Universidad de los Andes
Colombia

Departamento de Ingeniería de Sistemas y Computación

FOROS ISIS

# 5to FORO

## en Seguridad de la Información

# RETOS Y SOLUCIONES

PARA LA PRIVACIDAD EN UN MUNDO CONECTADO

**Universidad de los Andes | Vigilada Mineducación.**

Reconocimiento como Universidad: Decreto 1297 del 30 de mayo de 1964 | Reconocimiento Personería Jurídica: Resolución 28 del 23 de febrero de 1949 Minjusticia.

# Retos para garantizar la Privacidad

Sandra Julieta Rueda Rodríguez, Ph.D.
Departamento de Ingeniería de Sistemas y Computación
Grupo de Investigación COMIT
Universidad de Los Andes
sarueda @ uniandes.edu.co

***5to Foro en Seguridad de la Información***
***Universidad de Los Andes***
***Septiembre 20, 2018***

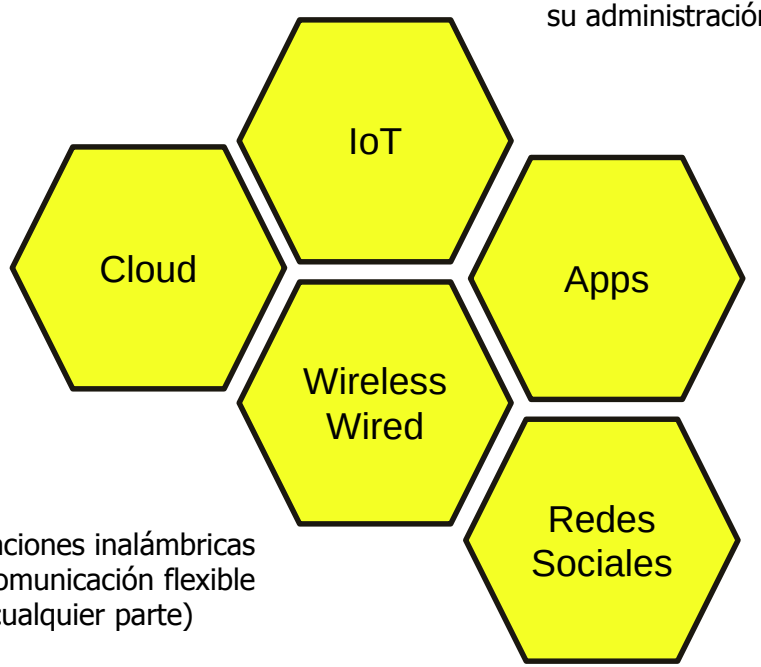
# Temas

- Contexto
  - Convergencia de tecnologías
  - Recolección masiva de datos
- Retos para garantizar la Privacidad
- Conclusiones

# Convergencia de Tecnologías

IoT extiende los elementos conectados a la red, habilitando su administración remota

Cloud ofrece acceso, desde cualquier parte, a cualquier hora, a un conjunto compartido, configurable y elástico de recursos de cómputo que pueden ser manejados con mínimo esfuerzo



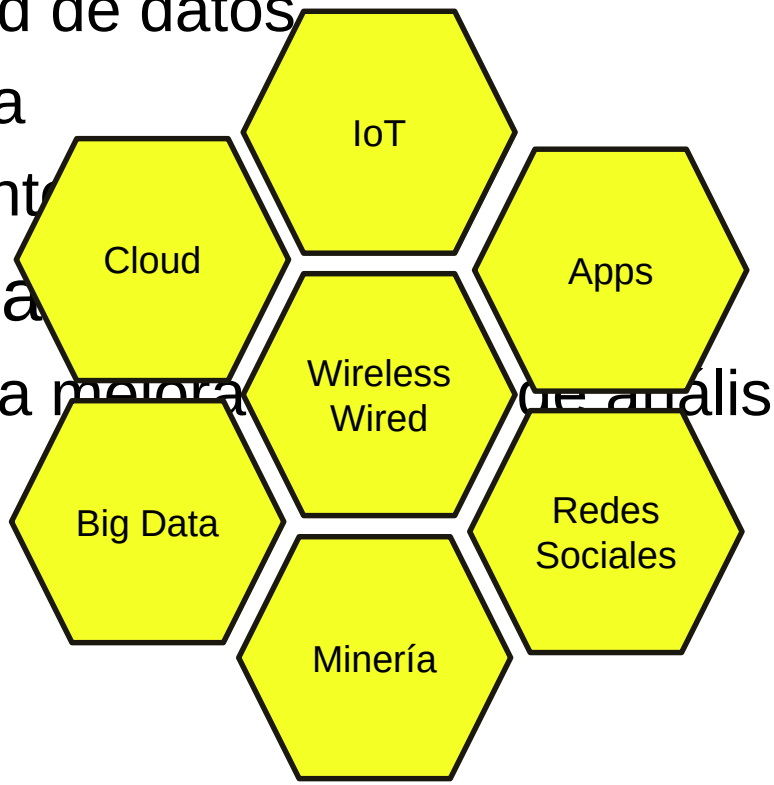

Los teléfonos inteligentes y las aplicaciones móviles permiten a los usuarios conectarse de forma remota con gran variedad de servicios

