expresados.
- Asegurar la calidad y precisión de los datos.
- Establecer los resguardos de seguridad.
- Apertura y transparencia en las prácticas y las políticas referidas a datos personales.
- Permitir que las personas tengan acceso a sus datos personales y cuenten con la capacidad de poder corregirlos.
- Identificar personas que sean responsables por la

Figura 3.1: Principios de PIPEDA

1. **Responsabilidad**: Una organización es responsable de la información personal que está bajo su control y debe designar a una o varias personas que sean las responsables del cumplimiento por parte de la organización de los siguientes principios.
2. **Identificación del propósito**: El propósito por el cual se recoge la información personal debe ser identificado por la organización en el momento de recoger dicha información o antes de ello.
3. **Consentimiento**: Se requiere el conocimiento y consentimiento de la persona en cuestión, para recolectar, utilizar y divulgar su información personal, excepto cuando sea inapropiado.
4. **Limitación a la recolección**: La recolección de información personal deberá limitarse a aquella que sea necesaria para el propósito identificado por la organización. La información debe recogerse utilizando medios legales y justos.
5. **Limitación al uso, divulgación y retención**: La información personal no debe ser utilizada ni divulgada para ningún otro propósito distinto del que se estableció para su recolección, excepto que se obtenga el consentimiento de la persona o se lo requiera por ley. La información personal sólo debe ser retenida por el tiempo que sea necesario para satisfacer tales propósitos.
6. **Precisión**: La información personal debe ser tan precisa, completa y actualizada como sea necesario según los propósitos para los que se la utiliza.
7. **Resguardos**: La información personal debe estar protegida mediante resguardos de seguridad que sean apropiados para el grado de confidencialidad de la información.
8. **Apertura**: Una organización debe poner prestamente a disposición de las personas toda la información respecto de sus políticas y prácticas referidas a la gestión de la información personal.
9. **Acceso individual**: A pedido específico, se debe informar a la persona sobre la existencia, uso y divulgación de su información personal y se le debe otorgar acceso a esa información. Una persona debe poder cuestionar la precisión e integridad de la información y poder enmendarla según sea apropiado.
10. **Cuestionamiento al cumplimiento**: La persona debe poder presentar su cuestionamiento al cumplimiento de los principios anteriores ante la o las personas responsables del cumplimiento de la organización.

adhesión a estos principios.

Los principios de privacidad de la OECD se refieren a lo siguiente: Limitación a la recolección de información, Calidad de los datos, Especificación del propósito, Limitación de uso, Resguardos de seguridad, Apertura, Participación individual y Responsabilidad.

El Código Modelo de la Asociación Canadiense de Normas de 1996 para la Protección de la Información Personal, ahora incorporado a la Ley de Protección de Información Personal y Documentos Electrónicos (PIPEDA, en inglés), proporciona una consolidación amplia de los principios de privacidad (consulte la *Figura 3.1: Principios de PIPEDA* de la página anterior).

Los principios de la Ley de Protección de Datos de 1984/1998 del Reino Unido, de manera similar, establece que los datos personales deben cumplir las siguientes pautas:

- Que sean procesados de manera justa y legal.
- Que sean procesados para propósitos limitados.
- Que sean adecuados, relevantes y no excesivos.
- Que sean precisos.
- Que no se los conserve por más tiempo del necesario.
- Que sean procesados conforme a los derechos de los sujetos de datos.
- Que sean seguros.
- Que no sean transferidos a otras jurisdicciones sin la protección adecuada.

Esos principios de privacidad se consideran esenciales para la protección y gestión apropiadas de la información personal. Proporcionan pautas a los auditores internos que tienen a su cargo la tarea de revisar las prácticas de privacidad.

3.2 Enfoques de privacidad

Desde 1968, cuando la ONU reconoció que la privacidad electrónica se convertiría en un problema global, surgió una amplia variedad de enfoques. Desde un punto de vista legal y técnico, estos varían entre enfoques obligatorios y de aplicación voluntaria a regímenes. Algunos son aplicables globalmente y otros son normas individuales. Además, las personas y las organizaciones pueden aplicar su simple sentido común, seguir la legislación o pronunciarse sobre cómo planean responder a las potenciales cuestiones de la privacidad, por grupo o mediante declaraciones individuales (vea la *Figura 3.2: Normas de privacidad*).

Figura 3.2: Normas de privacidad

Tipología	Alcance
• Sentido común, ética	• Global.
• Constitucional.	• Regional.
• Legislativa.	• Nacional tipo "ómnibus".
• Reglas y regulaciones.	• Sector, industria.
• Leyes blandas, autoregulaciones.	• Individual.
• Sellos, certificados.	• Enfoques: en todos los niveles.
• Aplicación de los enfoques.	
• Compromiso de realización.	

¿Cuáles son las implicancias para la auditoría interna y la dirección de las organizaciones auditadas? Los auditores, cuando proporciona aseguramiento sobre controles y riesgos de privacidad, deben conocer y comprender los enfoques aplicables, además de determinar si la organización está sujeta a algún enfoque específico, o se espera que adhiera a uno. Las secciones restantes de este capítulo proporcionan una descripción general de los enfoques clave que delinean los conceptos básicos de privacidad, así como la información sobre los recursos apropiados para ofrecer más orientación, más detalles respecto de las expectativas e indicar qué es lo que funciona bien en una amplia variedad de lugares y situaciones.

Marcos transnacionales no vinculantes

Los marcos transnacionales no vinculantes inicialmente fueron establecidos para garantizar el libre flujo de información entre los países afiliados a la organización. En 1980, fue creada la Guía de Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales por Consejo de la OECD con el fin de establecer puntos de acuerdo para el libre flujo transfronterizo de datos entre los 24 miembros de la OECD. Aunque no fue legalmente vinculante, el conjunto de principios, neutro en cuanto a tecnología y ampliamente aplicable, se aceptó en todas partes con el transcurso del tiempo. Los comités de la OECD regularmente emiten informes de investigación en el área de protección de datos y privacidad.

En 1990, 10 años después de que se publicó la Guía de la OECD, la Asamblea General de la ONU emitió su Guía para Archivos de Datos Personales Computarizados, basada en los derechos humanos. Los estados miembro deben tener en cuenta estas pautas al implementar su legislación nacional de protección de datos. Las pautas recomiendan que los estados miembro proporcionen garantías básicas respecto de la privacidad de la información de sus ciudadanos y un conjunto de resguardos mínimos para el procesamiento de datos personales equiparables a los principios de la OECD. También exigen que haya autoridades de supervisión y abordan el tema del procesamiento de datos personales por parte de instituciones internacionales.

En 2004, se desarrolló el Enfoque de Privacidad del APEC y este es coherente con los valores principales de las pautas de la OECD. Esta destinado a proporcionar orientación y dirección, para los negocios de las economías del APEC, sobre los problemas de privacidad comunes y determinar el impacto que estos tienen en la manera de hacer negocios.

Marcos transnacionales legalmente vinculantes

Algunos regímenes regionales, particularmente la Convención 108 del Consejo de Europa y la Directiva 95/46/CE de la Unión Europea (UE), son instrumentos legalmente vinculantes. La Convención 108 para la protección de las personas respecto del procesamiento automático de datos personales, publicada el 28 de enero de 1981, obliga legalmente a los 30 signatarios a implementar los principios de privacidad de la convención en sus leyes nacionales. De esta forma, en el caso de que los derechos de las personas no estén suficientemente protegidos a nivel nacional, pueden apelar a un tribunal del Consejo de Europa. Los principios de privacidad de la convención son equiparables a las pautas de la OECD de 1980, con algunos resguardos adi-

cionales que se requieren para los datos confidenciales.

La Directiva 95/46/CE de la UE sobre la protección de las personas respecto del procesamiento automático de datos y el libre movimiento de tales datos, publicada el 24 de octubre de 1995, apunta a homogeneizar los regímenes nacionales de los estados miembro de la UE para simplificar las transferencias de datos y fortalecer los derechos de los individuos. Contiene principios de privacidad más amplios y detallados que las pautas de la OECD, así como disposiciones adicionales sobre datos confidenciales, divulgación, registro y derechos a no participar y de reparación. Otorga, a los cuerpos de supervisión independiente, la autoridad de investigación, los poderes de intervención y la capacidad de involucrarse en actuaciones legales. Una directiva posterior regula el procesamiento de los datos personales en las telecomunicaciones.

Legislación nacional

La legislación nacional se presenta en forma de leyes de tipo "ómnibus" y de regulaciones del sector. Estas leyes tipo "ómnibus" generalmente son leyes del sector público o privado, que operan como resguardo de los ciudadanos contra la acción invasiva del gobierno y tienden a ser más sólidas que las intervenciones legalistas con el fin de balancear el interés privado. Esta GTAG no abarca una revisión detallada de la legislación nacional., Sin embargo, en los sitios Web de diversos comisionados del tema privacidad y de las "iniciativas de privacidad global" se pueden encontrar descripciones generales y vínculos al respecto (consulte las páginas 26 a 28 del Apéndice).

El trabajo de parches de las leyes nacionales (vea la *Figura 3.3: Leyes de protección de datos*) tiene significativas implicancias para los auditores internos. Ellos deben comprender qué leyes son aplicables y deben poder comparar las prácticas existentes con todos los marcos legales que, en efecto, se aplican o aquellos que podrían aplicarse. En muchos casos, por ejemplo, cuando se prestan servicios a través de Internet, no será posible la limitación a un enfoque específico. En esas situaciones, los auditores internos deben consultar al asesor legal interno a fin de lograr la comprensión orientada a los controles de las prácticas generales, los enfoques, las expectativas para evaluar las prácticas y poder asesorar a la dirección adecuadamente.

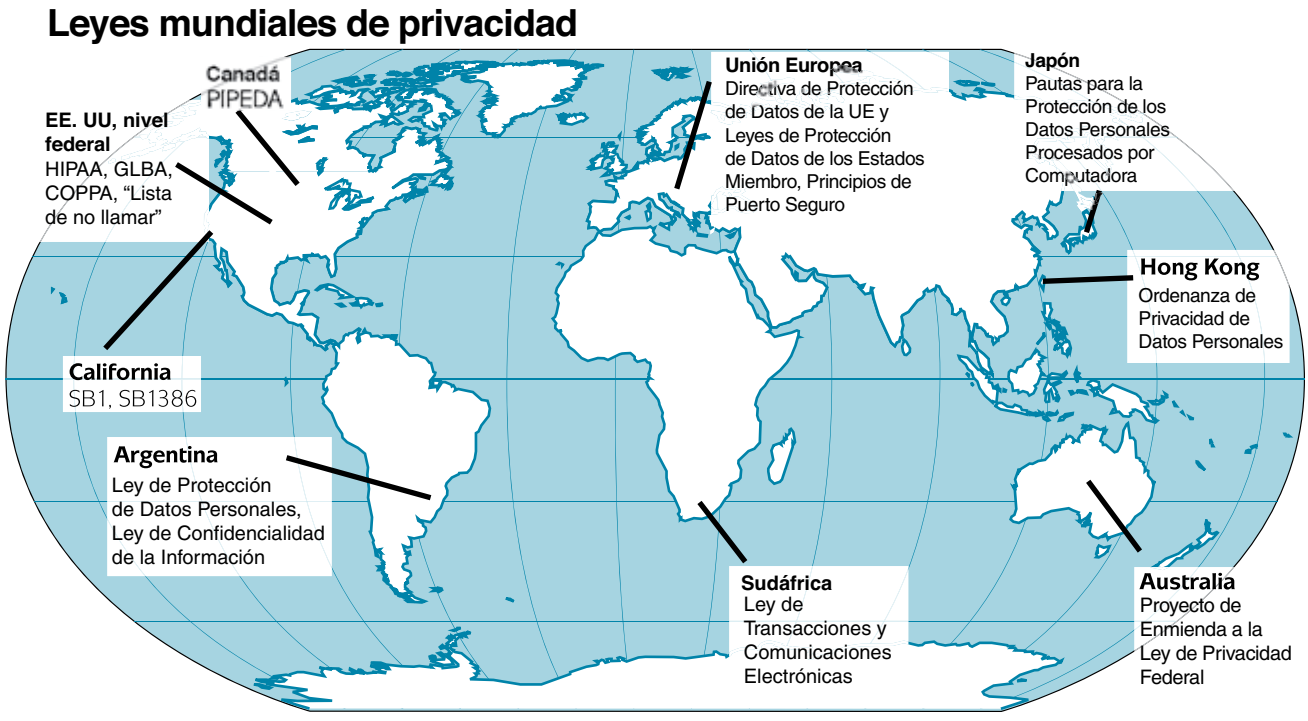
Enfoques no gubernamentales

Existe una amplia variedad de enfoques que se originan en las asociaciones profesionales, los prestadores de servicios, los proveedores, los órganos de estandarización y otros grupos de interés. Algunas leyes de privacidad, como por ejemplo, las de Australia, prevén que los organismos de supervisión avalen códigos de privacidad autoregulados que tal vez se vuelvan legalmente vinculantes una vez revisados y publicados. Las leyes también pueden sugerir auditorías de privacidad y sellos para los sistemas o servicios, como la Ley Federal de Privacidad de Alemania de 2003.

Organismos de estandarización

La Organización Internacional de Normalización (ISO, en inglés), el Instituto Nacional Estadounidense de Normas (ANSI, en inglés), la Asociación Canadiense de Normas, Normas de Australia y muchos otros organismos han desarrollado distintos enfoques de privacidad. El Código Modelo de la Asociación Canadiense de Normas para la Protección de la Información Personal (Q830) establece 10 principios que balancean los derechos de privacidad de las personas y los requerimientos de información de las organizaciones privadas. Los elementos clave del código de privacidad han sido incor-

Figura 3.3: Leyes de protección de datos (Deloitte/IIA 2004)



porados en la Ley PIPEDA Canadiense.

La Norma ANSI X9.99:2004 (Norma de Evaluación del Impacto de la Privacidad para el sector de servicios financieros) apunta a respaldar la implementación de Ley Gramm-Leach Bliley (GLBA, en inglés) de EE. UU. de 1999. La norma reconoce que la evaluación del impacto de la privacidad (PIA, en inglés) es una herramienta de gestión importante que se debe utilizar en una organización o por los terceros, para identificar y mitigar los problemas y riesgos de privacidad asociados con el procesamiento de datos del consumidor utilizando sistemas de información automatizados y conectados por redes. La norma PIA describe la actividad de evaluación del impacto de la de privacidad, define los componentes comunes de una PIA y explica cómo mejorar la calidad de los sistemas de negocio en función de las PIA.

Normas de Australia ha desarrollado la norma AS 2805.9-2000: Transferencia Electrónica de Fondos – Requerimientos para las Interfaces – Privacidad de las Comunicaciones. Esta norma especifica los métodos de protección contra la divulgación de la información contenida en determinados mensajes electrónicos. Normas de Australia ha desarrollado la norma AS 4721-2000: Prácticas de Privacidad Personal para el Sector Económico de Pago Electrónico de Tarifas, que describe los métodos de operación y las modalidades de conducta comercial que deben ser adoptadas por los operadores de sistemas de cobro electrónico de peajes y sistemas electrónicos de gestión de estacionamiento con el fin de proteger la privacidad personal de sus clientes.

El proyecto Plataforma de Preferencias de Privacidad (P3P) es un proyecto de estandarización técnica de World Wide Web Consortium (W3C) que proporciona una norma para establecer y negociar las políticas de privacidad entre operadores de sitios Web y usuarios de la Web. La norma proporciona un medio simple y automatizado para que los usuarios tengan más control del uso de su información personal en los sitios Web que visitan.

