Política Modelo

Evaluación del impacto en la privacidad

G20 Global Smart Cities Alliance

Esta directiva se considera fundamental para los principios de **privacidad y transparencia** de la guía de políticas de la Alianza Global de Ciudades Inteligentes del G20**.** Puede encontrar contenido complementario en nuestro sitio web[1] para proporcionar apoyo práctico para la adopción y aplicación de esta política.

Antecedentes

Las ciudades de todo el mundo están creciendo a un ritmo increíble con residentes que acuden en masa para aprovechar las oportunidades económicas y las comodidades que estas brindan. Los gobiernos municipales están respondiendo a su continuo crecimiento en parte mediante el despliegue de tecnologías y soluciones de "ciudades inteligentes" que permitan servicios más centrados en los ciudadanos y el progreso hacia ciudades más sostenibles, incluyentes y abiertas.

[1] Puede visitarhttps://globalsmartcitiesalliance.org/

Para lograr estos objetivos, las ciudades y comunidades de todos los tamaños deben garantizar que los datos generados por estas tecnologías acerca de las personas y sus comunidades estén adecuadamente protegidos y asegurados.

La recopilación de datos ocurre en las operaciones diarias de la ciudad, desde pagar una factura de servicios públicos, navegar por una página web e incluso en actividades como caminar por una calle, viajar en transporte público o conducir por una carretera administrada por la ciudad. El uso de tecnologías para ciudades inteligentes, tales como sensores, dispositivos conectados y flujos constantes de datos que administran sistemas de transporte, apoyan el mantenimiento de infraestructura en tiempo real, gestionan automáticamente los servicios públicos, permitiendo una gobernanza transparente y datos abiertos, y apoyando los servicios de emergencia en áreas públicas, con el fin de brindar beneficios reales a los gobiernos y las comunidades. Aunque bien intencionadas, también pueden crear el riesgo de perjuicios a la privacidad individual y generar temores de vigilancia que se opongan a los beneficios de la vida de la ciudad y desalienten activamente a las personas de participar de los espacios públicos.

Los crecientes cambios y la complejidad de las tecnologías emergentes, los sistemas empresariales, las leyes y las regulaciones, así como el mayor escrutinio público, requieren que las ciudades tomen las medidas adecuadas para integrar de manera proactiva y metódica la privacidad y la protección de datos en sus actividades. Aunque la privacidad se entiende tradicionalmente como un concepto más amplio que abarca diferentes derechos, la protección de datos implica la protección del individuo en relación con la recopilación, el uso y el procesamiento de datos personales.

Las ciudades deben equilibrar su propia necesidad de utilizar y compartir datos para su desarrollo productivo teniendo presente los intereses más amplios de bienestar público y privacidad individual de tal manera que ayude a construir y mantener la confianza pública. Sin confianza pública, los beneficios de las tecnologías en las ciudades inteligentes serán en última instancia insostenibles. Las ciudades deben invertir en políticas y prácticas que ayuden a las personas, las comunidades locales y los proveedores de tecnología a maximizar los beneficios del uso responsable de los datos, al tiempo que minimicen los riesgos de privacidad para las personas y las comunidades.

Al implementar las políticas de Evaluación de Impacto en la Privacidad (PIA por sus siglas en inglés), las ciudades pueden establecer un método consistente para identificar, evaluar y abordar los riesgos de privacidad. La elaboración de una política modelo PIA es un proceso complicado, ya que existe una amplia variación en los enfoques culturales y jurídicos de privacidad y protección de datos en todo el mundo. En esta política, esperamos que al determinar el proceso que debe seguirse y los temas que deben ser considerados, podremos aumentar la probabilidad en que las ciudades consideran y abordan con más confianza los riesgos de privacidad de una manera consistente con las expectativas de la comunidad.