Las comunicaciones inalámbricas habilitan la comunicación flexible (desde cualquier parte)

Las redes sociales facilitan la comunicación asincrónica entre personas viviendo en diferentes ubicaciones geográficas con algún lazo en común

# Convergencia de Tecnologías

- Big Data
  - Gran cantidad de datos
  - Sin estructura
  - Diversas fuent
- Minería de Da
  - Técnicas para mejora de análisis de datos



# Convergencia de Tecnologías

- *Wearables*

Dispositivo


*Bluetooth Low Energy*

Obtiene y almacena los datos

*Aplicación*

Recoge los datos (del dispositivo) para presentarlos al usuario y para enviarlos al sitio web

*Sitio web del Proveedor*

Los usuarios pueden crear cuentas para ver sus datos (configuran edad, ubicación, email, etc.)

*Proveedor y Socios*

Terceros pueden tener acceso a los datos para análisis:

- Consolidar datos
- Buscar patrones
- Mejorar el servicio

*Análisis*
*Minería de Datos*

*Otros Usuarios*

Compartir Información

*Redes Sociales*

*IoT* *Wireless* *App* *Wired/ Wireless* *Cloud Big Data*

# Recolección de Datos

- Actividad natural en la sociedad de la información
- Objetivo
  - Análisis para tomar decisiones informadas que beneficien a todo el mundo
    - Individuos
      - Proveedores – Mejorando la experiencia de usuario
    - Grupos de individuos
      - Gobiernos – Definición de políticas públicas
      - Autoridades – Detección de riesgos (riesgos de seguridad)
      - Empresas – Estrategias de crecimiento

*Recolección y Análisis Masivos*

# Redes Sociales


- Algunas características del servicio:
  - "Usamos los datos que tenemos, por ejemplo, las conexiones que entablas, las opciones y la configuración que seleccionas, y lo que compartes en nuestros Productos o fuera de ellos, para personalizar tu experiencia."
  - "Usamos los datos que tenemos para hacer sugerencias a ti y a otras personas, por ejemplo, grupos a los que puedes unirte, eventos a los que puedes asistir, páginas que puedes seguir o a las que puedes enviar mensajes, programas que puedes ver y personas que quizás quieras incluir en tu lista de amigos."
  - "Te mostramos anuncios, ofertas y otro contenido patrocinado para que descubras contenido, productos y servicios que ofrecen los numerosos negocios y organizaciones que usan Facebook y otros de sus Productos. Nuestros socios nos pagan para que te mostremos su contenido, y nosotros diseñamos nuestros servicios para que el contenido patrocinado que ves te resulte tan útil y relevante como todo lo que se muestra en nuestros Productos."

https://www.facebook.com/legal/terms/update

# Redes Sociales

- Política de Datos
  - Información recopilada
    - Información y contenido que los usuarios proporcionan
    - Redes y conexiones
    - Uso
    - Transacciones
    - Actividad de otros usuarios e información que proporcionan sobre ti
    - Información de los dispositivos. Atributos, operaciones, identificadores, configuración, red y conexiones, cookies.

https://www.facebook.com/legal/terms/update

# Retos

- Manejo de datos personales
  - Dato personal
    - “cualquier información vinculada o que pueda asociarse a a una o varias personas determinadas o determinables.” [L1581,2012]
  - Principios rectores
    - Legalidad
    - Finalidad
    - Libertad
    - Transparencia
    - Acceso y circulación restringida
    - Seguridad
    - Confidencialidad

# Retos

- Manejo de datos sensibles
  - Dato sensible
    - “[…] aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar discriminación, tales como […] origen racial o étnico, orientación política, […] datos relativos a la salud, vida sexual y los datos biométricos.” [L1581,2012]
  - Se prohíbe el tratamiento de datos sensibles
    - excepto
      - Si hay autorización del titular (o su representante si el titular está incapacitado).
      - Por actividades legítimas por parte de una entidad sin ánimo de lucro con referencia exclusiva a sus miembros.
      - Como parte de un proceso judicial.
      - Con finalidad histórica, estadística o científica siempre y cuando se suprima la identidad del titular.