Enfoques profesionales

El Instituto Estadounidense de Contadores Públicos Certificados (AICPA, en inglés) y el Instituto Canadiense de Contadores Certificados (CICA, en inglés) desarrollaron un enfoque de privacidad amplio que incluye un conjunto de Principios de Privacidad Generalmente Aceptados (GAPP, en inglés), que apuntan a ayudar a las organizaciones con sus programas de privacidad. El enfoque de los GAPP fue desarrollado desde una perspectiva de negocio y hace referencia a las regulaciones de privacidad internas e internacionales más significativas. Cada uno de los 10 principios está respaldado por criterios objetivos y medibles que se deben satisfacer. Los principios son: gestión, avisos, elección y consentimiento, recolección, uso y retención, acceso, divulgación, seguridad, calidad, supervisión y puesta en vigor.

Los GAPP son útiles para los que supervisan y controlan los programas de privacidad, implementan y gestionan temas de privacidad o seguridad. También, se pueden utilizar para benchmarking, diseño e implementación de políticas y para mediciones de desempeño. El enfoque de los GAPP es un recurso excelente para los auditores internos que tienen la responsabilidad de evaluar el cumplimiento o de auditar los programas de privacidad o seguridad (consulte la página 25 del Apéndice para obtener los GAPP de AICPA/CICA).

Las normas de la Federación Internacional de Contadores (IFAC, en inglés) relativas a trabajos de privacidad están cubiertas por las Normas Internacionales sobre Trabajos de Aseguramiento (ISAE, en inglés) 3000. La ISAE establece principios básicos y procedimientos esenciales para los contadores profesionales dedicados a la práctica pública a fin de que puedan realizar trabajos de aseguramiento que no sean auditorías ni revisiones de los estados contables históricos. La ISAE 3000 cubre áreas como, por ejemplo, requerimientos éticos, control de calidad, aceptación y continuación del trabajo, planificación y ejecución del trabajo, obtención de evidencias y preparación del informe de aseguramiento.

Enfoques de negocio

La Alianza Internacional por la Seguridad, Confianza y Protección de la Privacidad (ISTPA, en inglés) es un ejemplo de una alianza global de proveedores de negocio y tecnología, cuyas meta es proporcionar una investigación y evaluación objetivas de las normas de privacidad, herramientas y tecnologías y definir un enfoque de privacidad para desarrollar soluciones tecnológicas. El enfoque de privacidad de la ISTPA se puede utilizar como guía para desarrollar soluciones operativas para los temas de privacidad y como herramienta analítica para evaluar la integridad de las soluciones propuestas.

Las asociaciones de marketing como la Asociación Australiana de Marketing Directo (ADMA, en inglés), la Asociación de Marketing Directo (DMA, en inglés) de EE. UU. y organismos equiparables de otras regiones han desarrollado iniciativas de auto-regulación para guiar a sus socios y aumentar la aceptación de su negocio por parte de las personas y los defensores de los derechos del consumidor.

Sellos de privacidad

Muchas organizaciones que realizan sus negocios en línea utilizan sellos de privacidad para obtener la confianza del cliente. Un sello de privacidad es un símbolo identificable otorgado a un operador Web por un programa de cumplimiento de terceros que significa que el operador ha implementado y acepta respetar prácticas de privacidad eficaces.

De acuerdo con la Alianza para la Privacidad en Línea (OPA, en inglés), las características de un programa de sello de privacidad ofrecido por un proveedor debe incluir lo siguiente: que su adopción sea ubicua, que sea lo suficientemente amplio como para abordar información confidencial y no confidencial, que el usuario tenga accesibilidad a este y que sea asequible. El proveedor también debe poder explorar las avenidas para mantener la integridad del sello, además debe tener la profundidad necesaria como para manejar consultas y reclamos.

Algunas de las organizaciones conocidas que proveen sello de privacidad son TRUSTe, BBBOnline, y Webtrust. TRUSTe proporciona un sello de privacidad de sitio Web a las organizaciones que completan una autoevaluación de privacidad, participan en una auditoría de sitio Web y aceptan someterse a una supervisión continua y admiten la resolución de controversias. El programa de privacidad de BBBOnLine otorga el sello de privacidad a los negocios que cumplen con los requerimientos del programa, como por ejemplo:

- Publicar un aviso de privacidad en línea que incluya el compromiso respecto de la privacidad y seguridad de los datos, que explique cómo se recoge y se utiliza la información, cómo se obtiene acceso a ella o se la corrige y como comunicarse con la organización.
- Realizar una evaluación amplia de la privacidad.
- Someterse a la supervisión y revisión por parte de la organización BBBOnline.
- Participar en el sistema de resolución de conflictos del consumidor con que cuenta el programa.

WebTrust es un sello de los institutos AICPA/CICA que requiere una auditoría realizada por un contador público certificado (CPA, en inglés) o por un contador certificado (CA, en inglés). Incorpora principios y criterios relacionados respecto de la seguridad, disponibilidad, integridad del procesamiento, privacidad y confidencialidad. Estos principios y criterios están organizados en cuatro áreas: políticas, comunicaciones, procedimientos y supervisión.

Este capítulo revisa el impacto de los problemas de privacidad, las amenazas, los riesgos y los mecanismos de control básico necesarios para su mitigación en las organizaciones comerciales, sin fines de lucro y gubernamentales.

Las organizaciones comerciales tienen tres grupos de interés principales: propietarios/prestamistas, empleados/personal y clientes/público general. Las organizaciones sin fines de lucro tienen implementados mecanismos de supervisión para administrar sus actividades de recolección de fondos, en lugar de hacer que los propietarios asuman esa responsabilidad. Las organizaciones gubernamentales prestan sus servicios a los ciudadanos y a los extranjeros, y también pueden tener clientes. En todos los casos, el buen gobierno recomienda a las organizaciones considerar los riesgos de privacidad, aún cuando se basen en motivos muy diferentes que pueden variar desde derechos constitucionales a simplemente buenas prácticas de negocio.

4.1 Impactos de la privacidad

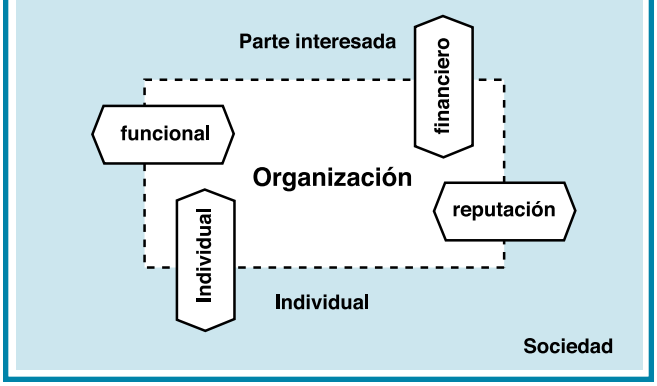
La información personal del individuo es utilizada por las organizaciones en diversas actividades de negocio, como investigación de mercado, calificación de clientes, gestión de derechos, marketing directo y transacciones de datos. También puede ser de interés para la comunidad, los amigos, la familia y la red profesional de las personas.

La información personal puede ser recogida y utilizada por gobiernos locales y extranjeros, competidores, empleados descontentos, piratas informáticos, ciberterroristas, saboteadores, ladrones de identidad y otros similares. Las amenazas contra los sujetos de datos requieren que las organizaciones protejan la información personal adecuadamente evitando litigios y consecuencias adversas.

4.2 Modelo de riesgos de privacidad

Los riesgos de privacidad se originan en la recolección, el uso, la retención y la divulgación de la información personal del individuo cuando actúa en su rol de consumidor, comprador, socio, cliente, trabajador, paciente, beneficiario, afiliado o ciudadano. Si bien es importante comprender las amenazas consiguientes para las personas, la dirección y los auditores internos centrarán la evaluación principalmente en las amenazas potenciales para la organización con relación al gobierno, las partes interesadas, los gerentes, el personal o los prestadores de servicios.

Figura 4.1: Categorizar las amenazas, los riesgos y los impactos respecto de la privacidad



Las amenazas y los riesgos referentes a la privacidad se pueden analizar utilizando un modelo en capas que describa la organización, las partes interesadas, las personas y la sociedad en general (tal como se muestra en la *Figura 4.1: Categorizar las amenazas, los riesgos y los impactos respecto de la privacidad*). Las fallas de privacidad tendrán consecuencias en lo concerniente a la función de negocio, la reputación, las finanzas y el individuo.

Amenazas para las organizaciones

Las organizaciones deben enfrentar las amenazas y los riesgos más tangibles: ellas perciben las consecuencias de las fallas de privacidad casi de inmediato. El impacto a escala de la organización, con frecuencia, atrapa la atención de la prensa, las autoridades de supervisión y de los organismos de control de la privacidad.

Las amenazas funcionales restringen la capacidad de la organización para alcanzar sus objetivos, ocasionan interrupciones operativas, ineficiencias e ineficacias. Las amenazas a la reputación de una organización limitan su capacidad futura de desempeño puesto que disminuyen la respuesta de los clientes y ciudadanos. Si bien las amenazas y los riesgos respecto de la privacidad limitan la capacidad de desempeño de la organización, se puede obtener una ventaja competitiva gestionando estas amenazas y riesgos con eficacia. Los impactos financieros en una organización son de gran utilidad para las partes interesadas, dichos impactos son, en la mayoría de los casos, consecuencia de problemas funcionales y de reputación relacionados con riesgos de privacidad. Los impactos en la sociedad se originan en un desempeño insuficiente, pérdidas financieras y efectos adversos para los socios de la sociedad. Existen riesgos de privacidad adicionales que salen a la superficie cuando una organización terceriza o externaliza parte de sus operaciones de negocio, combina o interrumpe sus actividades de negocio, contrata nuevos empleados, los reasigna o los separa de sus funciones.

Amenazas para las partes interesadas

Aunque implementar prácticas y controles de privacidad excesivos tal vez restrinja las eficiencias de procesamiento interno y externo de una organización, las partes interesadas generalmente enfrentan riesgos mucho más altos cuando hay daños en la reputación o litigios, con la consiguiente reducción del valor y de la rentabilidad de sus inversiones. Las prácticas de privacidad adecuadas son importantes para garantizar el valor de las inversiones de las partes interesadas en una corporación.

Amenazas para las personas

Las personas, con frecuencia, enfrentan las consecuencias directas de las amenazas a la privacidad. Tal vez, deban soportar costos adicionales, experimentar discriminaciones o tener opciones limitadas, a no ser que expongan su esfera privada a riesgos excesivos al ofrecer sus datos a proveedores y prestadores de servicios.

Cuando emprenden la búsqueda de nuevo empleo, las personas envían su currículum vítae a portales, consultores o potenciales empleadores, quienes pueden utilizar su información personal para otros propósitos sin el consentimiento o el conocimiento de la persona en cuestión. La información personal puede ser procesada utilizando técnicas de depuración o trazado de perfiles que pueden ser invasivas, desleales, poco confiables o provocar efectos adversos al individuo.

Es práctica común, por parte del empleador, supervisar las llamadas, el correo, las computadoras y el ámbito de la ofi-

cina en sí. Las personas confían en la confidencialidad de sus comunicaciones y ámbito cuando no se les informa sobre tales prácticas de supervisión.

Un individuo no tiene demasiado poder como para cuestionar las prácticas de privacidad de los negocios o del gobierno, o para obtener compensación por daños. Este desequilibrio es la razón principal por la cual la regulación de privacidad protege a los individuos.

Figura 4.2: Riesgos de privacidad en el procesamiento de datos personales

- Recolección excesiva.
- Información incompleta.
- Datos dañados.
- Información desactualizada.
- Controles de acceso inadecuados.
- Compartir la información de manera excesiva.
- Procesamiento incorrecto.
- Uso inadecuado.
- Divulgación inadecuada.

Amenazas para la sociedad

El desarrollo económico y social requiere un grado relativamente alto de libertad individual. Las sociedades en su conjunto pueden ser manipuladas para que realicen movimientos no deseados cuando el poder de los ciudadanos y del gobierno no están en el equilibrio adecuado. Los investigadores del comportamiento humano han observado que los ciudadanos sólo pueden ejercer su poder con eficacia si pueden conservar una mínima esfera de privacidad y si pueden comunicarse con libertad dentro de su comunidad. En consecuencia, la amenaza más grande para una sociedad sería el control sobre sus ciudadanos dado que implicaría una derrota para el progreso social, la adaptación y los mecanismos de estabilización (vea más abajo la *Figura 4.3: Oportunidades y amenazas a la privacidad*).

4.3 Temas del sector y la industria

Es crucial que los auditores comprendan el marco legal en el que opera la organización y que tengan en cuenta todas las leyes relevantes, regulaciones y guías del sector. Además, es importante que los auditores internos consulten al asesor legal interno cada vez que realicen actividades de evaluación o consultoría relacionadas con el programa y las prácticas de privacidad de la organización en todo lo concerniente a recolección, uso, divulgación y retención de información personal. Estos servicios de evaluación y consultoría pueden incluir las siguientes tareas:

- Buscar impulsores de riesgos de privacidad, entre ellos, identificación de la información personal recogida, consecuencias específicas para la organización y un enfoque de privacidad a aplicar.
- Identificar prácticas o enfoques de actividades del sector público o privado que sean equiparables y que puedan ser aplicadas.
- Rastrear las interfaces del sistema que procesan la información personal y evaluar las bases y la eficacia de cualquier intercambio, así como las potenciales exposiciones del sujeto de datos y la organización.
- Mediante consulta con el asesor legal interno, determinar si la recolección y el uso compartido de la información personal se realiza de manera excesiva y más allá de los límites del propósito del procesamiento.
- Mediante consulta con el asesor legal interno, evaluar las exposiciones de privacidad provocadas por la transferencia transnacional de datos y determinar las amenazas específicas, el riesgo para la organización y si se han implementado controles adecuados.

El gobierno y el ciudadano

Diversas instituciones gubernamentales recogen, almacenan e intercambian datos relativos a las personas. Los sujetos de datos y los tenedores de datos enfrentan la amenaza constante de que la información personal se use indebidamente, se pierda o sea robada de los vastos archivos gubernamentales.

Existe una regulación especial del sector público que determina cómo se debe tratar la información personal. En muchos países, existen leyes de tipo "paraguas" para los distintos niveles de entidades públicas. Otros países tienen reglas que se apli-

Figura 4.3: Oportunidades y amenazas a la privacidad

	Amenazas	Oportunidades
Organizaciones	• Litigios. • Publicidad negativa. • Pérdidas financieras, costo extra. • Interrupciones operativas. • Fracasos en el mercado.	• Inteligencia de mercado. • Reducción de costos. • Comunicación eficaz. • Ventaja competitiva.
Individuos	• Costo externalizado. • Supervisión. • Robo de identidad. • Spam. • Restricciones de los derechos civiles.	• Servicios personalizados. • Productos más económicos. • Ofrecimientos dirigidos. • Construcción de una red.

can según cada caso en particular. Por lo tanto, los auditores gubernamentales deben centrarse en una amplia variedad de registros y programas, como por ejemplo, registros de propiedad de bienes raíces, registros de votantes, censos y encuestas de opinión, registros impositivos, archivos de seguridad nacional e información recogida para los programas de asistencia social y para trabajo social, educación y cumplimiento de leyes.

El seguro social y la vida comunitaria

Numerosas instituciones de seguridad social, aseguradoras, programas de bienestar social, programas de trabajo social, al igual que otras organizaciones sin fines de lucro, mantienen bases de datos significativos y confidenciales para realizar sus actividades. En muchos casos, rigen regulaciones de tipo "paraguas" para el sector público o privado. Algunas instituciones, las iglesias por ejemplo, pueden estar exentas de los marcos legales generales, lo cual puede dar lugar a un régimen de privacidad algo débil. En muchos casos, se almacenan y se procesan datos confidenciales. Las comunidades tienen alto riesgo de perder la confianza de sus miembros cuando tratan los datos personales de manera inapropiada.

Los sistemas de seguridad social y gubernamentales pueden ocasionar exposiciones adicionales mediante la combinación de datos de manera inapropiada y excesiva, o comparando los datos personales originados en distintas fuentes. Con frecuencia, hay reglas, leyes y acuerdos específicos que determinan en qué circunstancias y hasta qué punto combinar y compartir datos es una actividad legítima. Otro problema que surge de la combinación de datos y sus fugas es la obtención de identificadores (ID) que se pueden usar indebidamente para recoger y combinar datos, para manipular o robar una identidad.

