Principio: Aborde la privacidad y la seguridad

Resumen

Abordar la privacidad y la seguridad en el área del desarrollo digital implica sopesar cuidadosamente cuáles datos se recopilan y de qué manera se adquieren, se usan, se almacenan y se comparten. Las organizaciones deben tomar medidas para minimizar la recopilación de datos y proteger la información confidencial y las identidades de los individuos representados en los conjuntos de datos frente al acceso no autorizado y la manipulación por parte de terceros. Las prácticas responsables para las organizaciones que recopilan y usan datos de individuos incluyen tomar en consideración las susceptibilidades en torno a los datos que han recopilado, ser transparentes en cómo se recopilan y usan los datos, reducir al mínimo la cantidad de personas identificables y de información sensible que se recopila, crear e implementar políticas de seguridad que protejan los datos y defiendan la privacidad y dignidad de los individuos, y crear una política de fin de ciclo de vida para la gestión de los datos tras la conclusión del proyecto.

Preceptos básicos

- **Defina la propiedad, la soberanía y el acceso a los datos antes de recopilar o capturar cualquier dato.** Determine cuáles leyes y reglamentos nacionales en materia de protección de datos se deben cumplir, quién decide qué se hace con los datos, quién está autorizado para acceder a los datos o usarlos y dónde pueden (o deben) almacenarse los datos.
- **Mantenga el interés superior de los usuarios finales y de los individuos cuyos datos se recopilan** en el primer plano de su planificación con el fin de proteger la privacidad de los usuarios y garantizar la seguridad de los datos y una implementación ética. Esto es especialmente importante cuando los encargados de la implementación trabajan con comunidades vulnerables o marginadas que no han podido opinar sobre la manera como se han recopilado, usado o compartido sus datos.
- **Realice un análisis de los riesgos y beneficios asociados a los datos que se están procesando**, en el que se identifique quiénes se benefician y quiénes corren un riesgo. Podría ser necesario repetir este proceso en el transcurso del período de ejecución a

GUÍA PARA EL CICLO DE VIDA DEL PROYECTO

Las siguientes recomendaciones, consejos prácticos y recursos provienen de la comunidad de desarrollo digital y su objetivo es brindarle opciones para aplicar este principio durante cada etapa del ciclo de vida del proyecto o del software. Esta guía no pretende ser exhaustiva, sino sugerirle las medidas que puede tomar para aplicar este principio en su trabajo. Si tiene otros consejos prácticos, recursos o comentarios que añadir, compártalos con la comunidad en https://forum.digitalprinciples.org/.

medida que se requieran nuevos datos, surjan o se identifiquen nuevos riesgos o se tomen en consideración nuevos aliados que compartan los datos.

- **Evalúe los riesgos** del acceso no autorizado o la fuga de cualquier dato almacenado. Sopese las consecuencias que estos datos podrían tener para los individuos si se accede a ellos o se publican maliciosamente, así como los riesgos que surgirían si se combinaran con otros conjuntos de datos.
- **Comprenda que los riesgos dependen en una gran medida del contexto,** no solo de los países sino también de las comunidades, poblaciones y períodos de tiempo. Si trabaja con comunidades vulnerables o marginadas, ¿qué grupos podrían estar motivados a adquirir los datos que usted tiene?, ¿qué tan capaces son esos grupos, y son suficientes los controles de información y acceso con los que se protegen los datos?
- **Minimice la recopilación de información personal identificable.** Evalúe qué tan crucial es la información personal para el éxito del proyecto y cuáles serían las consecuencias si esos datos se exponen a terceros, especialmente cuando trabaje con usuarios de poblaciones vulnerables, como grupos minoritarios, personas discapacitadas, y mujeres y niños. Incluya una evaluación de riesgos de la recopilación de información personal.
- **Catalogue y haga seguimiento a la información personal o sensible recopilada durante el proyecto:** Cree un plan para destruir o asegurar el almacenamiento fuera de línea de los datos sensibles a mediados del proyecto y tras su finalización, incluyendo la revisión de los discos duros, del almacenamiento de archivos en la nube, de las unidades de memoria USB, de las bandejas de entrada de correo electrónico y de otras vías comunes de fuga de datos.
- **Sea transparente** con las personas cuyos datos se recopilan y explíqueles de qué manera su iniciativa usará y protegerá sus datos.
- **Obtenga el consentimiento informado** antes de recopilar datos. Es crucial garantizar que los participantes entiendan por qué se recopilan sus datos, cómo se usan y comparten

"Recuerde que las medidas de seguridad técnica son solo tan fuertes como los usuarios humanos de la tecnología. Diseñe seguridad que se pueda utilizar en los contextos donde se use la tecnología."