Contenido

Política Modelo

Objetivos

Una ciudad debe trabajar para encontrar un equilibrio justo entre la recopilación de información para proporcionar los servicios necesarios y la protección de la privacidad del público, especialmente cuando se utilizan tecnologías innovadoras en ciudades inteligentes. Las Evaluaciones de Impacto en la Privacidad (PIA) son herramientas esenciales de evaluación de la privacidad. Las PIAs se componen de un conjunto de procesos para identificar y gestionar los riesgos de privacidad durante todo el ciclo de vida de los datos, desde la recopilación hasta la eliminación. La implementación de un PIA antes de la adquisición o el uso de tecnologías en una ciudad inteligente puede aumentar la transparencia y la responsabilidad; apoyar la confianza pública; mitigar los posibles daños a la privacidad o los impactos dispares antes de que ocurran; mejorar el cumplimiento y reducir el riesgo legal; y permitir una toma de decisiones más segura y coherente sobre datos y la tecnología por parte de los funcionarios de la ciudad, sus aliados y la comunidad en general.

Una política PIA en una ciudad tendría que identificar los temas que deben ser tratados y los procesos que deben ser seguidos en la identificación y mitigación de los riesgos sobre la privacidad. Específicamente, una política de Evaluación de Impacto en la Privacidad (PIA) debería:

- Articular propósitos específicos para datos y tecnologías, así como riesgos potenciales de privacidad y medidas de mitigación, y evaluarlos en contraste con los valores, prioridades y derechos legales de la ciudad y los miembros de la comunidad.
- Estar integrado a lo largo de todo el ciclo de vida del proyecto y de los datos (incluyendo intersecciones con las obligaciones de la ciudad en cuanto a adquisiciones, seguridad de datos, accesibilidad y registros públicos).
- Tratar todos los datos recopilados por una tecnología o servicio, no solo los datos considerados "personales" o "personalmente identificables" en un momento determinado.
- Facilitar la comunicación y la cooperación acerca de las prácticas de privacidad interna y externamente, y crear un entendimiento claro sobre cuándo la ciudad debe reconsiderar una tecnología en particular o notificar a sus comunidades, socios y proveedores de tecnología.
- Fomentar la innovación apoyando la toma de decisiones éticas y optimizando los usos beneficiosos de los datos, minimizando al mismo tiempo las consecuencias adversas para la privacidad individual y la sociedad en su conjunto.
- [Opción más participativa]: incorporar oportunidades significativas e incluyentes para la participación pública y la toma de decisiones sobre las prácticas de datos y tecnología.

Ejemplos:

- http://www.longbeach.gov/globalassets/health/healthy-living/office-of-equity/clb_toolkitbook_singlepages
- https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/691383/Consultation_Principles__1_.pdf

Fundamentos para las Evaluaciones de Impacto sobre la Privacidad

Componentes fundamentales del procedimiento para apoyar los objetivos específicos de la política PIA, y su objetivo general de maximizar los beneficios sociales y minimizar los riesgos para las personas y las comunidades.

1. Valores organizativos y riesgo

a. Las ciudades deben identificar explícitamente los valores públicos, las prioridades y los principios de privacidad contra los cuales se evaluarán determinadas tecnologías o servicios durante el proceso PIA.

> **Ejemplos:**
> - Directrices de la IOT de Nueva York
> - Principios de privacidad de Seattle
> - Estándares de servicio digital de Barcelona
> - La estrategia de ciudades DataSmart de la India

b. Las ciudades deben identificar explícitamente las normas legales y la autoridad, así como las políticas y principios existentes de la ciudad, contra los cuales se evaluarán tecnologías o servicios particulares durante el proceso de un PIA.

c. Las Evaluaciones de Impacto en la Privacidad (PIA) debe tener en cuenta consideraciones que van más allá del cumplimiento legal al evaluar los riesgos y beneficios, incluyendo la ética, la equidad y la participación pública. Estas consideraciones deben incluir tanto el impacto individual como grupal.

d. [Opción de mayor madurez]: el proceso de un PIA puede incluir una puntuación preliminar aproximada de oportunidades basada en los valores identificados anteriormente.