# Retos

- Manejo de datos privados
  - Privacidad
    - La información puede ser publicada siempre y cuando no ocasione fugas de información sensible para su propietario
  - vs. Confidencialidad
    - La información solo puede ser consultada por aquellos que están autorizados.
    - No debe ser publicada
- Proteger la privacidad los usuarios (considerando los entornos)
  - Aplicaciones, Consolidación de datos, Recolección, Cloud, Manejo agregado de datos

# Aplicaciones

- Cayla
  - Juguete inteligente
  - El Gobierno Alemán dijo a los padres que debían destruir la muñeca porque podría ser hackeada [Febrero 17, 2017]
    - “An official watchdog in Germany has told parents to destroy a talking doll called Cayla because its smart technology can reveal personal data.”
    - “student Stefan Hessel […] said a bluetooth-enabled device could connect to Cayla's speaker and microphone system within a radius of 10m (33ft). He said an eavesdropper could even spy on someone playing with the doll "through several walls".

[https://www.bbc.com/news/world-europe-39002142]

# Aplicaciones

- Apps

## iPhone apps Path and Hipster offer address-book apology

**The makers of two iPhone apps have apologised after it emerged they had uploaded users address-book information without explicit permission.**

Path and Hipster both sent contact data to company servers in order to help users find friends who were also using the apps.

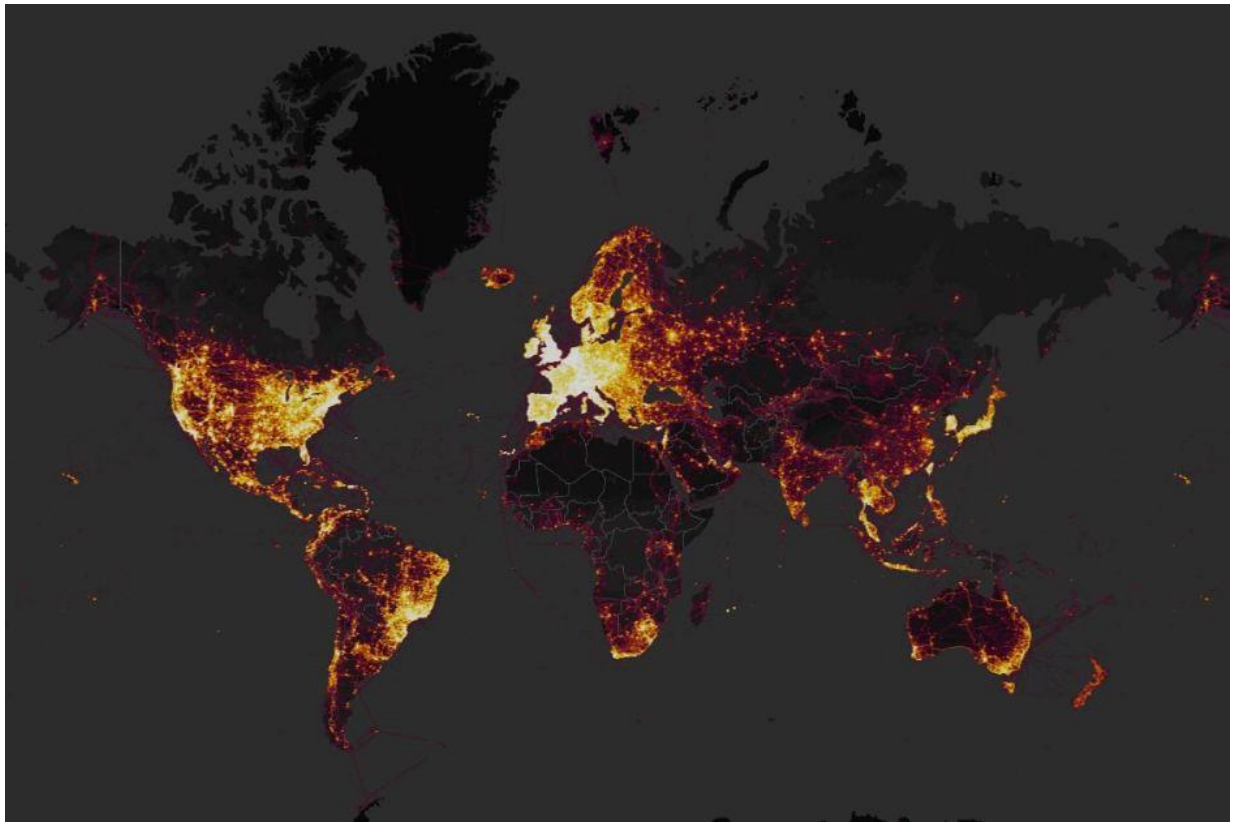
Both companies said they had now updated their apps to fix the problem.