CLAYTON SIMS, DIMAGI

sus datos y de qué manera los participantes pueden acceder a los datos recopilados o modificarlos, y que pueden tener la opción de negarse a participar. Se debe informar a los participantes de los riesgos que conlleva que sus datos se compartan y los participantes deben comprenderlos plenamente. Los formularios de consentimiento deben redactarse en el idioma local y de tal forma que sean fácilmente comprensibles para las personas cuyos datos se recopilan.

- **Proteja los datos** adoptando las mejores prácticas para proteger y restringir el acceso a los datos. Algunos ejemplos de las mejores prácticas son: encriptar los archivos, usar la autenticación de dos factores, restringir los permisos de acceso, almacenar los datos en servidores seguros o servicios seguros de almacenamiento en la nube, e implementar políticas y procedimientos de seguridad organizaciones, incluyendo acuerdos sobre el intercambio de datos con todos los actores interesados que comparten datos.

El cumplimiento de estos preceptos es esencial para garantizar la implementación ética de las iniciativas de desarrollo digital y evitar las consecuencias negativas que pueden tener las fallas de seguridad. El cumplimiento de las prácticas de privacidad de los datos y de las salvaguardas de seguridad protege los intereses de las comunidades, y a la vez se fomenta la confianza entre los usuarios finales y los especialistas en desarrollo. La confidencialidad y seguridad de los datos personales deben mantenerse con el objetivo de preservar la dignidad y seguridad de los individuos representados.

ANÁLISIS Y PLANIFICACIÓN

CONSEJOS PRÁCTICOS Y RECURSOS

CONSEJO PRÁCTICO: Siga las mejores prácticas para recopilar y gestionar datos privados e información sensible:

- Obtenga el consentimiento informado de los dueños de los datos en los procesos que se emplean para acceder, usar y compartir sus datos personales.
- Sea transparente con las personas cuya información se recopila en relación con cómo usará usted los datos.
- Defina mecanismos para que las personas pueden acceder a la información sobre cómo recopila y usa usted sus datos personales.
- Recopile datos personales únicamente para un uso específico, justo y justificado.
- Minimice la recopilación de datos y limite la notación de los datos a los detalles esenciales.
- Aplique las normas y cumpla las mejores prácticas para el acceso, las actualizaciones y la gestión de los datos.

RECURSO: EL SISTEMA DE AUDITORÍAS Y PLANTILLAS DE EL SISTEMA DE AUDITORÍAS Y PLANTILLAS DE EVALUACIÓN PARA GRUPOS DE DEFENSORÍA. https://SAFETAG.org

RECURSO: DIRECTRICES PARA LA SEGURIDAD DE SISTEMAS Y REDES DE INFORMACIÓN HACIA UNA CULTURA DE SEGURIDAD: https://www.oecd.org/sti/ieconomy/34912912.pdf

RECURSO: Guia del Reglamento de General de Proteccion de Datos. https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf

Análisis y planificación

En esta etapa, piense estratégicamente en cuáles datos se recopilarán y cómo se usarán durante el ciclo de vida del proyecto. Determine cómo se protegerá la confidencialidad de la información sensible en cada etapa y sopese los riesgos de los datos comprometidos en comparación con la necesidad de recopilar los datos en primer lugar.