> **Ejemplos:**
> - https://wellington.govt.nz/~/media/about-wellington/emergency-management/files/covid-19/wcc-privacy-impact-assessment-digital-contact-tracing.pdf?la=en

e. [Opción más participativa]: involucrar al personal de la ciudad y al público, especialmente a las poblaciones vulnerables, para determinar los valores públicos, principios y umbrales de riesgo más ampliamente. Los modelos incluyen juntas ciudadanas, programas de representación ciudadana, asambleas de ciudadanos, modelos digitales para aumentar el voto o presupuestar las finanzas de las ciudades, difusión pública de borradores y/o participación en las redes sociales.

2. Alcance y frecuencia

a. Se debe realizar una evaluación inicial (u otro análisis de umbral para determinar si se requiere un PIA completo):

i. Cuanto antes, para el desarrollo o adquisición de cualquier nueva tecnología [y deben incluirse protecciones conscientes a la privacidad incorporadas en los criterios de adquisición o en el proceso de desarrollo de una tecnología]. La adecuación o modificación de un sistema para reducir los riesgos de privacidad después de que éste ha sido diseñado o implementado ha demostrado ser costosa.

ii. Al planificar cambios materiales en los procesos y sistemas existentes, incluidas actualizaciones de proyectos que pueden contener nueva actividad de datos o cambios en el alcance.

b. Un PIA completo o actualizado debe ser desarrollado cuando sea requerido por la regulación o la normativa de la ciudad o cuando la Evaluación Inicial indique que:

i. Se introducirán nuevas tecnologías, nuevos propósitos o procesos de datos que pueden identificar personalmente a los individuos.

ii. Se proyectan cambios significativos en las políticas, los procesos empresariales o los sistemas que pueden afectar la separación física o lógica de la información personal de otra información dentro de un sistema.

iii. Se deben procesar datos sensibles, o la tecnología o el servicio pueden permitir el procesamiento de datos de alto riesgo [(como calificación/perfilado de personas, monitoreo sistemático, procesamiento a gran escala, fusión o correspondencia de datos de múltiples fuentes, focalización de niños o personas vulnerables, riesgo de daño físico, o el uso de nuevas tecnologías o una nueva aplicación de las tecnologías existentes)].

iv. Cuando la tecnología o el sistema permite la toma de decisiones automatizada o asistida que puede tener efectos legales o de importancia similar en los individuos.

c. Cuando sea necesario, se debe llevar a cabo un PIA antes de la adquisición o despliegue de una tecnología de recolección de datos en el entorno de la ciudad o en los procesos de toma de decisiones de un gobierno local.

d. Las Evaluaciones de Impacto en la Privacidad (PIA) deben utilizarse para evaluar todos los datos recopilados por una tecnología o servicio, no solo los datos considerados legalmente "personales" o "personalmente identificables" en el momento de la recopilación.

e. La Evaluación de Impacto en la Privacidad debe ser solo una parte de un programa de privacidad integral. Debe entenderse de la misma forma que métodos tales como la no recopilación de datos, capacitación en habilidades de privacidad, regulación, auditoría y publicación de los PIAs dentro de cada gobierno local o como métodos utilizados por parte de las autoridades.

3. Herramientas y componentes

a. Las ciudades deben desarrollar y realizar una evaluación inicial preliminar u otro análisis de umbral a fin de revelar si se requiere una revisión adicional, tal como el desarrollo completo de un PIA [o una evaluación de impacto ético para los datos no personales].

b. Las evaluaciones iniciales deben contener una evaluación preliminar de los riesgos de privacidad generados por el sistema, el producto y/o el servicio, y pueden incluir diagramas de flujo de datos de alto nivel o datos preliminares y características de uso.