Servicios financieros

Las organizaciones de servicios financieros, como los bancos, los emisores de tarjetas de crédito, los fondos y las aseguradoras mantienen información personal confidencial exhaustiva, como por ejemplo, calificaciones crediticias, ingresos, patrones de gastos, lugar de residencia e historial de crédito. Como resultado de ello, existen numerosas regulaciones y órganos de supervisión activos.

Marketing y venta minorista

El sector de marketing y venta minorista es un vasto recolector, usuario y distribuidor de información personal. Los datos que se mantienen para propósitos de marketing y venta minorista pueden ir desde listas de domicilios a perfiles detallados de consumidores, información financiera e historiales de compras.

Figura 4.4: Código de conducta de marketing directo de ADMA

Principios de privacidad

- Recolección.
- Uso y divulgación.
- Calidad de los datos.
- Seguridad de los datos.
- Apertura.
- Acceso y corrección.
- Identificadores.
- Anonimato.
- Flujos transfronterizos de datos.
- Información confidencial.

Por ejemplo, cuando una persona realiza una compra, el pago se debita inmediatamente de su cuenta, con un registro de la transacción que muestra la fecha, la hora, el lugar y el proveedor. El sistema de gestión de inventario del comercio minorista captura electrónicamente y retiene los datos del artículo, su tamaño, color e ID del cliente. Además, los mecanismos de seguimiento y etiquetado, como las tecnologías de identificación por radiofrecuencia están comenzando a aparecer y surgen cuestiones de privacidad sobre la capacidad de realizar un seguimiento de las personas.

Los datos se recogen constantemente desde distintas fuentes e incluyen datos transaccionales, datos compartidos con otras organizaciones, datos recopilados de fuentes públicas o de los mismos individuos y datos comprados a intermediarios de información. La información se puede utilizar para determinar y contactar potenciales clientes, para definir grupos de clientes utilizando minería de datos, o para crear perfiles detallados con el objeto de centrarse en las necesidades e intereses individuales.

Las asociaciones del sector ofrecen diversos códigos de conducta para las empresas de marketing. Por ejemplo, la ADMA proporciona el Código de Conducta de autoregulaciones que cubre los principios de privacidad que deben ser considerados y abordados por todos sus miembros (consulte la *Figura 4.4: Código de Conducta de Marketing Directo*).

Comunicación y medios

La privacidad de la comunicación y los medios comprende la capacidad de mantener la confidencialidad de la información personal, así como la libertad de acceso a los medios y a los canales de comunicación. Más allá de eso, la información personal es capturada por los registros de cliente, suscriptor y prestamista. La totalidad de dichos datos puede ser usada para deducir preferencias y perfiles individuales. Los datos transaccionales adicionales proporcionan un repositorio de información personal relacionada con la compra y la utilización de patrones, incluidos patrones de comunicación, la hora, el lugar y el contenido. Eso puede provocar problemas como SPAM, escuchas secretas, divulgación inesperada de la comunicación y su contenido, y vigilancia gubernamental excesiva.

Servicios públicos, transporte y viajes

El uso de los servicios públicos alguna vez fue un hecho simple y anónimo, no más que una moneda en el medidor de electricidad o en una estación de peaje, o una simple perforación en un boleto de papel cuando uno deseaba viajar en ómnibus. Sin embargo, hoy los sistemas son sofisticados y están conectados en red. Cuando una persona pasa por una cabina de peaje, se registra la patente de su vehículo y se carga el gasto a su tarjeta de crédito. Otro sistema registra el vehículo cuando ingresa a un estacionamiento cinco minutos más tarde. Estos sistemas integrados pueden generar perfiles detallados de las personas al combinar los datos de los sistemas de control de tráfico y acceso con información transaccional adicional. Numerosos países prevén la necesidad de establecer resguardos adicionales o de remitirse a cláusulas constitucionales para evitar la recolección excesiva de datos a fin de proteger la privacidad de ciudadanos y consumidores en esas circunstancias.

Servicios de salud e investigación

Los servicios de salud requieren y generan información confidencial de los pacientes. La información personal es necesaria

para la investigación clínica, los servicios médicos, las pruebas médicas y la gestión relativa a enfermedades. En Estados Unidos, la Ley HIPAA fue promulgada en 1996 para proteger la información personal del paciente y se aplica a planes de salud, centros de liquidación de servicios de salud, prestadores de servicios de salud y empleadores. (vea la *Figura 4.5: Regla de privacidad de la Ley HIPAA 2003 de EE. UU.*). Otros países tienen leyes similares amplias que se aplican a estos casos.

Figura 4.5: Regla de Privacidad de la Ley HIPAA 2003 de EE. UU.

El objetivo de la Ley HIPAA es mejorar la eficiencia y eficacia de los sistemas de servicios de salud al facilitar el intercambio electrónico de la información, a la vez que admite los desafíos que ello implica para la confidencialidad de la información de salud. La Ley HIPAA:

- Protege toda la información de salud identificable individualmente.
- Define y limita las circunstancias en las que la información de salud de un individuo puede ser utilizada o divulgada.
- Requiere la autorización por escrito para el uso o la divulgación de la información de salud protegida siempre que no sea por razones de tratamiento, pago u operaciones de servicios de salud, y cuando no sea permitido o requerido por la Regla de Privacidad.
- Limita los usos y las divulgaciones al grado mínimo necesario.
- Requiere el desarrollo y la implementación de políticas y procedimientos que restrinjan el acceso y los usos.
- Requiere que se proporcione un aviso de las prácticas de privacidad y que se incluya un punto de contacto para obtener más información y poder realizar reclamos.
- Otorga a los individuos el derecho de revisar y obtener una copia de su información de salud protegida.
- Otorga a los individuos el derecho de obtener una explicación por la divulgación de su información de salud protegida.
- Requiere resguardos administrativos, técnicos y físicos para evitar el uso intencional o no, o la divulgación.

Negocios internacionales

Numerosas leyes y regulaciones exigen que la información personal de los individuos no abandone la zona regulada. Estas reglas ayudan a abordar la preocupación respecto de la pérdida de control cuando la información personal se transfiere a otra jurisdicción legal. Las organizaciones que transfieren tales datos están sujetas a situaciones de bochorno serio, daños a su reputación y pérdidas financieras si la información es administrada de manera indebida.

Esto crea importantes desafíos en un mundo de sistemas conectados por redes donde la información se transporta a través de las fronteras dentro de una organización, o bien entre sus socios comerciales que utilizan y procesan esa información personal en una escala transnacional. Ejemplos de tales casos son los sistemas de reservas, las funciones de recursos humanos en empresas multinacionales y la cooperación de cumplimiento de la ley a nivel transnacional (consulte la *Figura 4.6: Flujo transfronterizo de datos, Problemas para los sujetos de datos*).

Figura 4.6: Flujo transfronterizo de datos. Problemas para los sujetos de datos

- Barreras idiomáticas.
- Pérdida de control sobre los datos.
- Pérdida de protección legal.
- Controversias, no factibles.
- No hay garantías de acceso.
- Seguridad difusa.

Los regímenes internacionales [OECD 1980 y APEC 2004] y regionales [CE 1981 e UE 1995] crean un enfoque para establecer un grado de confianza. Las organizaciones comerciales y sin fines de lucro deben asegurarse de que la información personal que recogen, utilizan, divulgan y retienen permanezca en un lugar seguro y controlable, en el que las normas aplicables sean aceptadas y estén vigentes.

Los convenios de puerto seguro (como el de la *Figura 4.7: Convenio de Puerto Seguro de EE. UU/UE 2000*), el reconocimiento mutuo de los instrumentos legales, la autoregulación y, en algunos casos, la referencia a las regulaciones de tipo "paraguas" como las pautas de la OECD y del CE, proporcionan una base para que los regímenes de privacidad aborden las transferencias de datos internacionales. La Cámara Internacional de Comercio (ICC, en inglés), la UE y otros organismos proporcionan contratos modelo para asegurar la adopción de resguardos de privacidad generalmente aceptados, para cuando en los negocios se intercambian datos personales a través de las fronteras.

Figura 4.7: Convenio de Puerto Seguro de EE. UU/UE del 2000

Autocertificación de los tenedores de datos a siete principios establecidos por el Departamento de Comercio de EE. UU:

- Principio de emisión de aviso.
- Principio de elección.
- Tranferencia hacia adelante.
- Seguridad.
- Integridad de datos.
- Principio de acceso.
- Principio de puesta en vigor.

4.4 Enfoque de control de privacidad

Las actividades básicas del enfoque de control de privacidad se centran en fijar los objetivos, establecer políticas y procedimientos, y estipular mecanismos de supervisión y mejoras. El establecimiento de objetivos es importante para asegurar que la organización tenga conciencia de sus necesidades de privacidad y que pueda implementar y supervisar los procedimientos requeridos en todos los niveles. Las políticas y los procedimientos de la organización establecen una estructura para liderar y coordinar esfuerzos relacionados con la operatividad y la privacidad. Los mecanismos de supervisión y mejora son necesarios para desarrollar experiencia y para adaptar los objetivos y dirigir la organización en un entorno cambiante.

Aplicar modelos de control a la gestión de privacidad

Numerosas organizaciones utilizan enfoques de control como el Enfoque Integrado de Control de Interno de 1992 del Comité de Organizaciones Patrocinadoras de la Comisión Treadway (COSO, en inglés), o su versión mejorada de 2004, Enfoque

Figura 4.8: Enfoques de control más utilizados

- Enfoque Integrado de Control Interno de 1992 de COSO.
- Enfoque Integrado de Gestión de Riesgo Empresarial de 2004 de COSO.
- Criterios de Control (CoCo, en inglés) de 1995 del CICA.
- Objetivos de Control de Información y Tecnología Relacionadas (CobiT, en inglés) de 2005 del Instituto de Gobierno de TI.
- ISO/Comisión Electrotécnica Internacional (IEC, en inglés) 27001 (BS 7799).

Figura 4.9: Controles de privacidad en el Enfoque de COSO ERM	
Entorno interno.	La cultura y la imagen de privacidad de una organización están estrechamente vinculadas a sus clientes y a la responsabilidad social, y son críticas para el entorno interno de control y riesgos de privacidad. Este entorno interno abarca el código de privacidad, las políticas de privacidad implícitas y explícitas, y la cultura de privacidad de la organización, según lo establece y lo comunica la alta dirección; todo lo cual debe estar en concordancia con las leyes y regulaciones aplicables.
Definición de objetivos	La dirección debe establecer una misión y visión para la organización, a partir de las cuales se puedan derivar los objetivos de privacidad y la política de privacidad, directa o indirectamente. Las políticas organizacionales, los perfiles de los puestos de trabajo y los planes de desempeño individual pueden abarcar explícitamente los objetivos de privacidad.
Identificación de incidentes	La tarea de identificar las potenciales amenazas internas o externas para la privacidad forma parte principalmente de la evaluación periódica y permanente en cuanto a riesgos de la tecnología de la información y de las operaciones.
Evaluación de riesgos	Según el campo de actividad de la organización, la privacidad puede ser un aspecto más o menos importante en la evaluación de riesgos de TI y de las operaciones. En consecuencia, las exposiciones inherentes y residuales de privacidad deben ser bien entendidas por la dirección y el personal de operaciones, así como las funciones de TI.
Respuesta al riesgo	Los procesos de negocio basados en la privacidad, la limitación a la recolección, la seguridad de los datos, la gestión de contingencias y las medidas en cuanto a gestión de datos impiden, aceptan, reducen o comparten los riesgos relacionados con la privacidad.
Actividades de control	Las políticas de la organización, los procedimientos y las estructuras que aseguran una respuesta al riesgo, abarcan elementos tales como seguridad de datos, controles de acceso, controles de integridad y contingencias, revisiones de privacidad, defensor de privacidad y muchos otros más.
Información y comunicación	La información relevante debe ser facilitada oportunamente para permitir un control eficaz; entre los instrumentos se incluye la observación de las métricas de privacidad y el informe sobre los problemas y su mitigación.
Supervisión	El sistema de gestión de riesgos de privacidad requiere supervisión y adaptación, según sea necesario. Una organización puede designar a un comisario de privacidad, mantener un registro de datos, evaluar las solicitudes de acceso a los registros de información personal y realizar auditorías de privacidad.

Integrado de Gestión de Riesgo Empresarial. Las organizaciones también pueden buscar otros enfoques de control, como por ejemplo los incluidos en la lista de la *Figura 4.8: Enfoques de control más utilizados* (de la página anterior), que son útiles a la hora de desarrollar una óptica para analizar y mitigar las exposiciones de privacidad. Al aplicar las categorías del enfoque de Gestión de Riesgo Empresarial (ERM, en inglés) de COSO a la gestión y control de privacidad, se proporciona un ejemplo práctico para evaluar la privacidad dentro del enfoque de control y riesgo de la organización. (Vea la *Figura 4.9: Controles de privacidad en el enfoque de COSO ERM*)

El enfoque de COSO ERM comprende tres dimensiones: la organización, los objetivos y los componentes de la gestión de riesgos. La dimensión de la organización describe los elementos estructurales que se deben utilizar para analizar los impulsores de riesgo y para implementar mecanismos o responsabilidades. La dimensión de los objetivos ayuda a definir los objetivos estratégicos, operativos, de cumplimiento y de los informes que se deben tener en cuenta para una evaluación de la privacidad. La dimensión referente al componente de gestión de riesgos es instrumental para considerar los controles de privacidad en una organización. Con una mirada más minuciosa en esta dimensión, la auditoría interna puede conocer cuáles son las áreas potenciales a revisar.

Usar un modelo de madurez de privacidad

El auditor necesita criterios para evaluar dónde está una organización respecto a sus prácticas de privacidad. Para ilustrar la etapa de desarrollo de las prácticas de privacidad se puede utilizar un modelo de madurez de capacidad como el de la *Figura 4.10: Niveles genéricos de madurez de privacidad*, en la página siguiente.

Cuando una organización decide emplear un modelo de madurez, el rol de la auditoría interna es respaldar el desarrollo del modelo para recoger y analizar datos, comunicar los resultados de una evaluación y validar las autoevaluaciones realizadas por las líneas o unidades de negocio. La auditoría interna también debe supervisar la implementación de los planes de mejora.

La evaluación, basada en el modelo de madurez, de las prácticas de privacidad se centrará en los niveles de madurez respecto de un conjunto de principios de privacidad o criterios específicos obtenidos de un programa de trabajo o de un cuestionario de benchmarking. En función de la madurez de las prácticas existentes en la organización, los resultados de auditoría interna pueden conducir a:

- Medir el nivel de madurez.
- Servir como impulsor de la toma de conciencia y ejercer influencia para lograr el compromiso de las partes.
- Evaluar las políticas y los procedimientos.
- Realizar o respaldar las evaluaciones de riesgos.
- Recomendar el establecimiento de un responsable de la privacidad o de un equipo de trabajo al respecto.
- Establecer auditorías de cumplimiento.
- Evaluar funciones, procesos, controles, productos y servicios.