- **Identificar cuáles datos son críticos para el éxito de la iniciativa equilibrar la recopilación de datos sensibles esenciales con los mejores intereses de las personas.** Tenga presente que el acto de la recopilación de datos en sí misma puede poner en peligro a las poblaciones de alto riesgo. Recopile la cantidad mínima de información personal identificable y de datos sensibles; asegúrese de obtener el consentimiento informado usando unos formularios y una redacción que sean comprensibles para las personas cuyos datos se están recopilando. Evalúe si sería posible combinar los conjuntos de datos anónimos para identificar a usuarios específicos y relacionar con ellos datos confidenciales anónimos.
- **Realice una evaluación de riesgos** con el fin de identificar las amenazas internas y externas a las que se están expuestos sus datos, así como las vulnerabilidades del sistema. Dé prioridad a las amenazas o vulnerabilidades, tomando en cuenta el potencial de daños, la cantidad de usuarios afectados, la capacidad de explotación y el riesgo para la reputación. Diseñe un plan de gestión de riesgos en el que se describan las contramedidas que está tomando para hacer frente a las amenazas de alta prioridad.
- **Tome en cuenta las ramificaciones para la sostenibilidad y la ampliación** cuando esté decidiendo cuáles datos recopilar. Es posible que necesite reunir más información para apoyar el despliegue generalizado [https://digitalprinciples.org/resource/principio-4-siente-las-bases-para-la-sostenibilidad/] [https://digitalprinciples.org/resource/principio-3-disene-para-la-ampliacion/].
- **Conozca las normas y los reglamentos locales en materia de privacidad y seguridad de los datos, incluyendo la reglamentación de la junta de revisión institucional**. Hable

ANÁLISIS Y PLANIFICACIÓN

CONSEJOS PRÁCTICOS Y RECURSOS

RECURSO: African Union Convention on Cyber Security and Personal Data Protection, African Union. https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

RECURSO: The Hand-Book of the Modern Development Specialist, Responsible Data Forum. https://responsibledata.io/resources/handbook/.

con funcionarios del gobierno, líderes locales y reguladores de datos (como organizaciones multinacionales y administradores de hospitales) y con sus usuarios [http://digitalprinciples.org/resource/principio-1-disene-con-el-usuario/]. Conozca las consecuencias del incumplimiento (p. ej., multas o sanciones), así como cualquier impacto negativo que tendrá el incumplimiento sobre la reputación de su organización y el éxito de la iniciativa.

- **Planifique para tener capacidad de supervisión.** Asigne la responsabilidad de la seguridad y gestión de riesgos a personas específicas y organice sesiones de concientización y capacitación sobre seguridad orientadas a los usuarios finales. Identifique y asegure fondos estables para financiar las medidas y la supervisión de la seguridad.

Diseño y desarrollo

En esta etapa se deben crear, poner a prueba y formalizar los planes de gestión y seguridad de los datos. También podría recopilar datos con el fin de proporcionar información para el diseño y desarrollo de las herramientas digitales que se usan en el programa.

- **Diseñe un plan de gestión de datos** antes de que comience cualquier recopilación de datos. Un plan de gestión de datos detalla qué hará con los datos durante y después de su iniciativa con el fin de garantizar que los datos sean accesibles y seguros. Incluya en su plan las respuestas a las siguientes preguntas:
  - Recopilación de datos: ¿Cuántos datos se recopilarán, durante qué período se recopilarán los datos y quiénes serán los responsables de la recopilación, gestión y seguridad de los datos?
  - Verificación y limpieza: ¿La eliminación de la información personal identificable forma parte del proceso de limpieza (especialmente de los datos cualitativos)?
  - Organización y almacenamiento: ¿De qué manera está documentando y guardando sus datos para que otros puedan entenderlos y acceder a ellos, qué formatos de archivo y convenciones para los nombres está utilizando y cuáles son sus procedimientos de almacenamiento para garantizar que los datos estén seguros?
  - Acceso: ¿Quiénes tienen los derechos sobre los datos, cómo

ANÁLISIS Y PLANIFICACIÓN

CONSEJOS PRÁCTICOS Y RECURSOS

DISEÑO Y DESARROLLO

CONSEJOS PRÁCTICOS Y RECURSOS

RECURSO: Data Management Plan Tool, Stanford Libraries. https://library.stanford.edu/research/data-management-services/data-management-plans/dmptool

RECURSO: Data Management, Massachusetts Institute of Technology Libraries. https://libraries.mit.edu/data-management/plan/write/

RECURSO: The Hand-Book of the Modern Development Specialist: Designing a Project, Responsible Data Forum. https://responsibledata.io/resources/handbook/chapters/chapter-01-designing-a-project.html

se compartirán los datos, de qué manera protegerá usted los datos personales y se permitirá la reutilización?