Ejemplos:

- Evaluación inicial de Helsinki
- Políticas PIA de Seattle
- Políticas PIA de Toronto

c. Si se determina que se requiere un PIA completo, debe incluir los siguientes componentes (favor consultar "Fundamentos de un PIA" a continuación):

i. Evaluación de los riesgos de privacidad. La realización de una evaluación de riesgos de privacidad ayuda a una organización a identificar los riesgos de privacidad generados por el sistema, el producto o el servicio y a priorizar los mismos para poder tomar decisiones informadas sobre cómo responder a los riesgos.

ii. Una determinación de la respuesta al riesgo - al determinar cómo responder a los riesgos evaluados, las ciudades deben referirse a sus valores organizativos y a la determinación de la tolerancia al riesgo. Los enfoques de respuesta incluyen:

- **Mitigación** (los riesgos se mitigan a un nivel aceptable de riesgo residual mediante medidas técnicas y políticas como la minimización de datos),
- **Transferir/compartir** (los riesgos se comparten con otras partes, por ejemplo, a través de contratos o seguros; los mecanismos de consentimiento son una forma de compartir los riesgos con las personas. Los individuos deben ser capaces de entender razonablemente los riesgos relevantes antes de que se les pida que den su consentimiento),
- **Evitar** (las ciudades pueden optar por no utilizar ciertas tecnologías o llevar a cabo ciertos tipos de procesamiento de datos donde los riesgos superan los beneficios, o.
- **Aceptar** (las ciudades pueden optar por aceptar el riesgo cuando la probabilidad o el impacto de las consecuencias adversas son bajos, y los beneficios son grandes).

iii. Requisitos y controles seleccionados que permiten a la ciudad

- **Cumplir con las obligaciones legales aplicables.** Los requisitos de privacidad a nivel organizacional son un medio para expresar las obligaciones legales, los valores de privacidad y las políticas a las que una ciudad pretende adherirse. Los requisitos de privacidad a nivel organizacional pueden derivarse de diversas fuentes, incluido el entorno jurídico (por ejemplo, leyes, reglamentos, políticas o valores culturales; normas pertinentes; y principios de privacidad) y,
- **Enfrentar los riesgos** determinados para ser mitigados.

d. Las ciudades deben consultar a las autoridades locales de protección de datos y a otros expertos en privacidad y protección de datos para obtener orientación especializada, plantillas y herramientas para llevar a cabo PIAs y evaluar el riesgo de privacidad (Ver las recomendaciones adicionales más abajo)

> Un método probado en la realización de PIAs es el método del taller, que comienza con una reunión inicial, a la que se invita a todos los interesados necesarios o *stakeholders*. La asignación de responsabilidades tiene lugar en la reunión inicial. En el taller (o talleres) de evaluación de impacto después de la reunión inicial, los expertos han resuelto por adelantado los aspectos relacionados con sus responsabilidades, mientras que la documentación de los datos en la herramienta puede hacerse conjuntamente.

4. Funciones y responsabilidades

a. Un funcionario superior designado, como un Jefe/Oficial de Privacidad de la Ciudad (CPO por sus siglas en inglés) [con el apoyo de un equipo dedicado a la privacidad] debe ser responsable de:

i. Desarrollar plantillas, recursos y componentes apropiados para la Evaluación inicial de la Ciudad y las herramientas PIA,

ii. Establecer las normas y las calificaciones de los recursos permitidos para llevar a cabo un PIA,

iii. Revisar la evaluación inicial o determinar de otra manera dónde es necesario un PIA (incluida la revisión de PIAs existentes),

iv. Conducir y aprobar un PIA, incluyendo la entrega de requerimientos y recomendaciones para mitigar impactos en la privacidad.

v. Establecer contactos con otros funcionarios para resolver los problemas de privacidad y seguridad planteados durante el curso de un PIA, y.

vi. Determinar la respuesta de la ciudad a los riesgos de privacidad identificados.

b. Los funcionarios de agencias/departamentos/secretarías/programas deben ser responsables de:

i. Proporcionar información y documentación adecuadas sobre la tecnología propuesta y su uso (por ejemplo, funcionalidad de la tecnología, caso de negocio, propósitos propuestos, costos de protección continua de la privacidad y la seguridad, etc.),

ii. Completar la Evaluación Inicial y apoyar la finalización de un PIA completo, cuando sea apropiado,

iii. Implementar el plan de uso y manejo de datos y todas las salvaguardias apropiadas identificadas en un PIA como necesarias para mitigar los riesgos asociados con la tecnología propuesta,

iv. Asegurar que la PIA se comunique al personal y que se le dé tiempo y recursos suficientes para participar en el proceso de la PIA, y.