Figura 4.10: Niveles de madurez de privacidad genérica	
Inicial	Las actividades son específicas para el caso y: • No hay políticas, reglas ni procedimientos definidos. • Finalmente existen actividades de nivel inferior, no coordinadas. • Existen redundancias y falta trabajo en equipo y compromiso.
Repetible	La política de privacidad se define y: • Hay cierto compromiso de la alta dirección. • Hay conciencia y compromiso general. • Existen planes específicos en las áreas de alto riesgo.
Definido	La política de privacidad y la organización están en su sitio y: • Se realizan evaluaciones de riesgos. • Se establecen prioridades y se asignan recursos en consecuencia. • Existen actividades para coordinar e implementar controles de privacidad eficaces.
Gestionado	En la organización se refleja un nivel eficaz coherente de gestión de privacidad, requerimientos y consideraciones al respecto, y además: • Existen consideraciones anticipadas respecto de la privacidad en los sistemas y el desarrollo de procesos. • Se observan elementos de privacidad integrados en las funciones y en los objetivos de desempeño. • Hay supervisión a nivel funcional y organizacional. • Existen revisiones periódicas basadas en el riesgo.
Optimizado	Se observa una mejora continua de las políticas de privacidad, prácticas y controles, y: • Sistemáticamente se examinan los cambios en profundidad para ver su impacto en la privacidad. • Se asignan recursos exclusivos para lograr los objetivos de privacidad. • Existe un alto nivel de integración interfuncional y trabajo en equipo para satisfacer los objetivos de privacidad.
— Fuente: Hargraves et al 2003	

- Establecer o validar las autoevaluaciones.
- Ofrecer recomendaciones, planes de acción e implementar la supervisión.

4.5 Identificar organizaciones de alto y bajo rendimiento

El nivel de rendimiento de una organización se puede determinar empleando un modelo de madurez, al mismo tiempo que se aplica el método de benchmarking contra los principios generales, un enfoque de control o mejores prácticas.

Indicadores de problemas potenciales de privacidad

Los problemas potenciales de privacidad se ponen de manifiesto cuando se efectúa una tarea de benchmark de nivel superior sobre las prácticas de privacidad de la organización en relación con cada conjunto de principios de privacidad básicos. Por ejemplo, los ocho principios de la OECD de la *Figura 4.11: Indicadores de problemas de privacidad*, hacen posible realizar ese tipo de análisis rápido.

Mejores prácticas de privacidad

Se puede obtener una amplia gama de mejores prácticas a partir de los enfoques de privacidad existentes, las investigaciones y las guías de organizaciones como la OECD, el Consejo de Europa, la Comisión de la UE, AICPA, CICA y muchas otras asociaciones del sector. Varias de las siguientes prácticas de privacidad han demostrado que respaldan una buena gestión de privacidad y que evitan sorpresas frustrantes:

- Realizar evaluaciones adecuadas y regulares de riesgos de privacidad.
- Designar un mediador, funcionario u organización a cargo de la privacidad para que esté disponible y actúe como punto central de la coordinación de las actividades relativas a la privacidad y del manejo de los reclamos y los problemas.
- Desarrollar conciencia respecto de los riesgos del manejo de datos clave y de robo de identidad.

Figura 4.11: Indicadores de problemas de privacidad

Principio	Indicador de problema de privacidad
Limitación a la recolección	No hay bases legales ni consentimiento explícito para la recolección de datos.
Calidad de los datos	Nunca se revisa la idoneidad y precisión de los datos.
Especificación del propósito	El propósito para la recolección de datos no está claramente definido.
Limitación de uso	La información personal se utiliza para otros propósitos diferentes de los que inicialmente se previeron, con la consecuente ausencia de base legal o consentimiento.
Resguardos de seguridad	La información personal no está protegida adecuadamente contra daños, pérdida o divulgación.
Apertura	Las políticas, las prácticas y los medios utilizados para procesar los datos personales no son transparentes.
Participación individual	Las personas no tienen la oportunidad concreta de obtener información sobre la información personal de su pertenencia que se procesa y se retiene.
Responsabilidad	La organización tiene la responsabilidad de establecer e implementar los controles y procesos.

- Enmascarar los números de identificación personal, como los números de seguridad social y cualquier otra información confidencial, siempre que sea posible.
- Supervisar y capacitar al personal del centro de atención telefónica para impedir la ingeniería social y otros riesgos similares.
- Gestionar con eficacia todas las relaciones con proveedores independientes y listas de marketing.
- Crear conciencia sobre las vulnerabilidades de la Web y del correo electrónico.
- Desarrollar políticas para la retención y destrucción de registros.
- Implementar un esquema de clasificación basado en la confidencialidad y el mapeo de datos.
- Realizar evaluaciones de riesgo de los controles de acceso, las restricciones físicas de acceso de seguridad y modificar los controles al respecto.
- Implementar tecnologías de detección y prevención de intrusiones.
- Efectuar pruebas de penetrabilidad, junto con revisiones y pruebas independientes de los controles, sistemas y procedimientos clave.

Limitar la recolección de datos a aquellos necesarios operativamente, otorgar anonimato a la información personal, utilizar tecnologías de seguridad como el cifrado y usar mecanismos de inclusión y exclusión voluntaria también ayuda a que las personas tengan confianza en la organización, a la vez contribuye a que la organización evite o mitigue los riesgos de privacidad. Además, las auditorías de privacidad, los sellos y las certificaciones muestran un compromiso por parte de la organización para establecer un enfoque y un nivel de desempeño determinados. Los informes de privacidad establecen la transparencia y la confianza adicional en el compromiso de la organización para tratar adecuadamente los datos personales (consulte la *Figura 4.12: Buenas prácticas de privacidad*).

Figura 4.12: Buenas prácticas de privacidad

- Crean confianza en el consumidor.
- Protegen la integridad de la marca de su organización.
- Aumentan la lealtad del cliente.
- Contribuyen en el resultado final.

— Fuente: Industry Canada

Auditar las prácticas de privacidad de la organización comprende la evaluación de riesgos, la planificación y el desempeño del trabajo, la comunicación de los resultados y el seguimiento. No obstante, hay aspectos adicionales que el DEA debe tomar en cuenta, como por ejemplo, violaciones de la privacidad, gestión de personal y problemas respecto de la retención de registros. Muchos de estos aspectos están cubiertos a través de las prácticas profesionales de la profesión de auditoría interna, externa y de TI. En este capítulo se describen los problemas y las metodologías clave.

5.1 Rol de la auditoría interna dentro del enfoque de privacidad

En el entorno de negocio actual, los controles de privacidad son requerimientos legales y de negocio, y las políticas y prácticas generalmente aceptadas están en su etapa de desarrollo. El organismo de gobierno de la organización tiene a su cargo establecer un enfoque de privacidad apropiado, y la auditoría interna puede evaluar ese enfoque, identificar los riesgos significativos y realizar las recomendaciones apropiadas. Cuando se evalúa el enfoque de privacidad de la organización, los auditores internos deben considerar lo siguiente:

- Las leyes y regulaciones de todas las jurisdicciones en las que se ejecutan los negocios.
- Las políticas y pautas de privacidad interna.
- Las políticas de privacidad destinadas a los clientes y al público general.
- La posibilidad de vincularse y comunicarse con el asesor legal interno para comprender las implicancias legales.
- La posibilidad de vincularse con los especialistas de tecnología de la información y los propietarios del proceso de negocio para comprender las implicancias de seguridad de la información.
- La madurez de los controles de privacidad de la organización.

El rol del auditor abarca realizar evaluaciones de riesgos de privacidad y proporcionar aseguramiento sobre los controles de privacidad en toda la organización. Las áreas típicas que la auditoría interna debe revisar son:

- La supervisión que ejerce la dirección.
- Políticas y controles de privacidad.
- Avisos de privacidad aplicables.
- Tipos e idoneidad de la información que se recoge.
- Sistemas que procesan la información personal.
- Metodologías de recolección.
- Usos de la información personal de acuerdo al propósito declarado, leyes y otras regulaciones aplicables.
- Prácticas de seguridad que cubren la información personal.

Cuando los auditores internos asumen parte de la responsabilidad de desarrollar e implementar un programa de privacidad, su independencia se puede ver afectada. Por esta razón y debido a la posible necesidad de contar con suficiente experiencia técnica y legal, tal vez se requiera la participación de terceros independientes.

5.2 Planificación de la actividad

Norma 2010 del IIA: La planificación requiere que el DEA configure un plan de auditoría basado en riesgos. PA 2010-1: Vincular el plan de auditoría al riesgo y exposiciones, detalla de manera adicional que es necesario tener en cuenta el universo de la auditoría, los objetivos de negocio, los riesgos y los controles. Todos ellos pueden verse influenciados por los objetivos y los riesgos de privacidad.

Durante la planificación de la auditoría y la evaluación de riesgos, el auditor interno debe tener en cuenta temas tales como la divulgación de la información de negocio confidencial, las violaciones a la privacidad y los daños a la reputación. Las cuestiones legales, como por ejemplo, el aumento de las regulaciones en todo el mundo para proteger la privacidad individual, el cumplimiento de los contratos fuera del país de la organización, y los temas impositivos y contables son algunas de las áreas de control y riesgo más críticas que debe abordar el auditor interno.

5.3 Establecer prioridades y clasificar datos

Los datos privados de una organización se pueden considerar un activo corporativo y su valor será positivo o negativo en función del control ejercido sobre este. Los datos bien controlados y utilizados adecuadamente realzan la valía de una organización al ofrecer un valor adicional a sus clientes. Los datos personales divulgados constituirán un pasivo al reducir la confianza del cliente y aumentar el riesgo de acciones legales y de regulaciones. La dirección puede no estar muy dispuesta a asignarle un valor monetario a la privacidad hasta que esta se pierda.

Un programa de clasificación corporativa de los datos de privacidad protegidos servirá de ayuda para priorizar los datos. Asignar un nivel de confidencialidad a los datos (como por ejemplo, de propiedad, confidenciales o públicos) sirve de ayuda para evaluar la idoneidad de los controles sobre la tecnología y los procesos de negocio que los utilizan. El auditor se puede preguntar lo siguiente:

- ¿Cuáles son las sanciones reglamentarias impuestas por el mal manejo de datos de privacidad protegidos? ¿Cuál será el recurso legal que tendrán las personas afectadas?
- ¿Cómo se asignó la propiedad de los datos? ¿Se establecieron controles apropiados para el manejo de datos?
- ¿Se han clasificado los datos? ¿Los niveles de clasificación son apropiados como para garantizar que se hayan implementado los controles de privacidad adecuados?
- ¿Hasta dónde una violación de privacidad divulgaría datos? ¿A quién se debería notificar? ¿Cómo se los debería notificar?
- ¿Qué costo tendría la tarea de solucionar los diversos tipos de divulgaciones de privacidad no autorizadas?
- ¿Cómo impactaría una violación de privacidad sobre la confianza de los clientes, los ciudadanos (en el caso de entidades públicas) o los inversores? ¿Cuánto costaría recuperar la confianza?

5.4 Evaluar los riesgos

Durante toda la planificación de auditoría y cuando se prepara la determinación de riesgo individual, hay cuatro áreas principales de riesgo que se deben abordar: legal y organizacional, infraestructura, aplicaciones y procesos de negocio.

Riesgos legales y organizacionales

El cumplimiento con leyes y regulaciones aplicables es la base de la mayoría de los programas de privacidad. Un abogado versado en cuestiones de privacidad puede liderar la actividad de cumplimiento al respecto, ayudando en el diseño de un programa de privacidad, revisando contratos con terceros para garantizar que existan controles de privacidad apropiados y proporcionando asesoramiento ante incidentes de divulgación de privacidad. Dado que las leyes y regulaciones de privacidad siguen evolucionando en virtud de las acciones, casi diarias, de tribunales y organismos de control, una organización debe obtener los servicios de un profesional del área legal especializado en el sector específico de la organización.

Además, todas las organizaciones deben designar una persona que sea el coordinador o contacto principal y que tenga a su cargo la responsabilidad primaria de los problemas de privacidad. En las organizaciones más pequeñas, esta responsabilidad puede ser parte de las obligaciones habituales del asesor legal de la organización, del director de cumplimiento, del gerente de recursos humanos o del director de seguridad de la información. En las organizaciones que, como parte central de su negocio, deben manejar información financiera o de salud, se justifica disponer de una persona exclusivamente dedicada a esta función, o también es posible que esto sea requerido por las leyes que rigen sobre el sector en particular. Muchas organizaciones han establecido el puesto de director de privacidad (CPO, en inglés), quien responde directamente al director ejecutivo o al consejo de administración. Una persona en este nivel puede proporcionar el nivel de conciencia y defensa necesario para asegurar que se identifiquen y se comuniquen los riesgos de privacidad, y que se asignen recursos suficientes para abordarlos.

Para una organización es igualmente importante la protección de la privacidad como el manejo de los incidentes de violación de la privacidad. El contacto principal de privacidad debe coordinar el equipo de respuesta ante incidentes de privacidad que actúa como nexo con las áreas operativas, legales, administrativas y de tecnología dentro de la organización, así como también con los potenciales reclamantes, la prensa y el cumplimiento de ley.

Si no se cuenta con la imagen de gerencia apropiada y liderazgo sólido en cuanto a privacidad, el programa al respecto de la organización puede carecer de recursos y quedar sepultado dentro de la estructura de la organización. Esas condiciones negativas minimizarán la eficacia del programa de privacidad y contribuirán al riesgo de no cumplimiento.

Algunas preguntas legales y organizacionales que se pueden realizar cuando se planifica una auditoría de privacidad son las siguientes:

- ¿Quiénes son los contactos designados a cargo de la privacidad? ¿Qué porcentaje de su tiempo dedican a los problemas de privacidad? ¿Cuentan con suficiente presupuesto y respaldo de la dirección como para implementar y mantener el programa de privacidad?
- ¿De qué manera los líderes de privacidad de la organización se mantienen al tanto en cuanto a sus conocimientos sobre leyes y regulaciones que afectan a la organización?
- ¿La organización tiene un plan para responder a un incidente de privacidad? ¿En dicho plan, se incluyen a las personas adecuadas? ¿El plan está actualizado?
- ¿Cómo están involucrados los contactos de privacidad en la evaluación de nuevas tecnologías y programas que impactan sobre los problemas de privacidad?

Riesgos de infraestructura

Un principio básico de la seguridad de la información es proporcionar confidencialidad, integridad y disponibilidad de datos, lo cual se superpone con muchas de las metas de un programa de privacidad. La privacidad descansa en los controles implementados por seguridad de la información, pero no toda la seguridad de la información se ocupa de la privacidad. Una auditoría de un programa de privacidad necesariamente implica realizar una revisión significativa de los controles de seguridad de la información. La parte más ardua tal vez sea simplemente identificar cómo fluye la información hacia adentro y hacia afuera de la organización.

Para ser útil, la información debe ingresar y egresar de la aplicación y frecuentemente cambia de soporte varias veces durante su vida útil. Los datos pueden iniciar su procesamiento como copia en papel, luego se los transporta a través de Internet, se los almacena en un disco magnético, se los imprime y archiva en ficheros, se realiza una copia de respaldo en un disco óptico para finalmente enviarlos fuera del lugar en cinta magnética. Cada vez que los datos se mueven y cambian su formato, su vulnerabilidad cambia.

Las trituradoras de papel, el cifrado, las cajas fuertes y los gabinetes con llave cumplen un papel importante como medidas contra la fuga de datos. Los auditores deben revisar el ciclo de vida de la información personal que la organización maneja y determinar si se lo hace con el cuidado apropiado en cada paso.

Por ejemplo, ¿cómo se utiliza el cifrado en el manejo de datos? Los auditores deben rastrear los datos tanto cuando están en tránsito en las redes públicas y privadas, como en los medios de datos manejados por el servicio de mensajería. También deben realizar un seguimiento de los datos almacenados en producción, así como en los entornos de respaldo y de recuperación de desastres.

Además, los auditores deben preguntar cuántas veces los datos se convierten de una a otra forma, y rastrear tales datos a medida que pasan de papel a paquetes de bits, a cinta, a papel, a cinta y a discos magnéticos. Deben determinar si los datos están siendo transferidos o copiados y si los datos residuales pos transferencia se tratan con el mismo conjunto de reglas que los datos de origen.

Riesgos de la aplicación

Descubrir no sólo *quién*, sino *qué* maneja su información adquiere una importancia crítica cuando se identifican riesgos de privacidad. El software ofrece velocidad y exactitud en oposición a las funciones manuales proclives a numerosos errores. Lamentablemente, los sistemas de software pueden ser complejos, con fallas y comportamientos no deseados. Evaluar las funciones del software no es una tarea simple porque las organizaciones, con frecuencia, utilizan una mezcla de software desarrollado internamente, software comercial (COTS, en inglés) adaptado a medida y sistemas operativos e intermedios de respaldo para procesar, compartir y distribuir sus datos.