- Archivo: ¿Durante cuánto tiempo se guardarán almacenados los datos, cómo se destruirán cuando ya no sean necesarios y de qué manera se harán anónimos? ¿Existe un repositorio de fuente abierta disponible para almacenar los datos, o los datos serán transferidos a otra organización?

Alinee su plan con las políticas de gestión responsable de los datos, de seguridad y de privacidad de la organización, así como con los estándares de la comunidad de fuente abierta, si procede. Comparta su plan con los aliados, usuarios objetivo y la comunidad de desarrollo digital más amplia con el fin de fomentar la transparencia, la rendición de cuentas y la confianza. Asegúrese de que el plan sea comprensible y abordable para estos diversos actores interesados.

- **Identifique a los miembros del equipo que serán los responsables de la gestión y seguridad de los datos durante todo el ciclo de vida del proyecto.** Las responsabilidades incluyen introducir cambios en el plan de gestión de datos cuando cambie el entorno externo, realizar un análisis de riesgos, monitorear los datos para garantizar que estén seguros y responder a brechas de seguridad, así como brindar capacitación a las personas que asumirán la propiedad de los datos si la iniciativa es transferida.
- **Conduzca una revisión regular de las funciones del sistema que recopilan datos automáticamente.** Durante el desarrollo, pueden agregarse nuevas funciones para recopilar datos dentro del sistema. ¿La iniciativa puede justificar la necesidad de recopilar esos datos y existen políticas claras sobre cómo se recopilarán, almacenarán, usarán y destruirán los datos?
- **Diseñe la herramienta digital de tal forma que se cumplan las normas actuales de seguridad física y de la información para proteger la información personal.** Por ejemplo, asegúrese de que la plataforma que está usando su iniciativa pueda gestionar el acceso de los usuarios y los permisos para ver o usar los datos.

DISEÑO Y DESARROLLO

CONSEJOS PRÁCTICOS Y RECURSOS

RECURSO: Beyond Data Literacy: Reinventing Community Engagement and Empowerment in the Age of Data, Data-Pop Alliance. http://datapopalliance.org/item/beyond-data-literacy-reinventing-community-engagement-and-empowerment-in-the-age-of-data/.

RECURSO: Data Innovation Risk Assessment Tool, UN Global Pulse. http://unglobalpulse.org/sites/default/files/Privacy%20Assessment%20Tool%20.pdf

RECURSO: Girl Safeguarding Policy: Digital Privacy, Security, & Safety Principles & Guidelines, Girl Effect. http://www.girleffect.org/media/3052/gem-girl-safeguarding-policys_19-05-16.pdf.

RECURSO: Responsible Data Management, Oxfam. https://policy-practice.oxfam.org.uk/publications/responsible-data-management-training-pack-620235.

RECURSO: Improving Data Privacy & Data Security in ICT4D: Meeting Report, UN Global Pulse. http://www.unglobalpulse.org/blog/improving-data-privacy-data-security-ict4d-meeting-report

DESPLIEGUE E IMPLEMENTACIÓN

CONSEJOS PRÁCTICOS Y RECURSOS

CONSEJO PRÁCTICO: Use una lista de control de protección de datos para asegurarse de que sus datos están seguros. También puede usar esta lista de control para definir los indicadores para monitorear y evaluar la seguridad y la privacidad de los datos.

- ¿Todos los archivadores se cierran con llave y los registros en papel están protegidos?
- ¿Las contraseñas de las computadoras se protegen

Despliegue e implementación

Durante esta etapa, ponga en marcha el plan de gestión de datos. Dependiendo de la iniciativa, usted también podría estar recopilando información personal. Comunique con regularidad cuáles datos está recopilando, cómo se están usando los datos, de qué manera se mantienen seguros y quiénes están usando los datos.