v. Autorizar y aprobar la PIA, según corresponda, antes de la implementación de tecnologías que impacten la privacidad.

c. Un ejecutivo o funcionario superior, como un director municipal o director de tecnología, debe tener autoridad para supervisar el cumplimiento de la política del PIA, incluyendo:

i. Asegurar que la política del PIA se comunique a todo el personal, se implemente y se aplique,

ii. Asegurar que la información sea compartida y accesible en la mayor medida posible, respetando al mismo tiempo los requisitos de privacidad y seguridad,

iii. Proporcionar el presupuesto y la estructura organizativa adecuados para permitir que el funcionario superior designado para la privacidad y otro personal lleve a cabo regularmente las PIAs,

iv. Desarrollar e implementar medidas apropiadas de rendición de cuentas (por ejemplo, procedimientos de ajuste, capacitación y sensibilización del personal, sistemas de notificación y admisión de quejas o amenazas potenciales relacionadas con la privacidad),

v. Supervisar la eficacia y los resultados de la política de PIA, y.

vi. Revisar la alineación del cronograma del PIA con el cronograma de los proyectos de Ciudad Inteligente.

d. Se debe consultar a otros funcionarios de la ciudad y a los interesados externos o *stakeholders* cuando se considere apropiado, dada la naturaleza de la tecnología o servicio en particular, tales como:

i. Un representante ejecutivo que asesore al programa PIA y apoye hasta el final la participación del departamento o dependencia,

ii. CISO (Chief Information Security Officer) u otros expertos en TI para ayudar en el diseño de sistemas tecnológicos y la evaluación y mitigación de los riesgos de seguridad de datos,

iii. Abogados de la ciudad o consultores legales para garantizar el cumplimiento de las normas legales, incluida la normativa de protección de datos aplicable,

iv. Funcionarios de registros públicos y de datos abiertos para identificar las circunstancias en las que los datos pueden ser divulgados (intencionalmente o por ley),

v. Funcionarios de compras,

vi. Funcionarios de otras agencias de la Ciudad para identificar intereses adicionales en los datos o la tecnología,

vii. Expertos externos en la materia,

viii. Socios tecnológicos, y.

ix. Miembros de las comunidades impactadas.

e. [Opción más madura]: un funcionario superior de temas de privacidad cuenta con el apoyo de profesionales especializados en protección de datos, gestión de riesgos y seguridad que son expertos en la realización de PIAs. El equipo de privacidad de datos cuenta con el apoyo de una red de "campeones de la privacidad" en toda la ciudad, que son expertos en la materia dentro de departamentos específicos capaces de ayudar en el proceso de PIA. El equipo de PIA es capaz de construir conocimiento institucional y mejores prácticas, apoyar la toma de decisiones de privacidad más

Ejemplos:

- Toronto RMIS w/in I&T division
- Campeón de privacidad de Seattle

consistente en toda la ciudad, e identificar oportunidades para mejorar los procesos y resultados del PIA.

f. [Opción más participativa]: Un organismo u organización externa se dedica a proporcionar información, hacer recomendaciones, utilizar la experiencia de la comunidad o proporcionar aprobación para la PIA. El grupo incluye a diversos representantes de las partes interesadas o *stakeholders*, incluidos expertos en privacidad y protección de datos y miembros de la comunidad.

Ejemplos:

- Grupo de Trabajo de Vigilancia de Seattle
- Comisión Asesora de Privacidad de Oakland

5. Supervisión y registro

a. Todas las evaluaciones y PIAs iniciales deben documentarse completamente por escrito, y deben ser desarrolladas según el cronograma de mantenimiento de registros de la Ciudad. Ejemplos: Registro de datos de Helsinki, Revisiones del PIA de Seattle

b. Cualquier tecnología que se determine que está exenta de la revisión mediante un PIA también deberán registrarse y documentarse por escrito.

c. Las PIAs pueden ser clasificadas y categorizadas de existir múltiples PIA por ciudad.