Una vez que el auditor identifica los procesos automatizados, es necesario abordar preguntas de seguridad muy básicas en relación a cualquier aplicación que maneje información privada:

- ¿Se identificaron problemas de privacidad en los requerimientos de definición de la aplicación?

- ¿Se han implementado normas de clasificación de datos en la aplicación para garantizar que existen controles apropiados sobre los datos y la información?
- ¿Cómo fue validada la implementación de los requerimientos en el desarrollo e instalación de la aplicación?
- ¿De qué manera la aplicación autoriza y autentica a los usuarios?
- ¿Qué clase de roles de usuario tiene la aplicación? ¿Cuáles son sus autorizaciones?
- ¿De qué manera se registra y rastrea el acceso del usuario a los datos?
- ¿Hay interfaces externas a otras aplicaciones? ¿Estas aplicaciones proporcionan un nivel equivalente de control sobre los datos?
- ¿Quién es responsable de mantener y actualizar las aplicaciones y la base de datos subyacente?
- ¿Quién responde a los problemas de seguridad potenciales y asegura que se prueben y se coloquen parches en los fallos de seguridad? ¿Quién es responsable de la seguridad general de la aplicación?
- En el desarrollo y prueba de las aplicaciones, ¿se utilizan datos de prueba? ¿A esos, se les ha proporcionado el anonimato apropiado? De no ser así, ¿los controles del entorno de prueba son equivalente a los controles del entorno de producción?

Riesgos de proceso de negocio

A pesar de los esfuerzos de los especialistas para proteger, cifrar y asegurar los datos de privacidad, el proceso de negocio, finalmente, necesitará que los datos se utilicen con el propósito expresado oportunamente. A medida que los datos se utilizan, es importante que las personas los traten con el debido nivel de cuidado que corresponde dada su clasificación. Las medidas para proteger la información impresa deben respetar los mismos principios utilizados para clasificar y proteger los datos electrónicos. Como mínimo, esas copias impresas no deben dejarse en los escritorios, los cajones y gabinetes de archivo deben estar cerrados con llave. Se debe adoptar una actitud de suma discreción en los lugares abiertos al público.

5.5 - Preparar el trabajo

Los auditores internos normalmente deben revisar el tipo de información recogida por la organización y determinar si es apropiada, revisar las metodologías de recolección y evaluar si el uso de la información recogida cumple con el propósito expresado, las leyes y las regulaciones aplicables.

La Guía 31 - Privacidad de la Asociación de Auditoría y Control de Sistemas de Información (ISACA, en inglés) hace referencia a los objetivos de control de CobiT 4.0, ME3 (Garantiza el cumplimiento de regulaciones) y DS5 (Garantiza la seguridad de los sistemas). Los objetivos de control minuciosos de la dirección con respecto al cumplimiento de regulaciones tienen que asegurar la identificación de leyes y regulaciones relevantes (ME3.1), y la evaluación de cumplimiento (ME3.3), a la vez que proporcionan aseguramiento positivo de cumplimiento (ME3.4). Los principales criterios relevantes para con la información son eficacia, cumplimiento, confidencialidad e integridad. La guía contiene una lista de verificación breve para medir el enfoque de privacidad de una organización contra los principios de la Guía de Privacidad de la OECD, así como también pasos a seguir en una auditoría relativa a la privacidad y criterios para la preparación de informes (consulte la *Figura 5.1: Secciones del programa de auditoría de privacidad*).

En diversas publicaciones se identifican enfoques para desarrollar un programa de auditoría de privacidad. En *Privacy Handbook* [Manual de Privacidad] (Marcella, 2003), se proporciona un modelo secuenciado intuitivamente para una estructura de programa de auditoría que se desarrolla sobre los criterios de la OECD y está basado en los principios de la Ley PIPEDA canadiense de 2001 emitida por la Oficina de Privacidad e Información de Ontario. En comparación, en *Assessing the Risk* [Evaluar el Riesgo] (Hargraves et al, 2003) se presenta un programa exhaustivo con una estructura más orientada a la tecnología. En Principios de Privacidad Generalmente Aceptados – Un Enfoque de Privacidad Global de 2004, de los institutos AICPA y CICA, se encuentran criterios y explicaciones detalladas sobre los 10 principios de estos institutos. En el Apéndice, se puede obtener información adicional sobre estos y otra guía de programa de auditoría.

Figura 5.1: Secciones del programa de auditoría de privacidad

- Responsabilidad.
- Identificación de propósitos.
- Recolección.
- Consentimiento.
- Uso, divulgación y retención.
- Precisión.
- Resguardos.
- Apertura.
- Acceso individual.
- Cuestionamiento al cumplimiento.

Evaluaciones de privacidad

Varios regímenes legales y de regulaciones requieren o recomiendan realizar evaluaciones de privacidad. Muchas organizaciones perciben también la necesidad operativa, impulsada por la gestión de riesgos y el control interno, de revisar la idoneidad de las políticas de privacidad y su eficacia. Los modelos de evaluación existentes proporcionan amplias pautas para establecer programas de trabajo de auditoría. Los GAPP y el Enfoque de Privacidad de AICPA y CICA, suministran un programa amplio que puede ser utilizado por cualquier organización para realizar una evaluación de privacidad. Este documento puede descargarse sin cargo del sitio www.infotech.aicpa.org/Resources/Privacy/.

Primero, se deben establecer los objetivos de una evaluación de privacidad. Por ejemplo, los objetivos pueden ser:

- Determinar los riesgos inherentes y residuales relacionados con la privacidad.
- Proporcionar aseguramiento sobre controles de riesgos de privacidad.
- Verificar la adhesión a un conjunto de normas de privacidad.

En *Data Protection Audit Manual* [Manual de Auditoría de Protección de Datos] del Comisario de Información del Reino Unido se describen los procesos generales de auditoría de privacidad: externa e interna, idoneidad y cumplimiento, vertical (funcional) u horizontal (proceso). Los auditores pueden

comenzar una evaluación determinando el alcance de las áreas de auditoría: toda la organización, una función, un proceso de negocio o una categoría de información. Una auditoría de alcance total se erige para cubrir todos los principios de privacidad. Un enfoque orientado al riesgo se centra en las áreas de riesgo clave que se deducen evaluando las dimensiones de las categorías estructurales, de proceso y de datos en función del impacto y la probabilidad de los eventos.

Los programas de trabajo listos para usar disponibles desde los órganos de supervisión, las organizaciones de la industria y los defensores de la privacidad (en el Apéndice, se puede obtener una lista de ejemplos) pueden prescribir trabajos de auditoría de cumplimiento obligatorio y generalmente proporcionan un buen punto de partida para los programas de trabajo de auditoría a medida, regulares o de una sola vez. El DEA o un delegado deben revisar o aprobar cada programa de trabajo de auditoría interna antes de que comience la auditoría de privacidad. En los casos en que un comisario de privacidad o una función equiparable tenga bajo su cargo o realice revisiones de privacidad, la auditoría interna debe revisar tanto la suficiencia de las auditorías realizadas como la eficacia del mecanismo de seguimiento implementado.

Comprender el procesamiento de los datos personales

Es importante tener en cuenta que el cumplimiento de leyes y regulaciones aplicables es un asunto esencial que se debe abordar cuando se realiza una evaluación de riesgo de privacidad amplia en una organización. Además, cuando se planifica una auditoría de privacidad, los auditores deben realizar lo siguiente:

- Obtener una comprensión integral de los datos personales que se conservan, su uso por parte de la organización, su manejo mediante tecnología y la regulación que rige sobre su procesamiento.
- Identificar las reglas que gobiernan los datos que procesa la organización.
- Entrevistar a la o las personas que tienen a su cargo la política de privacidad de la organización y su puesta en vigor para lograr comprender las leyes y regulaciones de privacidad que rigen sobre el negocio y el tipo de información que se maneja, así como también los riesgos conocidos, los controles diseñados y los incidentes informados.
- Determinar los órganos gubernamentales y de regulaciones que son responsables de hacer cumplir las reglas de privacidad. Pregúntele al director de privacidad cómo se codifican tales reglas en las políticas y procedimientos de la organización.
- Identificar los datos protegidos de clientes, empleados, socios de negocio que la organización recoge.
- Identificar cómo se comparten los datos con los terceros: los medios formales e informales mediante los cuales se comparten los datos personales dentro de la organización y con otras entidades, para poder identificar amenazas, vulnerabilidades y riesgo general para los datos.

Identificar las amenazas

Una amenaza es un actor que utiliza una vulnerabilidad para sacar provecho de un activo. A los fines de la gestión de privacidad, el activo son los datos personales protegidos. Entonces, ¿quién o cuál es la amenaza? La amenaza es la persona o el proceso que, intencionalmente o no, hace público los datos privados de la organización.

El pirata informático empleado por el crimen organizado es una imagen romántica, y puede ser una amenaza legítima. No obstante, el pirata conectado a la red, ubicado lejos del lugar, no puede hurgar en el cesto de papeles del presidente ni en el maletín del gerente, ni tampoco abrir un gabinete de archivos. Se ha verificado empíricamente que las amenazas que representan los empleados, el personal por contrato o temporario, los competidores, los programadores, los porteros y el personal de mantenimiento (todos los que a menudo tienen acceso autorizado a los depósitos de información confidencial) son las más relevantes. Sea por malicia o descuido, esas personas son las que tienen la mayor capacidad para hacer público cualquier tipo de datos de negocio. Si los datos protegidos de privacidad se comparten con socios de negocio y contratistas, se deben evaluar las amenazas adicionales dentro de sus operaciones y procesos.

Los auditores deben identificar las amenazas para con los datos de la organización utilizando actividades de investigación, *benchmarking* y tormenta de ideas para luego clasificarlas según su probabilidad de ocurrencia e impacto. Si tienen éxito en esta tarea, este esfuerzo genera una matriz que correlaciona los riesgos con el activo de privacidad (vea la *Figura 5.2: Matriz de evaluación de auditoría de privacidad*). Al asignar un valor a las amenazas y a los activos, se pone de relieve dónde deben estar las contramedidas y los controles más sólidos, además de las áreas donde los auditores deben centrarse para identificar vulnerabilidades.

Identificar los controles y contramedidas

Para determinar qué hace la organización para proteger los datos personales de las peores amenazas, los auditores deben explorar a fondo los controles activos utilizados en el programa de privacidad de la organización. Los pasos comunes para

Figura 5.2: Matriz de evaluación de auditoría de privacidad

Activo	Amenaza	Impacto	Controles	Trabajo de auditoría	Conclusión
Aplicación	Pérdida	Financiero	Preventivos	Pruebas	Control correcto
Base de datos	Daño	Reputación	Compensatorios	Entrevistas	Se requiere mejora
Tipo de archivo	No disponible	Cumplimiento	De detección	Observación	Control inadecuado
Relaciones	Divulgación	Operativo	...	...	
...	...	...	...	...	Los modelos de madurez pueden proporcionar una alternativa

identificar tales controles son:

- **Solicitar y revisar la documentación.** Revise el programa de privacidad tal como está implementado en las políticas, los procedimientos y los memorandos. ¿Cómo se combinan las políticas con las áreas de alto riesgo definidas en la matriz de evaluación de auditoría de privacidad? ¿Con qué frecuencia, si se lo hace, se revisan estas políticas? ¿Incorporan la última orientación reglamentaria y legal? ¿Esta orientación es coherente en todas las divisiones de la organización? Identifique las brechas para realizar un seguimiento.
- **Entrevistar y observar el procesamiento de datos en acción.** La brecha entre la política escrita y la acción operacional puede ser significativa. Siéntese con los empleados de las primeras líneas y determine si son conscientes del impacto de sus acciones en el manejo de los datos personales. Además, determine si hay controles sin documentar implementados y si el espíritu así como la letra del programa de privacidad motivan las decisiones del personal.
- **Revisar los contratos y los contactos de terceros.** La profundidad de la revisión dependerá de cómo los contratistas y los datos que ellos manejan se clasifican en la matriz de amenazas, pero el auditor debe realizar, como mínimo, una revisión para verificar que se cumplan aunque más no sea en la letra, las leyes y regulaciones aplicables. Si en esta se incluyen cláusulas de auditoría, ¿se llevan a cabo con la frecuencia y la profundidad apropiada?

Si se utilizan los controles de un proveedor independiente, en su totalidad o conjuntamente con los controles propios de la organización, eso impactará en la capacidad de esta para alcanzar sus objetivos de controles. La falta de controles o la debilidad en su diseño, funcionamiento o eficacia pueden dar origen a episodios como la pérdida de la confidencialidad y privacidad de la información. En consecuencia, los contratos con los proveedores independientes son un elemento crítico y deben contener cláusulas para la confidencialidad y privacidad de las aplicaciones y los datos.

Prioridades

A esta altura, los potenciales riesgos de alto impacto deben estar identificados con mayor precisión, y habrá preguntas significativas sin responder. Es hora de probar los controles y las contramedidas que golpean a los activos de mayor impacto y modelar las amenazas de mayor impacto.

5.6 Realizar la evaluación

Los pasos comunes a lo largo de una auditoría se describen minuciosamente en el *Marco Internacional para la Práctica Profesional del IIA*: una vez que se comprenden los objetivos de la organización, los tipos de datos que se manejan y el marco legal, se debe desarrollar y aprobar un programa de auditoría que incluya su alcance, objetivos y oportunidad. El equipo de auditoría recogerá la información, realizará las pruebas, analizará y evaluará el trabajo de pruebas para preparar el informe y las recomendaciones.

Evaluar la gestión de privacidad

Los institutos AICPA y CICA desarrollaron una serie de criterios para cada uno de los 10 principios de privacidad incluidos en el enfoque de los GAPP. Como ejemplo, el principio de gestión (vea la *Figura 5.3: Criterios de gestión de privacidad de AICPA/CICA*) se puede utilizar para revisar y evaluar la eficacia de la gestión de privacidad dentro de una organización. El principio requiere que una entidad defina, documente, comunique y asigne la responsabilidad por sus políticas y procedimientos de privacidad. Para evaluar la gestión de privacidad, los auditores internos deben revisar las políticas y las comunicaciones así como los procedimientos y controles.

Figura 5.3: Criterios de gestión de privacidad de AICPA/CICA

Principio 1: La entidad define los documentos, comunica y asigna responsabilidad por sus políticas y procedimientos de privacidad.

Políticas y comunicaciones
- Políticas de privacidad.
- Comunicación al personal interno.

Procedimientos y controles
- Revisión y aprobación.
- Coherencia de las políticas y los procedimientos de privacidad con las leyes y regulaciones.
- Coherencia de los compromisos con las políticas y procedimientos de privacidad.
- Gestión de infraestructura y sistemas.
- Recursos de respaldo.
- Calificaciones del personal.
- Cambios en los entornos de negocio y regulaciones.

Metodologías del trabajo de prueba

Una vez que se evaluaron los controles generales de gestión, debe quedar en claro cuál es el trabajo de pruebas necesario. Los potenciales métodos de prueba, más allá de las técnicas usualmente aplicadas, son las evaluaciones de vulnerabilidad y pruebas de penetrabilidad, las pruebas de control físico o las pruebas de ingeniería social.

Evaluaciones de vulnerabilidad y pruebas de penetrabilidad

Estos métodos, con frecuencia, se citan como métodos de aseguramiento para las aplicaciones e infraestructura de acceso a la red. Los consultores, muchas veces, utilizan términos audaces como "equipo de tigres" o "piratas de la ética" para describir esta metodología de identificar y aprovechar servicios vulnerables en un entorno de producción.