- **Controle el acceso a los datos para mantener su integridad y confidencialidad.** Cree grupos de acceso con permisos específicos dependiendo de las funciones de los usuarios. Configure los permisos predeterminados en el mínimo posible para la mayoría de las personas y habilite más permisos (como el acceso para leer y escribir) solo para los usuarios que sean esenciales. Establezca requisitos para las contraseñas individuales de todos los usuarios y considere usar la autenticación de dos factores. La autenticación de un solo factor es aquel en el que solo hay que introducir el nombre de usuario y una contraseña para iniciar sesión en una cuenta. Con la autenticación de dos factores hay que cumplir un paso más después de introducir la contraseña, como recibir por SMS un código de verificación enviado al número de teléfono asociado a la cuenta e introducir ese código para acceder a la cuenta.
- **Implemente contramedidas para los riesgos y las vulnerabilidades que tienen prioridad.** Continúe realizando con regularidad análisis de riesgos y auditorías de seguridad para identificar las vulnerabilidades emergentes. Responda inmediatamente a las brechas de seguridad con el fin de mitigar los efectos negativos rápida y fácilmente, e informe a las personas cuyos datos se hayan filtrado.
- **En el caso de que se esté cerrando el proyecto, implemente el plan para destruir los datos o para transferirlos a su lugar de almacenamiento de largo plazo.** Destruya los registros que considere sensibles o que ya no se requieren para iniciativas futuras o para su evaluación. Informe a los actores interesados relevantes cómo se están gestionando o destruyendo los datos.
- **En caso de ampliación de la escala o transferencia, trabaje con los nuevos miembros o las nuevas organizaciones de la iniciativa para asegurarse de que comprenden y cumplen el plan de gestión de datos establecido.** Identifique las

DESPLIEGUE E IMPLEMENTACIÓN

CONSEJOS PRÁCTICOS Y RECURSOS

usando contraseñas seguras?

- ¿Se asignaron números de identificación anónimos a todos los participantes?
- ¿Todos los miembros del personal recibieron capacitación en materia de confidencialidad y privacidad?
- ¿Todos los archivos de respaldo están protegidos?
- ¿En qué circunstancias se compartirán los datos y con quiénes? ¿Cómo se compartirán los datos de forma segura?
- ¿Los procedimientos de seguridad se revisan y actualizan con regularidad?
- No mantenga los datos en unidades de memoria USB ni otros dispositivos externos que puedan perderse o ser robados con facilidad.
- No use el correo electrónico para enviar información que pueda servir para identificar a los participantes.

RECURSO: Data Protection, Privacy and Security for Humanitarian & Development Programs, World Vision International. http://www.wvi.org/health/publication/data-protection-privacy-and-security-humanitarian-development-programs.

RECURSO: How to Develop and Implement Responsible Data Policies, MERL Tech. http://merltech.org/how-to-develop-and-implement-responsible-data-policies/.

RECURSO: The Hand-Book of the Modern Development Specialist: Getting Data, Responsible Data Forum. https://responsibledata.io/resources/handbook/chapters/chapter-02a-getting-data.html.

brechas de seguridad que puedan surgir como resultado de la ampliación de la escala o la transferencia. Trabaje con aliados para abordar las brechas y hacer las actualizaciones necesarias al plan de gestión de datos.

Transversalidad: Monitoreo y evaluación

Continúe siguiendo su plan de gestión de datos y haga las actualizaciones que sean necesarias con base en los hallazgos de su monitoreo y evaluación.

- **Diseñe un plan de recopilación de datos con base en su plan de monitoreo y evaluación,** e incorpore las consideraciones en el plan de gestión de datos. Asegúrese de que el personal haya completado la capacitación para ejecutar el plan y de que todos los responsables de la recopilación de datos reciba capacitación en el área de la ética de investigación. FHI360 ofrece un programa de capacitación en ética de investigación gratis para profesionales de desarrollo internacional [https://www.fhi360.org/sites/all/libraries/webpages/fhi-retc2/RETCTraditional/intro.html].
- **Siga los componentes de su plan de gestión de datos relativos a la organización, el almacenamiento y el acceso a los datos.** Cuando haya recopilado los datos, asegúrese de que se almacenen de forma segura mientras siga siendo posible acceder a ellos. Tenga en cuenta los siguientes aspectos:
  - ¿Cuál es la jerarquía y organización del sistema de archivos?
  - ¿Dónde estarán los metadatos del sistema de archivos (incluyendo el plan de gestión de datos)?
  - ¿Qué sistema usará para nombrar los archivos?
  - ¿Cuántas copias de los archivos se almacenarán en la base de datos electrónica?
  - ¿Se usará alguna de las tecnologías de redes de la organización para almacenar archivos (p. ej., una unidad de disco compartida o almacenamiento en la nube)?
  - ¿De qué manera se archivarán los datos?
  - ¿En qué formatos (p. ej., Microsoft Word y PDF) se guardarán los datos archivados?
  - ¿Cómo se protegerán los datos archivados (p. ej., base de datos bloqueada)?
  - ¿Cuánto espacio para almacenamiento de archivos será