d. Los gobiernos locales deberían crear un proceso secundario y agregado de PIA, realizado [cada tres años] para evaluar la forma en que interactúan los sistemas y los datos, con el fin de evitar que los datos que se consideraban no personales fuesen identificables con el tiempo; mediante la evaluación conjunta de todos los datos generados por una tecnología o conjuntamente con un servicio de IoT (Internet de las cosas), las ciudades pueden de esta manera evaluar en mayor medida su impacto futuro.

e. Un funcionario de nivel superior designado para temas de privacidad deberá revisar la política PIA anualmente (o antes, si es necesario), y actualizarla según sea el caso.

f. Los departamentos, divisiones o programas de la ciudad y cualquier socio o proveedor de servicios deben evaluar su propio grado de cumplimiento con la

Política PIA, [por ejemplo, mediante la realización de auditorías internas, revisiones de programas o evaluaciones de los mismos].

g. En caso que la ciudad reciba una queja de privacidad o experimente una violación de privacidad, un funcionario de nivel superior designado para la privacidad debe investigar y hacer recomendaciones, según sea necesario, para remediar la situación.

h. [Opción de mayor madurez]: Las ciudades deben desarrollar y mantener un inventario de sistemas/productos/servicios que procesen los datos, incluyendo las funciones de los propietarios u operaciones con respecto a los sistemas y sus componentes; la procedencia de los datos; las acciones de datos de los sistemas inventariados; el(los) propósito(s) de las acciones de datos y el entorno de procesamiento de datos.

Precedentes:

- Inventario de tecnología de vigilancia de Seattle
- Registro de IoT de Ámsterdam
- El Sentilo de Barcelona
- El piloto de Transparencia Digital Pública de la Ciudad de Boston
- Marco de privacidad del NIST

6. Transparencia y participación

a. En la medida de lo posible, las ciudades deben poner a disposición del público todas las PIA en un sitio web fácilmente accesible y orientado a la comunidad.

Precedentes:

- Inventario de PIA y SIR de Seattle
- Wellington DCTT PIA

b. Las ciudades deben desarrollar e implementar actividades apropiadas para permitir que las organizaciones y los individuos tengan una comprensión confiable y participen en un diálogo sobre cómo se procesan los datos y los riesgos asociados a la privacidad.

c. Las ciudades deben desarrollar mecanismos adicionales (por ejemplo, avisos, informes internos o públicos) para comunicar los propósitos de procesamiento de datos, prácticas y riesgos de privacidad asociados con tecnologías de ciudades inteligentes, informadas por las PIA pertinentes.

d. [Opción más participativa]: Se establecen mecanismos para obtener retroalimentación de las personas (por ejemplo, encuestas o grupos focales) sobre el procesamiento de datos y los riesgos asociados a la privacidad.

> **Orientación complementaria:**
>
> - Las PIAs deben evitar el uso de acrónimos, jergas u otros términos que no sean bien conocidos por el público externo. Además, las respuestas deben escribirse utilizando un lenguaje, principalmente, no técnico para garantizar que sean accesibles a las audiencias que no estén familiarizadas con el tema.
> - La señalización debe proporcionarse *in situ*, según sea necesario, para cumplir con las normativas locales de privacidad pertinentes [y debe considerarse para nuevas implementaciones o tecnologías de IoT de manera mucho más amplia a fin de informar al público sobre las actividades de recopilación y procesamiento de datos].

Fundamentos de una Evaluación de impacto de Privacidad

En esta sección se describen las cuestiones o preguntas fundamentales que debe abordar una PIA, a fin de permitir que las ciudades y sus socios identifiquen y mitiguen eficazmente los posibles riesgos de privacidad, al tiempo que maximizan los beneficios públicos de datos y tecnologías.

Una PIA debe claramente y de manera comprensible:

1. Identificar los departamentos, divisiones, secretarías o programas de la ciudad y cualquier socio o proveedor de servicios que usará o será responsable de la tecnología.

2. Describir la tecnología a ser diseñada o adquirida y una descripción de sus capacidades generales, funcionalidad, el tipo de datos que razonablemente generará, las fuentes y exactitud de cualquier información personal recopilada, incluyendo posibilidades de vigilancia razonablemente previsibles fuera del uso propuesto por el departamento o secretaría de la ciudad.