Las evaluaciones de vulnerabilidad generalmente se centran en identificar potenciales vulnerabilidades en los sistemas de información. Identifican y establecen prioridades entre las vulnerabilidades detectadas en la configuración, administración y arquitectura de los sistemas de información. Las pruebas de penetrabilidad llevan las evaluaciones de vulnerabilidad un escalón más arriba y sacan provecho de las vulnerabilidades identificadas. Las pruebas de penetrabilidad generalmente requieren de un mayor grado de habilidad técnica y pueden potencialmente interrumpir los sistemas de producción. Las evaluaciones de vulnerabilidad y pruebas de penetrabilidad requieren de un conjunto de habilidades que el auditor interno deberá adquirir, sea mediante contrato o capacitación. Una

excelente guía del tema es el *Manual de la Metodología Abierta de Pruebas de Seguridad* del Instituto para la Seguridad y las Metodologías Abiertas (ISECOM, en inglés).

Pruebas de control físico

La información protegida no está limitada a los datos digitales. Si su amenaza modelada tiene acceso al edificio, no habrá cifrado, ni filtros de seguridad, ni bases de datos con parches en el mundo que puedan impedir que el individuo pesque información impresa de la basura u obtenga acceso a datos a través de estaciones de trabajo que no tienen su acceso bloqueado. Las actividades como rebuscar en la basura para obtener información protegida, identificar estaciones de trabajo desatendidas en las cuales se inició sesión, y revisar el almacenamiento y los procesos de manejo de información de seguridad pueden servir para identificar vulnerabilidades en el manejo de la información privada. Este tipo de pruebas puede servir para responder a preguntas como las siguientes:

- ¿La información privada se desecha según la política y los procedimientos?
- ¿Los documentos se almacenan de manera segura antes de su eliminación o de pasarlos por la trituradora de papel?
- ¿Los documentos de trabajo que contienen datos privados se guardan de manera segura?
- ¿Los documentos o los monitores que exhiben información confidencial están a la vista de personal no autorizado?
- ¿Las estaciones de trabajo se bloquean por seguridad cuando están desatendidas?
- ¿La aplicación de controles de privacidad es coherente en los diversos departamentos?

Pruebas de ingeniería social

La ingeniería social es la técnica de obtener acceso no autorizado a través de una decepción no técnica. En el campo de probar un programa de privacidad, la ingeniería social se puede utilizar para probar la eficacia de los controles con respecto a la liberación de datos privados. En otras palabras, ¿puede un individuo obtener datos personales con simplemente solicitarlos? El auditor puede hacerse pasar por un ejecutivo, administrador de red u otro usuario autorizado e intentar obtener, mediante "engaños" o "zalamerías", las contraseñas o la información privada embaucando a los empleados que actúan como contramedidas clave. Las pruebas de ingeniería social pueden ayudar a responder a algunas de las siguientes preguntas de auditoría:

- ¿Cuán eficaces son los programas de capacitación y toma de conciencia respecto de la privacidad de la organización?
- ¿El equilibrio entre servicios al cliente y restricción de información es apropiado?
- ¿El programa de privacidad está respaldado por la cultura corporativa?

Las organizaciones tiene actitudes diferentes respecto al embacaumiento para con los empleados por parte de los auditores internos, por lo tanto, construya un modelo de amenaza e identifique las vulnerabilidades cuidadosamente. Analice el proceso con los equipos de recursos humanos y asuntos legales para asegurarse de que los resultados se utilizarán para mejorar las prácticas de privacidad y no para despedir a los empleados ocasionales con los que se realizó la prueba.

5.7 Comunicar y supervisar los resultados

En conformidad con la Norma 2400 del IIA: Comunicación de resultados, después de una asignación de auditoría de privacidad, se debe emitir un informe de auditoría para el cliente. Luego, el DEA debe supervisar el estado de las mejoras de implementación acordadas por el cliente de auditoría en el informe.

Muchas evaluaciones de privacidad son evaluaciones de programas de cumplimiento, y el auditor debe consultar al asesor legal para saber si, en las comunicaciones de auditoría, debe incluir las violaciones potenciales. La consulta y coordinación con el asesor legal puede reducir el probable conflicto entre las responsabilidades del auditor para documentar los resultados del trabajo y la obligación legal del asesor de defender a la organización.

Algunos de los desafíos específicos referidos a la comunicación de los resultados de una auditoría de privacidad son los siguientes:

- Lograr que se involucren todos los participantes. Un programa de privacidad eficaz debe ser puesto en práctica por casi todas las áreas de la organización. Asegúrese de que los participantes clave hagan su aporte.
- Desarrollar un lenguaje común, comprensible para describir los riesgos.
- Asegurarse de que el asesor legal interno haya revisado el plan de auditoría propuesto y bosquejar un informe de auditoría antes de su emisión para verificar que determinadas consideraciones de cumplimiento sean abordadas adecuadamente.

Las Normas 2500 y 2600 del IIA, así como la Norma 8 de la ISACA, establecen que a continuación de una auditoría, es necesario realizar un seguimiento de las acciones de la dirección o de la aceptación del riesgo para garantizar la mitigación eficaz del riesgo organizacional.

5.8 La privacidad y la gestión de auditoría

EL *Marco Internacional para la Práctica Profesional* del IIA recuerda a los auditores que deben tener en cuenta las regulaciones y riesgos de privacidad cuando planifican, realizan e informan sobre las asignaciones de aseguramiento y consultoría. Los órganos profesionales, los legisladores y las autoridades de supervisión emiten una amplia variedad de guías y regulaciones.

Debido al riesgo cada vez mayor de daños en la reputación y litigios, el DEA debe tener en cuenta un espectro significativo de problemas de privacidad y sus ramificaciones cuando gestiona la función de auditoría. Las áreas clave de inquietud son los procesos de gestión de personal, la planificación de auditoría, la recolección, manejo y almacenamiento de información al efectuar y comunicar los resultados de auditoría y las potenciales fugas de datos. La Sección 8 de la Guía 31 – Privacidad, de la ISACA, también enumera controles genéricos y áreas de inquietud, a la vez que incluye criterios útiles que el DEA debe utilizar cuando gestiona la función de auditoría.

Una organización debe utilizar el debido cuidado cuando delega autoridad discrecional sustancial a las personas. Cuando se evalúa a los postulantes a un empleo de cualquier nivel, se deben tomar todos los recaudos necesarios para asegurar que la empresa no viole ningún derecho de privacidad de los postulantes y empleados.

Cuando se contrata a auditores, existe una necesidad aún mayor de diligencia debida para garantizar que los auditores recientemente contratados actúen en conformidad con las leyes y políticas relevantes en todos los casos en los que utilicen

información personal en sus trabajos de consultoría o aseguramiento. Los auditores internos deben comprender que puede ser inapropiado, y en algún caso hasta ilegal, obtener acceso, recuperar, revisar, manipular o utilizar información personal durante la realización de los trabajos de auditoría interna. En la Figura 5.4: ¿Qué puede salir mal? Advertencias para los DEA, se enumeran ejemplos de potenciales escollos. Antes de iniciar una auditoría, los auditores deben investigar estos problemas y solicitar el asesoramiento de los asesores legales internos, de ser necesario. Por último, cuando los auditores comunican información hacia afuera de la organización, deben tener en cuenta regulaciones, requerimientos reglamentarios y consideraciones legales referidas a privacidad.

Figura 5.4: ¿Qué puede salir mal? Advertencias para los DEA

- Un control informal de antecedentes con el ex empleador de un nuevo empleado contratado se considera ilegal.
- Los riesgos de privacidad se cubren de manera insuficiente en la planificación anual del departamento de auditoría.
- En el aeropuerto, un miembro del personal embarca su equipaje con una computadora portátil en su interior.
- Los registros de recursos humanos se almacenan sin cifrar en una unidad de red del área local (LAN) del departamento.
- Un empleado renuncia y se lleva una copia de la base de datos de auditoría.
- Se roban una computadora portátil del equipaje de un empleado en una habitación de hotel.
- En el aeropuerto, desvalijan el equipaje de un auditor que contenía datos confidenciales.
- Se roban un disco duro con información personal de una computadora de la oficina de personal.
- En el espacio de trabajo del auditor, hay una pila de archivos de recursos humanos.

GTAG — Las 10 preguntas principales que debe formular el DEA — 6

1. ¿Qué leyes y regulaciones tienen impacto en la organización?
2. ¿Qué tipo de información personal recoge la organización?
3. ¿Tiene la organización políticas y procedimientos de privacidad con respecto a la recolección, el uso, la retención, la destrucción y la divulgación de la información personal?
4. ¿Tiene la organización asignadas la responsabilidad y la obligación de rendir cuenta por la gestión de un programa de privacidad?
5. ¿Sabe la organización dónde se almacena toda la información personal?
6. ¿Cómo se protege la información personal?
7. ¿Hay alguna información personal que recoge la organización que se revele a terceros?
8. ¿Están los empleados apropiadamente capacitados en el manejo de temas y preocupaciones respecto a privacidad?
9. ¿Tiene la organización recursos adecuados para desarrollar, implementar y mantener un programa de privacidad efectivo?
10. ¿Completa la organización una evaluación periódica para asegurarse de que las políticas y los procedimientos de privacidad se respetan?

7.1 Otras normas de auditoría y metodologías

Guía de la ISACA

Una guía relacionada con la privacidad se puede encontrar en:

- CobiT 4.0 ME3 - Garantiza el cumplimiento de regulaciones.
- CobiT 4.0 DS5 - Garantiza la seguridad de los sistemas.
- Guía 31 de la ISACA - Privacidad.
- CobiT 3.2 Pautas de auditoría - PO8.

Guía de AICPA/CICA

Los GAPP de AICPA/CICA constituyen un enfoque amplio con criterios que las organizaciones pueden utilizar para implementar, administrar o evaluar con eficacia sus programas de privacidad. Cada uno de los 10 principios siguientes está respaldado por criterios objetivos y medibles que están dentro del enfoque:

1. **Dirección**: La entidad define, documenta, comunica y asigna responsabilidad por sus políticas y procedimientos de privacidad.
2. **Aviso**: La entidad comunica sus políticas y procedimientos de privacidad, a la vez que identifica los propósitos para los que recoge, utiliza, retiene y divulga la información personal.
3. **Elección y consentimiento:** La entidad describe las elecciones disponibles para el individuo y obtiene consentimiento implícito o explícito con respecto a la recolección, el uso y la divulgación de la información personal.
4. **Recolección:** La entidad recoge la información personal únicamente para los propósitos identificados en el aviso.
5. **Uso y retención:** La entidad limita el uso de la información personal a los propósitos identificados en el aviso y para los que el individuo ha proporcionado su consentimiento implícito o explícito. La entidad retiene la información personal únicamente por el tiempo que sea necesario para completar los propósitos establecidos.
6. **Acceso:** La entidad proporciona acceso a los individuos a su información personal para su revisión y actualización.
7. **Divulgación a terceros:** La entidad revela la información personal a terceros únicamente para los propósitos identificados en el aviso y con el consentimiento implícito o explícito del individuo.
8. **Resguardo de la privacidad:** La entidad protege la información personal contra el acceso no autorizado (tanto físico como lógico).
9. **Calidad:** La entidad mantiene información personal precisa, completa y relevante para los propósitos identificados en el aviso.
10. **Supervisión y puesta en vigor:** La entidad supervisa el cumplimiento de las políticas y los procedimientos de privacidad, y tiene procedimientos para abordar los reclamos y disputas referidos a la privacidad.

Criterios del principio de gestión de AICPA/CICA

El principio de gestión de AICPA/CICA respalda la evaluación de las prácticas de gestión de privacidad de una organización. El documento completo con los 10 principios y criterios está disponible para su descarga sin cargo en infotech.aicpa.org/Resources/Privacy.

Principio de gestión

La entidad define, documenta, comunica y asigna responsabilidad por sus políticas y procedimientos de privacidad.

Criterios de gestión de privacidad:

1.1. Políticas y comunicaciones

1.1.0 Políticas de privacidad

- La entidad define y documenta sus políticas de privacidad con respecto a:
- Aviso.
- Elección y consentimiento.
- Recolección.
- Uso y retención.
- Acceso.
- Transferencia hacia adelante y divulgación.
- Seguridad.
- Calidad.
- Supervisión y puesta en vigor.

1.1.1 Comunicación al personal interno

Las políticas de privacidad y las consecuencias de su incumplimiento se deben comunicar, como mínimo anualmente, al personal interno de la entidad responsable de recoger, utilizar, retener y divulgar la información personal. Los cambios en esas políticas se deben comunicar a dicho personal poco después de que se hayan aprobado los cambios.

1.1.2 Responsabilidad y obligación de rendir cuenta por las políticas

La responsabilidad y la obligación de rendir cuenta están asignadas a una persona o grupo para que documente, implemente, ponga en vigor, supervise y actualice las políticas de privacidad de la entidad. Los nombres de tales personas o grupos junto con sus responsabilidades deben comunicarse al personal interno.

1.2 Procedimientos y controles

1.2.1 Revisión y aprobación

Las políticas y procedimientos de privacidad, y los cambios al respecto, son revisados y aprobados por la dirección.

1.2.2 Coherencia de las políticas y los procedimientos de privacidad con las leyes y regulaciones

Las políticas y el procedimiento se revisan y se comparan con los requerimientos de leyes y regulaciones aplicables como mínimo anualmente, y siempre que estas sufran cambios. Las políticas y los procedimientos de privacidad se revisan para satisfacer los requerimientos de leyes y regulaciones aplicables.

1.2.3 Coherencia de los compromisos con las políticas y procedimientos de privacidad

El personal o los asesores de la entidad revisan los contratos para determinar su consistencia con las políticas y procedimientos de privacidad, y abordan las inconsistencias.

1.2.4 Infraestructura y gestión de sistemas

El personal o los asesores de la entidad revisan el diseño, la adquisición, el desarrollo, la implementación, la configuración y la gestión de:

- infraestructura,
- sistemas,
- aplicaciones,
- sitios Web, y
- procedimientos,

y los cambios al respecto para lograr coherencia con las políticas y los procedimientos de privacidad de la entidad, además de abordar las inconsistencias.

1.2.5 Recursos de respaldo

Los recursos son proporcionados por la entidad para implementar y respaldar sus políticas de privacidad.

1.2.6 Calificaciones del personal

La entidad establece las calificaciones que debe tener el personal responsable de proteger la privacidad y la seguridad de la información personal, y asigna esas responsabilidades sólo a aquellos que satisfacen tales calificaciones y que han recibido la capacitación necesaria.

1.2.7 Cambios en los entornos de negocio y regulaciones

Para cada jurisdicción en la que opera la entidad, se identifica y aborda el efecto de los cambios sobre la privacidad en los siguientes factores:

- operaciones y procesos de negocio.
- personas.
- tecnología.
- legal.
- contratos, incluidos los acuerdos de nivel de servicio. Las políticas y los procedimientos se actualizan para tales cambios.

7.2 Monografías seleccionadas

AICPA/CICA: *Generally Accepted Privacy Principles – A Global Privacy Framework* (2006)

Carey: *Data Protection: A Practical Guide to UK and EU Law* (Oxford University Press, 2004)

Cate: *Privacy in the Information Age* (Brookings, 2001)

CICA: *20 Questions Directors Should Ask About Privacy* (CICA, 2002)

CICA: *Privacy Compliance: A Guide for Organizations & Assurance Practitioners* (CICA, 2004)

Hargraves et al: *Privacy – Assessing the Risk* (IIA RF, 2003)

Karol, T.J.: *A Guide to Cross-border Privacy Assessments* (ITGI, 2001)

Marcella/Stucki: *Privacy Handbook* (Wiley, 2003)

Margulis: *Contemporary Perspectives on Privacy: Social, Psychological, Political* (Blackwell, 2003)

OECD: *Privacy Online. OECD Guidance on Policy and Practice* (OECD, 2003)

Solove/Rotenberg/Schwartz: *Information Privacy Law* (Aspen, 2005)

Westby, Jody R. (Ed.): *International Guide to Privacy* (ABA, 2004)

7.3 Recursos gubernamentales regionales y globales

Consejo de Europa
www.coe.int/t/e/legal_affairs/legal_cooperation/data_protection
El 28 de enero de 1981, se abrió para su firma la "Convención para la protección de las personas respecto del procesamiento automático de datos personales"del Consejo de Europa. Al día de hoy, sigue siendo el único instrumento legal internacional vinculante con un alcance de aplicación mundial en este campo. Está abierta para que adhiera cualquier país, incluso aquellos que no son miembros del Consejo de Europa.