TRANSVERSALIDAD:
MONITOREO Y EVALUACIÓN

CONSEJOS PRÁCTICOS Y RECURSOS

CONSEJO PRÁCTICO: Una organización apropiada de los datos de las encuestas (y otros datos) depende del uso sistemático de códigos de identificación durante los procesos de recopilación e introducción de datos. Los códigos de identificación garantizan que toda la información pueda ser rastreada y vinculada, independientemente de la fuente.

RECURSO: The Hand-Book of the Modern Development Specialist: Sharing Data, Responsible Data Forum. https://responsibledata.io/resources/handbook/chapters/chapter-02c-sharing-data.html.

RECURSO: Ética e investigación en Tecnología Educativa: necesidad, oportunidades y retos. https://www.researchgate.net/publication/305622491_Etica_e_investigacion_en_Tecnologia_Educativa_necesidad_oportunidades_y_retos

RECURSO: Currículo de capacitación sobre ética de la investigación para los representantes comunitarios https://www.fhi360.org/sites/all/libraries/webpages/fhi-retc2/RETCTraditional/intro.html

RECURSO: WFP y la innovacion digital. http://documents.wfp.org/stellent/groups/public/documents/communications/wfp287772.pdf

RECURSO: EL CÓDIGO DE SEÑAL: UN ENFOQUE DE DERECHOS HUMANOS A LA INFORMACIÓN DURANTE LA CRISIS https://signalcode.org/code-intro/

RECURSO: Research Data Security: Protecting Human Subjects' Identifiable Data, University of California, Berkeley, Human Research Protection Program. http://cphs.berkeley.edu/policies_procedures/ga106.pdf

necesario? ¿Está disponible o será necesario adquirirlo?

- **Preste atención a los riesgos de privacidad y anonimice los datos para eliminar la información personal identificable.** Use códigos de identificación durante el proceso de recopilación e introducción de los datos para que las respuestas se puedan rastrear sin violar la confidencialidad. Esta es una consideración particularmente importante en el caso de las poblaciones vulnerables o marginadas. Tenga presente que combinar conjuntos de datos podría hacer posible volver a identificar a los individuos.
- **Continúe evaluando los riesgos a los que están expuestos los datos y las vulnerabilidades del sistema.** Asegúrese de que el plan de gestión de riesgos está plenamente implementado.
- **Sopese los problemas éticos más generales.**
- **Monitoree los indicadores relacionados con la seguridad y privacidad de los datos.** La lista de control de seguridad de los datos incluida en los Consejos prácticos y recursos para el despliegue y la implementación proporciona varios indicadores que pueden usarse.

TRANSVERSALIDAD:
MONITOREO Y EVALUACIÓN

CONSEJOS PRÁCTICOS Y RECURSOS

- **RECURSO**: Framework for Creating a Data Management Plan, ICPSR. http://www.icpsr.umich.edu/icpsrweb/content/datamanagement/dmp/framework.html
- **RECURSO**: Data Security, University of California, Berkeley, Committee for Protection of Human Subjects. http://cphs.berkeley.edu/datasecurity.pdf
- **RECURSO**: Framework for Creating a Data Management Plan, ICPSR. http://www.icpsr.umich.edu/icpsrweb/content/datamanagement/dmp/framework.html
- **RECURSO**: Data Security, University of California, Berkeley, Committee for Protection of Human Subjects. http://cphs.berkeley.edu/datasecurity.pdf