3. Describir el propósito y el uso propuesto de la tecnología, incluyendo su valor y beneficio para los individuos, la comunidad y la sociedad en general [y cualquier dato o investigación que demuestre esos beneficios]. Describir el problema que la tecnología busca resolver y si existen alternativas menos invasivas.

4. Describir la autoridad que tiene la ciudad para recopilar, utilizar y divulgar datos personales relevantes para la tecnología propuesta, según corresponda.

5. Describir cualquier valor público, principios, estándares legales y marcos de riesgo organizacional contra los cuales se está evaluando la tecnología.

6. Evaluar y describir los riesgos potenciales de privacidad asociados con el uso propuesto de la tecnología, [incluyendo la probabilidad de que se produzcan tales riesgos y la gravedad del impacto potencial en individuos y comunidades.]

7. Describir la respuesta de riesgo de la ciudad a los riesgos identificados, dados los valores organizacionales y la tolerancia al riesgo (por ejemplo, mitigación de riesgos, transferir/compartir riesgos, evitar o aceptar riesgos).

8. Describir una política clara de uso y gestión de datos para el uso propuesto de la tecnología, incluyendo:

    a. Cómo y cuándo se implantará o utilizará la tecnología y quién la utilizará (incluyendo, según proceda, las descripciones de quién tiene derechos de propiedad o licencia sobre los datos y en qué condiciones).

    b. Cualquier norma adicional que regule la tecnología (incluidas las normas legales que deban cumplirse antes de que se utilice la tecnología, como por ejemplo para los fines de una investigación penal).

    c. Cómo se almacenarán y destruirán o des-identificarán los datos de forma segura.

    d. Cuánto tiempo se conservarán los datos en formas identificables y no identificables.

    e. Cómo se supervisará y controlará el acceso a los datos, [incluidos los registros de acceso y las auditorías].

    f. Si la tecnología o los datos van a ser compartidos, de ser así en qué condiciones (incluyendo tanto el intercambio rutinario, como con socios o proveedores de servicios, otras entidades gubernamentales, investigadores,

solicitudes de registros públicos, o datos abiertos, y en circunstancias exigentes).

g. Qué medidas de capacitación y rendición de cuentas ayudarán a asegurar que todo el personal que opere la tecnología o acceda a los datos la use únicamente en cumplimiento con la política de la ciudad.

h. Qué medidas de protección existen para garantizar la confidencialidad, integridad y disponibilidad de los datos (incluida la protección contra amenazas como el *ransomware*, el *malware* o las vulnerabilidades de IoT).

i. Cualquier otra protección legal, organizativa, física y técnica destinada a mitigar los riesgos potenciales de privacidad asociados con el uso de la tecnología.

9. Describir la participación comunitaria y cualquier plan de participación futuro, cualquier comentario recibido y las respuestas dadas por parte de la ciudad, y las conclusiones acerca de los impactos potenciales y dispares locales que pueden resultar tras la adquisición y el uso de la tecnología.

10. Describir cualquier legislación de emergencia o de defensa civil que pueda cambiar la forma en que se utilizan los datos o los procesos que los rigen.

11. Describir cómo se han tenido en cuenta y mitigado los impactos potenciales de la tecnología sobre los derechos y libertades civiles y los impactos dispares potenciales sobre las comunidades marginadas.

12. Describir la disponibilidad de fondos para los costos continuos de privacidad y protección de datos relacionados con la operación de la tecnología (como personal, cumplimiento legal, auditoría, retención de datos y costos de seguridad).