Path says it helps you "share life with the ones you love"

[http://www.bbc.com/news/technology-16962129. Febrero 9, 2012]

# Consolidación de Datos

- Strava App
  - La aplicación registra información de ejercicio físico
  - La envía al servidor del proveedor
  - El proveedor la consolida



http://www.abc.net.au/news/2018-01-30/pentagon-reviewing-security-after-strava-app-reveals-locations/9373054

# Consolidación de Datos

- Strava App
  - “Nathan Russer, a student at the Australian National University in Canberra, drew attention to the data breach after stumbling upon GPS tracking company Strava's Global Heatmap. [..]”
  - Once you look at Syria you can see a bunch of bright spots," Mr Russer said."US bases are clearly identifiable and mappable [..]
  - US Defence Secretary Jim Mattis has ordered a review of security protocols [..]”
  - Pentagon reviewing security after Strava fitness app broadcast military personnel locations [Enero 27, 2018]

http://www.abc.net.au/news/2018-01-30/pentagon-reviewing-security-after-strava-app-reveals-locations/9373054

# Recolección

- Evitar la recolección (si no es necesaria)
  - En DEFCON 2016 dos hackers evaluaron la seguridad de un vibrador conectado (IoT):
    - El dispositivo permite la conexión de un compañero, vía la aplicación móvil. Esta conexión podía ser hackeada.
    - El fabricante registraba y enviaba a un servidor central temperatura, intensidad de la vibración y frecuencia de uso, sin consentimiento del usuario.
  - Una usuaria presentó una demanda y la compañía decidió negociar (llegó a un acuerdo).
    - ¿Cómo proteger a los usuarios?
    - ¿Por qué recoger esta información?

# Cloud

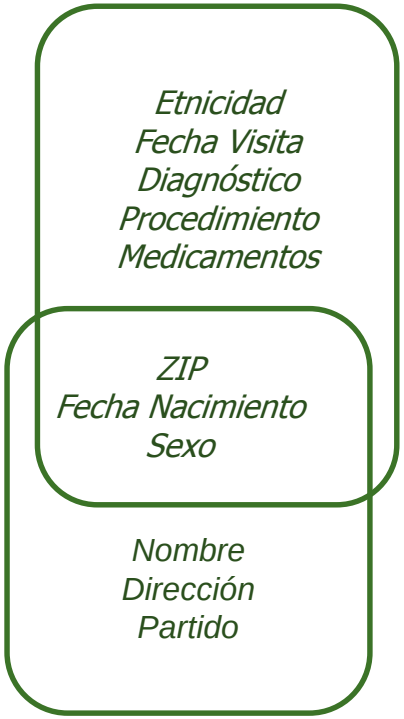
- Al hacer uso de infraestructuras cloud públicas (*off-premise*) las organizaciones ceden algo de control sobre su información
  - Es importante responder cuidadosamente:
    - ¿Tengo información sensible de clientes o proveedores?
    - ¿Cómo puedo salvaguardar su privacidad y cumplir con las obligaciones legales correspondientes?
  - Consideraciones
    - La responsabilidad técnica es compartida
    - ¿La responsabilidad legal?

# Manejo Agregado de Datos

- Anonimizar
  - Tipos de Datos
    - Datos anónimos
      - No pueden ser usados para identificar una persona de forma única
    - Identificadores
      - Dato o conjunto de datos que permiten la identificación directa (sin recurrir a otros datos) de una persona
    - Casi-identificadores
      - Conjunto de datos que en combinación pueden ser usados para reconocer a una persona de forma casi única (o única)

# Manejo Agregado de Datos

- Anonimizar
  - Remover identificadores
  - Tratar casi-identificadores o datos anónimos requiere mayor esfuerzo
    - Censo USA 1990
      - 216 millones / 248 millones (87%) tienen características únicas con base en ZIP, fecha de nacimiento, sexo
    - Encadenamiento/establecer relación con datos en otras bases de datos:
      - Datos de salud recopilados en hospitales incluyen ZIP, fecha de nacimiento, sexo, etnicidad
      - Datos de votantes incluyen nombre, dirección, ZIP, fecha de nacimiento, sexo



# Conclusiones

- Las nuevas tecnologías han creado nuevos retos
  - Las nuevas tecnologías y la convergencia de tecnologías han creado nuevos entornos con múltiples beneficios potenciales .. pero han introducido riesgos, en particular para la privacidad de los usuarios
- Las empresas que recopilan datos privados son responsables
  - Conocer las normas legales
  - Implementar políticas, procedimientos y mecanismos tecnológicos para cumplir con las normas legales y éticas
- Los usuarios juegan un rol
  - Las nuevas tecnologías facilitan la recolección masiva de datos,
  - mientras Big Data y Minería de datos mejoran las técnicas de análisis
  - con consentimiento del usuario, en la mayoría de los casos

# Gracias

Sandra Rueda
Departamento de Ingeniería de Sistemas y Computación
Grupo de Investigación COMIT
Universidad de Los Andes
sarueda @ uniandes.edu.co