Páginas de protección de datos de la Comisión Europea
www.europa.eu.int/comm/justice_home/fsj/privacy
El desarrollo del mercado interno y de la así llamada "sociedad de la información" aumenta el flujo transfronterizo de los datos personales entre los estados miembro de la UE. Para eliminar los obstáculos potenciales a tales flujos y para asegurar un alto nivel de protección dentro de la UE, se ha armonizado la legislación de protección de datos. Este sitio Web proporciona vínculos a los grupos expertos de la UE y a los comisarios de privacidad nacional.

Páginas de privacidad y seguridad de la información de la OECD
www.oecd.org/sti/security-privacy
La parte de la OECD que trabaja en seguridad y privacidad de la información impulsa un enfoque coordinado global para la formulación de políticas en estas áreas a fin de ayudar a generar confianza en línea.

Generador de declaración de privacidad de la OECD
www.oecd.org/sti/privacygenerator
El Generador, que ha sido aprobado por 30 países miembro de la OECD, ofrece pautas sobre el cumplimiento de las Guías de Privacidad y ayuda a las organizaciones a desarrollar políticas y declaraciones de privacidad.

7.4 Recursos reginales y nacionales

Consulte *ITAudit* para saber más sobre el Comité de Privacidad de Información de Salud y Servicios Humanos de EE. UU.
www.aspe.hhs.gov/datacncl/privacy
El Comité de Privacidad de Información de Salud y Servicios Humanos de EE. UU. garantiza la atención de la privacidad como consideración fundamental en la recolección y utilización de la información personal identificable.

Iniciativas de privacidad de la Comisión Federal de Comercio de EE. UU.
www.ftc.gov/privacy/index.html
La privacidad es un elemento central de la misión de protección al consumidor de la Comisión Federal de Comercio (FTC, en inglés). La FTC educa a los consumidores y al sector de negocios sobre la importancia de la privacidad de la información personal, incluida la seguridad de la información personal.

Proyecto de privacidad de información de salud en EE. UU.
www.healthprivacy.org
El Proyecto de privacidad de información de salud se centra en despertar la conciencia del público respecto de la importancia de asegurar la privacidad de la información de salud para mejorar el acceso y la calidad de los servicios de salud, tanto a nivel individual como de la comunidad.

Páginas de la Ley de Responsabilidad y Portabilidad del Seguro de Salud (HIPAA, en inglés) de la Oficina para los Derechos Civiles del Departamento de Salud y Servicios Humanos de EE. UU.
www.hhs.gov/ocr/hipaa
Las páginas de privacidad de la información médica de la Oficina para los Derechos Civiles del Departamento de Salud y Servicios Humanos de EE. UU contienen información sobre las normas nacionales para proteger la privacidad de la información de salud personal.

Páginas de la Ley HIPAA, Institutos Nacionales de Salud de EE. UU.
http://privacyruleandresearch.nih.gov
El organismo Institutos Nacionales de Salud, que forma parte del Departamento de Salud y Servicios Humanos de EE. UU., es el punto central federal de la investigación médica en Estados Unidos. Proporciona normas para la privacidad de la información de salud identificable individualmente, Regla Final.

7.5 Organizaciones profesionales y sin fines de lucro

Profesionales Informáticos pro-Responsabilidad Social (CPSR, en inglés)
www.cpsr.org
El centro CPSR es una organización global que promociona el uso responsable de la tecnología informática. Fue fundado en 1981 y desde entonces educa a los formuladores de políticas y al público en una amplia gama de temas. Ha incubado numerosos proyectos tales como Privaterra, Public Sphere Project, Centro de Información de Privacidad Electrónica (EPIC, en inglés), 21st Century Project, Civil Society Project, y la Conferencia sobre Computadoras, Libertad y Privacidad. El CPSR fue originalmente fundado por científicos informáticos de EE. UU. y hoy tiene miembros en más de 30 países en seis continentes.

Centro de Información de Privacidad Electrónica (EPIC, en inglés)
www.epic.org
El centro EPIC es un centro de investigación de interés público ubicado en Washington, D.C. Se estableció en 1994 para centrar la atención pública en temas de libertades civiles emergentes y para proteger la privacidad, la Primera Enmienda de EE. UU. y los valores constitucionales.

Equipo de Trabajo de Privacidad de AICPA/CICA
http://infotech.aicpa.org/Resources/Privacy
Los institutos AICPA y CICA han formado el Equipo de Trabajo de Privacidad de AICPA/CICA, que a su turno desarrollaron los Principios de Privacidad Generalmente Aceptados – Un Enfoque de Privacidad Global.

Alianza para la Privacidad en Línea
www.privacyalliance.org
La Alianza para la Privacidad en Línea lidera y respalda iniciativas de autorregulaciones para crear un entorno de confianza que propicie la protección de la privacidad, en línea y en el comercio electrónico, de los individuos.

Conferencia Internacional sobre Protección de Datos y Comisarios de Privacidad
www.privacyconference2005.org
Este sitio describe las características de la Conferencia Internacional sobre Protección de Datos y Comisarios de Privacidad.

PrivacyExchange
www.privacyexchange.org
PrivacyExchange es un recurso global en línea para la protección de datos y de la privacidad del consumidor. Contiene una biblioteca de leyes de privacidad, prácticas, publicaciones, sitios Web y otros recursos referidos a privacidad del consumidor, y desarrollos de protección de datos en todo el mundo.

Recurso de privacidad de Japón
www.privacyexchange.org/japan/japanindex.html
El Recurso de Privacidad de Japón ha sido diseñado y lanzado como un servicio gratuito para todos aquellos comprometidos

con los debates sobre privacidad.

Privacy International
www.privacyinternational.org
Privacy International (PI) es un grupo de derechos humanos formado en 1990 como organismo de control en temas de supervisión e invasión de privacidad por parte de los gobiernos y las corporaciones. PI tiene su sede central en Londres y una oficina en Washington, D.C. PI ha realizado diversas campañas y trabajos de investigación en todo el mundo.

Plataforma para Proyectos de Preferencia de Privacidad (P3P, en inglés)
www.w3c.org/p3p/
P3P es una norma desarrollada por W3C que proporciona un medio simple y automatizado para que los usuarios tengan más control del uso de su información personal en los sitios Web que visitan. La P3P mejora el control, por parte del usuario, al colocar las políticas de privacidad en lugares donde los usuarios pueden encontrarlas, en un formato que pueden comprender, y más importante aún, les permite actuar sobre lo que ven.

7.6 Más recursos disponibles en Internet

Foro de Cooperación Económica Asia-Pacífico (APEC, en inglés)
www.apec.org
El Enfoque de Privacidad de APEC fomenta un enfoque coherente para proteger la privacidad de la información entre las economías de los miembros de APEC, al mismo tiempo evita crear barreras innecesarias en los flujos de información.

Instituto Canadiense de Contadores Certificados (CICA, en inglés)
www.cica.ca
El CICA ha lanzado una iniciativa de privacidad amplia para despertar la toma de conciencia acerca de los temas de privacidad entre sus miembros y el sector de negocios. Esta iniciativa abarca el desarrollo de recursos para educar a ambos, miembros y sector de negocios, sobre los beneficios de las buenas prácticas de privacidad.

Consumers International
www.consumersinternational.org
Consumers International defiende los derechos de todos los consumidores a través de su apoyo a los grupos nacionales de consumidores y realizando campañas en el ámbito internacional.

Supervisor Europeo de Protección de Datos
www.edps.eu.int
Es una autoridad de supervisión independiente que tiene la responsabilidad de supervisar el procesamiento de datos personales por parte de las instituciones y órganos de la Comunidad Europea.

Cámara Internacional de Comercio (ICC, en inglés)
www.iccwbo.org
Los líderes y expertos de negocio extraídos de la lista de socios de la ICC establecen posiciones de negocio clave, políticas y prácticas en cuanto a comercio electrónico, tecnologías de la información y telecomunicaciones a través de la Comisión de Comercio Electrónico, TI y Telecomunicaciones.

Instituto para la Seguridad y las Metodologías Abiertas (ISECOM, en inglés)
www.isecom.org/osstmm
Este instituto proporciona el Manual de la Metodología Abierta de Pruebas de Seguridad.

Organismo Estatal de Política de Calidad de Vida, Oficina de Gabinete, Gobierno de Japón
www5.cao.go.jp/seikatsu/index.html
Este organismo proporciona detalles de la legislación de protección de la información personal e información relacionada, así como también un despacho de asesoría sobre información personal.

Corporación Japonesa del Desarrollo de Procesamiento de Información (JIPDEC, en inglés)
www.privacymark.org
Sus actividades en el campo de la privacidad y la seguridad abarcan la operación de un sistema para otorgar sellos de protección de datos personales y de privacidad.

Oficina del Comisario de Privacidad
www.privacy.gov.au
La oficina del Comisario de Privacidad del gobierno de Australia es una organización independiente que fomenta una cultura australiana de respeto a la privacidad.

Asociación Internacional de Profesionales de Privacidad (IAPP, en inglés)
www.privacyassociation.org
Es una asociación que reúne a los profesionales de privacidad y seguridad. Define y apoya la profesión al proporcionar un foro para la interacción, la educación y el debate. La IAPP emite una designación como Profesional Certificado en Privacidad de la Información .

Comisario de Privacidad de Canadá
www.privcom.gc.ca
El Comisario investiga los reclamos y realiza auditorías, publica información sobre prácticas de manejo de la información personal en los sectores privado y público, efectúa investigaciones en temas de privacidad, y fomenta la toma de conciencia y clara comprensión de los asuntos de privacidad.

Taller 2000 de Tecnologías de Privacidad en Línea de la Administración Nacional de Telecomunicaciones e Información (NTIA, en inglés)
www.ntia.doc.gov/ntiahome/privacy
La NTIA de EE. UU. organizó un taller público para examinar las herramientas y desarrollos tecnológicos que pueden mejorar la privacidad del consumidor en línea.

7.7 Glosario de términos

Acceso	Con respecto a la privacidad, es la capacidad del individuo de ver, modificar y cuestionar la exactitud e integridad de la información personal identificable que se ha recogido acerca de su persona.
Activo de información	Información en cualquier formato (por ejemplo, escrita, verbal o electrónica) a la que la organización le adjudica un valor medible. Aquí se incluye información creada por el controlador de datos, recogida por este o almacenada por el procesador de datos para los terceros externos.
Anonimato	Condición en la que no se conoce la verdadera identidad de una persona.
Archivo computarizado	Conjunto de información personal almacenada o procesada mediante un sistema automatizado.
Archivo manual	Recolección de la información personal almacenada en medios no computarizados.
Autenticación	Acto por el cual se verifica la identidad de una entidad del sistema (por ejemplo, usuario, sistema, nodo de red) y su elegibilidad para obtener acceso a la información computarizada. Su propósito es proteger contra actividades fraudulentas de control de inicio de sesión. La autenticación también se puede referir a la verificación de la idoneidad de un dato individual.
Autorización	Aprobación de una transacción o acción por parte del nivel apropiado de la dirección.
Autorregulación	Regulación, por parte de las organizaciones, de las actividades de sus afiliados.
Aviso	Informe enviado a las personas sobre las políticas o prácticas de datos de una entidad, antes de recoger su información personal.
Biométrica	Técnica de seguridad que verifica la identidad de una persona analizando un atributo físico único, como por ejemplo la huella de la mano.
Combinación de datos	Actividad que implica la comparación de datos personales obtenidos de una variedad de fuentes a los fines de tomar decisiones sobre las personas a quienes pertenecen los datos.
Comisario de privacidad	Cuerpo independiente que supervisa las prácticas de privacidad gubernamentales y, eventualmente, las del sector privado.
Conjunto de datos	Datos que se combinan sin divulgar la información personal identificable.
Consentimiento	Acuerdo que una persona otorga a la entidad para que recoja, utilice y revele la información personal de conformidad con el aviso de privacidad. Dicho acuerdo puede ser explícito o implícito. El consentimiento explícito se otorga verbalmente o por escrito, es inequívoco y no requiere ninguna inferencia por parte de la entidad que desea obtener tal consentimiento. El consentimiento implícito puede ser razonablemente inferido por la acción o inacción del individuo. (Consulte las modalidades de inclusión y exclusión más abajo).
Control	Política, manual o procedimiento computarizado diseñado para proporcionar aseguramiento razonable respecto al logro de los objetivos con eficacia y eficiencia de las operaciones, la confiabilidad de los informes financieros y el cumplimiento de leyes y regulaciones aplicables.
Controlador de datos	Organizaciones o funciones que controlan el acceso a la información personal y el procesamiento de ella.
Convenio de Puerto Seguro	Convenio entre Estados Unidos y la UE respecto a transferencia de información personal identificable desde la UE a Estados Unidos. El Convenio de Puerto Seguro es coherente con las Prácticas Honestas de Información. Las empresas que se registran ante el Departamento de Comercio de EE. UU. como Puerto Seguro y aceptan regirse en función del convenio, son consideradas por la UE como empresas que proporcionan una protección de datos adecuada a la información personal identificable que se transfiere desde la UE a Estados Unidos.
Convertir en anonimato	Datos previamente identificables se tornan no identificables cuando se les retira un código u

	otro vínculo que identifica al sujeto de datos.
Cumplimiento	Cumplimiento de políticas, procedimientos, guías, leyes, regulaciones y acuerdos contractuales a los que está sujeto el proceso de negocio.
Datos de preferencia	Datos acerca de los gustos y las cosas que no le gustan a una persona.
Datos de ubicación	Información que se puede utilizar para identificar la ubicación física del individuo en ese momento o para rastrear sus cambios de ubicación.
Datos personales (información personal, información personal identificable)	Información sobre una persona identificada o identificable, incluye datos fácticos o subjetivos, registrados o no, en cualquier formato.
Declaración de privacidad	Documento que describe la posición de una organización respecto a la privacidad detallando qué información recoge, con quién comparte los datos y de qué manera los usuarios pueden controlar el uso de sus datos personales.
Derechos de privacidad	Capacidad legal de una persona para impulsar acciones específicas o realizar solicitudes con respecto a los usos y divulgaciones de su información.
Director de privacidad	Función interna que tiene a su cargo la implementación y supervisión del programa de privacidad de la organización. Por lo general, esta función es el punto central para solicitudes externas, reclamos y órganos de supervisión.
Director de Privacidad	Persona a la que se le asigna la tarea de asegurar que los datos personales de un controlador de datos se guarden en forma segura, y más importante aún, que se mantengan altos niveles de satisfacción del cliente.
Disponibilidad	Aseguramiento de que cuando sea necesario, las personas que lo necesiten, obtendrán acceso a los sistemas encargados de entregar, almacenar y procesar la información y que esta será de una integridad aceptable.
Divulgación	Liberar, transferir, transmitir, suministrar el acceso a datos personales o transportar los datos personales de un individuo o entidad fuera del controlador de datos.
Eficacia	Objetivo de control que especifica que la información debe ser relevante y pertinente al proceso de negocio, se debe entregar oportunamente, de manera correcta, coherente y debe ser utilizable.
Eficiencia	Objetivo de control que atañe al suministro de información a través del uso más productivo y económico de los recursos.
Entitidad	Organización que recoge, utiliza, retiene y divulga la información personal.
Etiquetado	Etiquetar a los fines de identificación y rastreo.
Evaluación del impacto de la privacidad	Un análisis de cómo se maneja la información: (i) para asegurar que el manejo se realice conforme a la legislación y normativa aplicables, y a los requerimientos de políticas referidas a privacidad; (ii) para determinar los riesgos y los efectos de recolectar, mantener y distribuir la información de una forma identificable en un sistema de información electrónico y (iii) para examinar y evaluar las protecciones y los procesos alternativos para manejar la información a fin de mitigar los potenciales riesgos de privacidad.
Funcionalidad	Objetivo de control que específica que un sistema debe incluir todas las capacidades relevantes.
Identificación	Relación de la información personal con un individuo identificable.
Incidente de seguridad	Intento o concreción de acceso no autorizado, uso, divulgación, modificación o destrucción de información o interferencia con las operaciones de los sistemas en un sistema de información.
Individuo (sujeto de datos)	Persona cuyos datos personales se recogen.
Información de identificación del individuo	Dato individual o compilación de información que indica o revela la identidad de una persona, ya sea específicamente (como por ejemplo, el nombre del individuo o el número de