Orientación y recursos adicionales

Ejemplos de PIA de ciudad

- Registro de datos de Helsinki y Herramientas DPIA
- Política de Evaluación de impacto de Privacidad del Condado de Huron
- Políticas de uso de Vigilancia del Condado de Santa Clara

- PIA Reviews de Seattle y Reportes de vigilancia
- Política de impacto de privacidad de Toronto
- Rastreo de contacto digital PIA de Wellington

Orientación sobre la realización de un PIA o DPIA

- Las anteriores recomendaciones del Artículo 29 del Grupo de Trabajo sobre la Valoración de Impacto de la Protección de Datos (DPIA) y la determinación de si el procesamiento puede "resultar en un alto riesgo" (2017) + Estado miembro de la UE Listas Blancas y Negras de la DPIA (2019)
- DPA/CNIL francés -- Recursos de Evaluación de Impacto de Privacidad *(disponibles en francés e inglés)*, incluyendo orientación, plantillas, bases de conocimiento, ejemplos de IoT, infografía y una herramienta de software libre (2018)
- En español DPA/AEPD's modelo de informe de Evaluación de Impacto en la Protección de Datos (EIPD) dirigido a Administraciones Públicas (2019) *(Disponible en español)*
- OAIC Australiano -- Junta de Información del Sector Público (PSCIOC, por sus siglas en inglés) Guía para realizar evaluaciones de impacto de la privacidad
- Comisionado de Privacidad de Nueva Zelanda - - Manual de Evaluación de Impacto de la Privacidad
- OPC Canadiense - - Guía de PIA
- Bureau of Justice Assistance - - Departamento de Justicia de EE. UU., Guía para realizar evaluaciones de impacto de privacidad: Para entidades de justicia estatales, locales y tribales (2012)
- NIST Herramienta para mejorar la privacidad a través de la empresa Gestión de riesgos
- Sidewalk Labs, Evaluación responsable del uso de datos - Innovación Digital Apéndice Sección 2.2.3, página 237 - 295
- UN Global Pulse, Evaluación de los riesgos, daños y beneficios
- SynchroniCity: Ofrecer un Mercado Único Digital con IoT para Europa y otros territorios.

Agradecimientos

Co-Leads

Kelsey Finch, Asesor Principal, Foro del Futuro sobre la Privacidad

Michael Mattmiller, Director de Asuntos gubernamentales de Microsoft

Miembros del grupo de trabajo:

Pasquale Annicchino, Lex Digital y Archimede Solutions

Sean Audain, Ayuntamiento de Wellington

Chandra Bhushan, Quantela

Dylan Gilbert, Asesor de Política de Privacidad, NIST

Naomi Lefkovitz, Asesora y Gerente Senior de políticas de Privacidad, Programa de Ingeniería de Privacidad, NIST

Jacqueline Lu, Co-fundadora, Helpful Places

Eugene Kim, Director asociado, Privacidad y Gobernanza de datos, Sidewalk Labs

Dan Wu, Immuta

Colaboradores y revisores:

Héctor Dominguez-Aguirre, Ciudad de Portland

Dilip Krishnaswamy, Vicepresidente de I&D de nuevas técnicas, Reliance Jio

Masaru Yarime, Ph.D., Profesor asociado, División de Política Pública (PPOL), Universidad de Ciencia y Tecnología de Hong Kong

Acerca de la Alianza Global de Ciudades inteligentes del G20

Creada en junio de 2019, la Alianza Global de Ciudades Inteligentes del G20 sobre Gobernanza Tecnológica reúne a los gobiernos municipales, regionales y nacionales, a los socios del sector privado y a los residentes de las ciudades en torno a un conjunto compartido de principios para el uso responsable y ético de las tecnologías de las ciudades inteligentes. El Foro Económico Mundial, la Organización Internacional para la Cooperación Público-Privada, actúa como secretaría de la Alianza.

A través de la Alianza, expertos globales del gobierno, socios del sector privado y la sociedad civil, están recopilando y analizando políticas de todo el mundo para identificar políticas modelo necesarias para ciudades inteligentes, éticas y exitosas.

Puede encontrar más políticas modelo y más detalles sobre la Alianza en:
https://globalsmartcitiesalliance.org/

Foro Económico Mundial
91–93 route de la Capite
CH-1223 Cologny/Ginebra
Suiza
Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
info@globalsmartcitiesalliance.org
https://globalsmartcitiesalliance.org/

Portada: Imágenes de stock del