	seguridad social) o bien información a partir de la cual se puede averiguar razonablemente la identidad de la persona.
Información del consumidor	Información sobre las transacciones y la conducta de una persona en el mercado.
Información personal confidencial	Información personal que requiere un nivel extra de protección y debido cuidado (por ejemplo, historia clínica o de salud, origen racial o étnico, opiniones políticas, creencias religiosas, afiliación a organizaciones sindicales, información financiera o preferencia sexual).
Integridad	Propiedad de los datos respecto de que no se han alterado ni destruido de manera no autorizada.
Ley tipo "ómnibus"	Ley que se aplica en todos los aspectos.
Limitación de uso	Significa que los datos personales no se pueden revelar, ni poner a disposición, ni utilizar de alguna otra manera que no sean los propósitos especificados.
Mecanismo de reparación	Persona, proceso o agencia a quien un sujeto de datos puede acudir para obtener ayuda. Una manera de componer las pérdidas o daños.
Mediador (*ombudsman*)	Defensor o colaborador, que trabaja para solucionar problemas entre los sujetos de datos y los controladores o procesadores de datos.
Minería de datos (data mining)	Práctica de compilar, combinar y analizar la información sobre sujetos de datos que provienen de una variedad de fuentes, generalmente con fines de marketing.
Opción de exclusión	El consentimiento es implícito, y la persona debe denegarlo explícitamente si no desea que la entidad recolecte, utilice, retenga o divulgue su información personal.
Opción de inclusión	Se requiere el consentimiento explícito de la persona para que la entidad recoja, utilice, retenga o divulgue su información personal.
Política	Declaración por escrito que comunica la intención de la dirección, los objetivos, los requisitos, las responsabilidades y las normas.
Prácticas honestas de información	Conjunto de cinco principios: acceso, consentimiento, puesta en vigor, aviso y seguridad. Estos tienen su origen en la Ley de Privacidad de 1974 de EE. UU., que se diseñó para guiar a las entidades en sus prácticas de procesamiento de datos personales.
Privacidad	Derecho a vivir sin intrusiones no autorizadas.
Privacidad de la información	Derecho del individuo a controlar su información personal que está en manos de otros.
Programa de privacidad	Políticas, comunicaciones, procedimientos y controles implementados para gestionar y proteger la información personal de acuerdo con las leyes, regulaciones y mejores prácticas aplicables.
Propósito	Razón por la cual una entidad recoge información personal.
Puesta en vigor	Mecanismos que aseguran el cumplimiento y ponen a disposición los medios apropiados de recursos para las partes agraviadas (también formas de reparación).
Recolección	Reunir la información personal mediante entrevistas, formularios, informes u otras fuentes de información.
Resolución alternativa de controversias	Métodos utilizados para resolver las controversias fuera de un tribunal, como negociación, conciliación, mediación y arbitraje.
Resolución de controversias	Se incluyen todos los procesos para resolver un conflicto, desde los consensuales a los judiciales y desde las negociaciones a los litigios.
Riesgo aceptable	Nivel de riesgo que la dirección establece como aceptable para un activo de información en particular. El riesgo aceptable se basa en datos empíricos y en una opinión técnica de respaldo de que se comprende el riesgo general y de que los controles implementados sobre el activo o el entorno reducirán la posibilidad de su pérdida. Todo otro riesgo remanente se reconoce y se acepta como un tema de responsabilidad.

Robo de identidad	Uso deliberado del nombre de otra persona u otra información de su identificación, para cometer un robo, un fraude o para obtener acceso a la información confidencial de un individuo.
Salvaguarda	Tecnología, política o procedimiento que contrarresta una amenaza o protege los activos.
Seguridad	Protección de datos contra el acceso no autorizado, el uso indebido o abuso y la destrucción o corrupción de datos.
Seguridad de los datos	Protección de los datos contra modificación, destrucción o divulgación accidental o no autorizada mediante políticas, estructura organizacional, procedimientos, capacitación de toma de conciencia, software o hardware que aseguran que los datos sean exactos, que estén disponibles y que obtengan acceso a ellos sólo las personas autorizadas. Mantenimiento de la confidencialidad, integridad y disponibilidad de la información.
Sistema	Un sistema se compone de cinco principios clave organizados para alcanzar un objetivo específico. Estos son: infraestructura (instalaciones, equipos y redes), software (sistemas, aplicaciones y utilidades), personas (programadores, operadores, usuarios y gerentes), procedimientos (automatizado y manual) y datos (flujos de transacciones, archivos, bases de datos y tablas).
Sujeto de datos (individuo)	Persona cuyos datos personales se recogen.
Supervisión	Investigación sistemática o supervisión de las acciones o comunicaciones de una o más personas.
Tercerización	Uso y manejo de información personal por parte de un tercero que realiza una función de negocio para la entidad.
Tercero	Entidad no afiliada con la entidad que recoge la información personal o cualquier otra entidad afiliada que no está cubierta por el aviso de privacidad de la entidad.
Transparencia	Norma que requiere que el procesamiento de la información personal sea abierto y comprensible para la persona cuyos datos se procesan, exige que una organización informe a los usuarios qué información personal recoge y cómo se utilizan los datos.
Trazado de perfiles	Uso de los datos personales para crear o desarrollar un registro correspondiente a un sujeto de datos a los fines de compilar hábitos o información personal identificable.
Uso secundario	Usar información personal recogida para un propósito a los fines de un segundo propósito no relacionado.
Uso no rutinario	Uso de la información no a los fines para los cuales se recogió.
Voluntario	Proporciona información de manera voluntaria para su procesamiento.

7.8 Glosario de acrónimos

ADMA	Asociación Australiana de Marketing Directo
ADR	Resolución alternativa de controversias
AICPA	Instituto Americano de Contadores Públicos Certificados
ANSI	Instituto Nacional Estadounidense de Normas
APEC	Foro de Cooperación Económica Asia-Pacífico
CA	Contador certificado
CICA	Instituto Canadiense de Contadores Certificados
CobiT	Objetivos de Control de Información y Tecnología Relacionada
CoE	Consejo de Europa
COPPA	Ley de Protección de la Privacidad en Línea de los Niños
COSO	Comité de Organizaciones Patrocinadoras de la Comisión Treadway
COTS	Software comercial
CPA	Contador público certificado
CPO	Director de Privacidad
CPSR	Profesionales Informáticos pro-Responsabilidad Social
DEA	Director Ejecutivo de Auditoría
DMA	Asociación de Marketing Directo
EPIC	Centro de Información de Privacidad Electrónica
ERM	Gestión de Riesgo Empresarial
ETC	Cobro electrónico de peajes
GAPP	Principios de Privacidad Generalmente Aceptados
GLBA	Ley Gramm-Leach Bliley
GTAG	Guía de Auditoría de Tecnología Global
HIPAA	Ley de Responsablidad y Portabilidad del Seguro de Salud
IAPP	Asociación Internacional de Profesionales de Privacidad
ICC	Cámara Internacional de Comercio
IDs	Identificadores
IEC	Comisión Electrotécnica Internacional
IFAC	Federación Internacional de Contadores
IIA	Instituto de Auditores Internos
ISACA	Asociación de Auditoría y Control de Sistemas de Información
ISAE	Normas Internacionales sobre Trabajos de Aseguramiento
ISO	Organización Internacional de Normalización
ISTPA	Alianza Internacional por la Seguridad, Confianza y Protección de la Privacidad
ITGI	Instituto de Gobierno de TI
LAN	Red de área local
NTIA	Administración Nacional de Telecomunicaciones e Información
OECD	Organización para la Cooperación y el Desarrollo Económico

ONU	Organización de Naciones Unidas
OPA	Alianza para la Privacidad en Línea
P3P	Platforma para Preferenica de Privacidad
PA	Consejo para la Práctica
PET	Tecnología reforzadora de la privacidad
PI	Privacy International
PIA	Evaluación del impacto de la privacidad
PII	Información personal identificable
PIPEDA	Ley de Protección de Información Personal y Documentos Electrónicos
TI	Tecnología de la Información
UE	Unión Europea
W3C	World Wide Web Consortium

7.9 Autores, contribuyentes y revisores

Acerca de los autores

Ulrich Hahn, Ph.D., CIA, CISA, CCSA, Capacitador y consultor independiente, Suiza y Alemania
Hahn, quien obtuvo su título universitario en Ingeniería Industrial (Telecomunicaciones) de la Universidad Técnica de Darmstadt (Alemania), inicialmente se unió al sector de contabilidad global para realizar extensos trabajos de consultoría y aseguramiento para clientes del sector privado y público. Más tarde ocupó un puesto de auditoría en un importante centro de datos de servicios financieros, para luego unirse a una de las cinco firmas más importantes en prácticas de auditoría de sistemas de información. Posteriormente, trabajó en funciones de dirección de auditoría corporativa en firmas líderes del mercado global. Hahn tiene un Doctorado en el área de desarrollo de legislación internacional sobre privacidad de datos y es profesional acreditado por el IIA en evaluación y validación de calidad. También fue ganador del premio Medalla de Oro William S. Smith por lograr la calificación más alta en todas las partes del examen CIA de una sola vez. Ha sido presidente de la Confederación Europea de Institutos de Auditores Internos, vicepresidente de la ISACA de Alemania, miembro del consejo del IAI de Alemania y en la actualidad es miembro de la Comisión de Tecnología de Avanzada Internacional del IIA. Participa en diversos comités de capítulos y grupos de trabajo que se centran en prácticas profesionales, calidad, eventos y publicaciones. Hahn escribe sobre sistemas de información y asuntos de auditoría general; es orador y disertante de conferencias en dichos temas; además presta respaldo de gestión y técnico a las funciones de auditoría dentro de una red internacional de profesionales de auditoría de alto nivel muy conocidos en el ámbito. Además, dicta cursos para las certificaciones CIA, CISA y CCSA en varios países.

Ken Askelson, CIA, CPA, CITP, JCPenney Co., EE. UU.
Askelson es gerente superior de auditoría de TI de JCPenney en Plano, Texas. Supervisa al personal de auditoría de TI a cargo de auditar y supervisar las actividades de la infraestructura de TI. Sus puestos anteriores en JCPenney han sido gerente de auditoría, gerente de mercaderías y coordinador de contabilidad regional. Además, ha cumplido funciones en varios comités de la AICPA, entre ellos, el Comité Ejecutivo de TI, el Subcomité de Investigación de TI, el Subcomité de Prácticas de TI y el Comité Ejecutivo del Sector Económico y Negocios. En la actualidad, es comisario de la Comisión Nacional de Acreditaciones de AICPA, vicepresidente del Equipo de Trabajo de Privacidad de AICPA y miembro del Consejo Consultivo Editorial del Journal of Accounting. También participó en Partnership for Critical Infrastructure Security, entidad patrocinada por la Cámara de Comercio de EE. UU., y en la Oficina de Aseguramiento de Infraestructura Crítica del Departamento de Seguridad Interna. Ocupó varios puestos en los capítulos locales del IIA; en la actualidad, cumple funciones en la Comisión de Tecnología de Avanzada del IIA y fue reconocido con los galardones de "Auditor del año" y "Presidente del año" que le otorgó el capítulo del Condado de Orange (California) del IIA. Askelson posee títulos de grado en marketing y contabilidad de la Universidad del Norte de Iowa.

Robert Stiles, CISA, CFE, Texas Guaranteed, EE. UU.
Stiles es auditor superior de tecnología de Texas Guaranteed (TG), una corporación pública sin fines de lucro. En 1989 ingresó a Texas Guaranteed y desde entonces ha ocupado diversos puestos, entre ellos, analista de cumplimiento, investigador y auditor de tecnología. Sus actividades de auditoría se centran en los temas de privacidad, seguridad, redes y aplicaciones de Internet. Ha realizado evaluaciones de vulnerabilidad en la red externa, la red interior y la seguridad física de TG.

Contribuyentes

Sean Ballington, PricewaterhouseCoopers LLP, EE. UU.
Nancy Cohen, AICPA, EE. UU.
Heriot Prentice, The IIA Inc.
Kyoko Shimizu, PricewaterhouseCoopers, Japón

Revisores

La Comisión de Tecnología de Avanzada del IIA, filiales mundiales del IIA, AICPA, el Centro encargado de Seguridad en Internet, el Instituto de Ingeniería de Software de la Universidad de Carnegie Mellon, la Asociación de Seguridad de Sistemas de Información, IT Process Institute, la Asociación Nacional de Directores Corporativos y el Instituto SANS participaron en el proceso de revisión. El IIA agradece a las siguientes personas y organizaciones que brindaron valiosos comentarios que agregaron gran valor a esta guía:

- Equipo de Trabajo de Privacidad de AICPA/CICA
- David F. Bentley, Consultor, Reino Unido
- Lily Bi, The IIA Inc.
- Larry Brown, The Options Clearing Corp., EE. UU.
- Lars Erik Fjortoft, KPMG, Noruega
- Christopher Fox, PricewaterhouseCoopers LLP, EE. UU.
- Sara Hettich, Microsoft Corp., EE. UU.
- Grupo de Especialización en Auditoría de TI, IAI-Noruega
- Everett Johnson, Deloitte and Touche (retirado)
- Steve Mar, Microsoft Corp., EE. UU.
- Stuart McCubbrey, General Motors Corp., EE. UU.
- Peter Petrusky, PricewaterhouseCoopers LLP, EE. UU.
- Jay R. Taylor, General Motors Corp., EE. UU.
- Hajime Yoshitake, Nihon Unisys Ltd., Japón
- Nilesh Zacharias, PricewaterhouseCoopers LLP, EE. UU.

GTAG

Gestión y auditoría de riesgos de privacidad

Uno de los problemas, de mayor desafío y más significativos, de la gestión de riesgos que las organizaciones deben enfrentar actualmente es la protección de la privacidad de la información personal de los clientes y empleados. Esta guía incluye conceptos, principios y marcos de privacidad que ayudarán a los directores ejecutivos de auditoría (DEA), auditores internos y a la alta dirección a identificar los recursos correctos que les servirán de pautas para sus respectivas organizaciones. Brinda los conocimientos detallados sobre los riesgos de privacidad que la organización debe abordar cuando reúne, emplea, mantiene y divulga información personal. Esta GTAG dará más detalles de cómo abordar la privacidad dentro del proceso de auditoría y además proporcionará un resumen general para un programa de auditoría de la privacidad.

¿Qué es la GTAG?

Las Guías de Auditoría de Tecnología Global (GTAG) preparadas por el IIA están escritas en un lenguaje directo de negocio para abordar en forma oportuna problemas relacionados con la gestión, el control y la seguridad de la tecnología de la información. La colección GTAG se utiliza como un recurso disponible para los directores ejecutivos de auditoría sobre los distintos riesgos asociados a la tecnología y las prácticas recomendadas. Se publicaron las siguientes guías en 2005:

Guía 1: *Controles de tecnología de la información*

Guía 2: *Controles de gestión de parches y cambios: críticos para el éxito de la organización*

Guía 3: *Auditoría continua: implicancias para el aseguramiento, la supervisión y la evaluación de riesgos*

Guía 4: *Gestión de la auditoría de TI*

Consulte la sección de tecnología del sitio del Web del IIA technology en www.theiia.org/technology

The Institute of Internal Auditors
06403
www.theiia.org