Ingeniería de Sistemas

Redacción de paper individual para Seguridad de Sistemas TI

Seguridad de Sistemas TI

2022-1

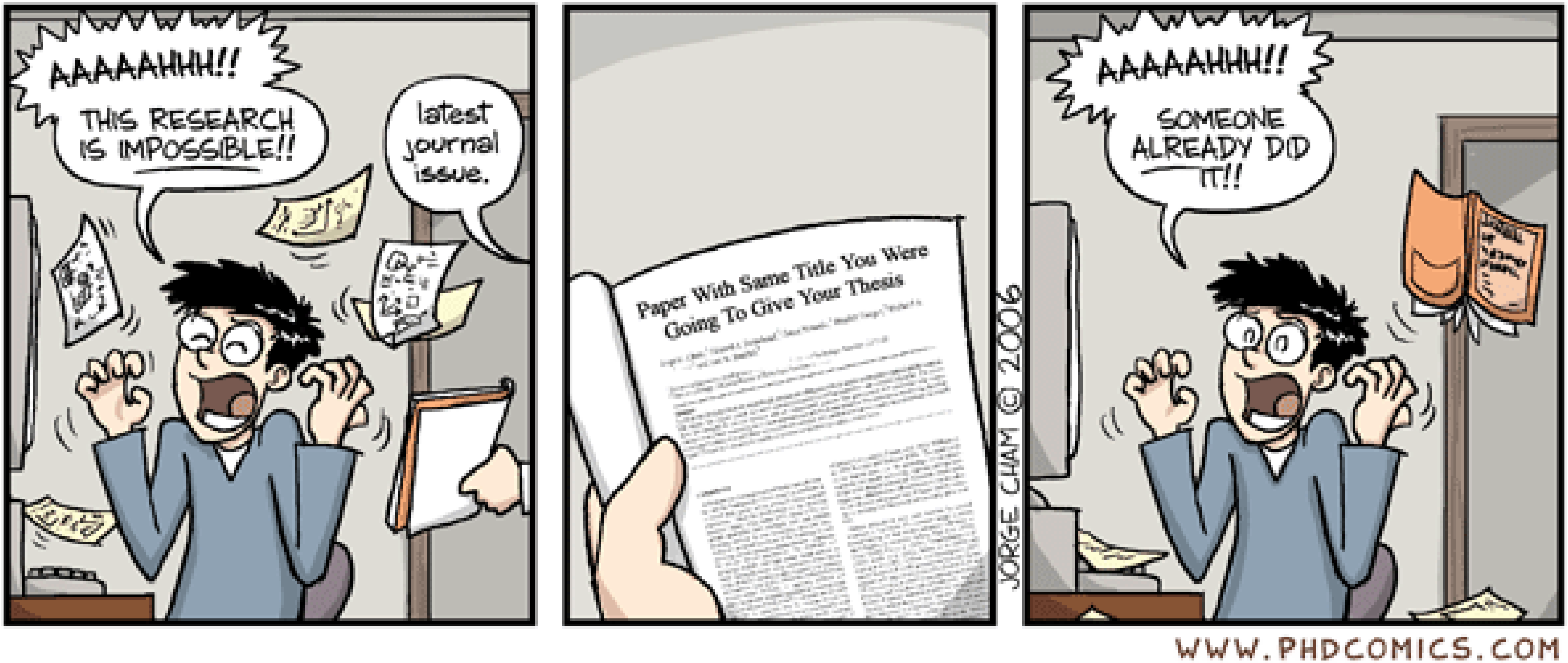
UNIVERSIDAD DE LIMA

Estructura de un paper

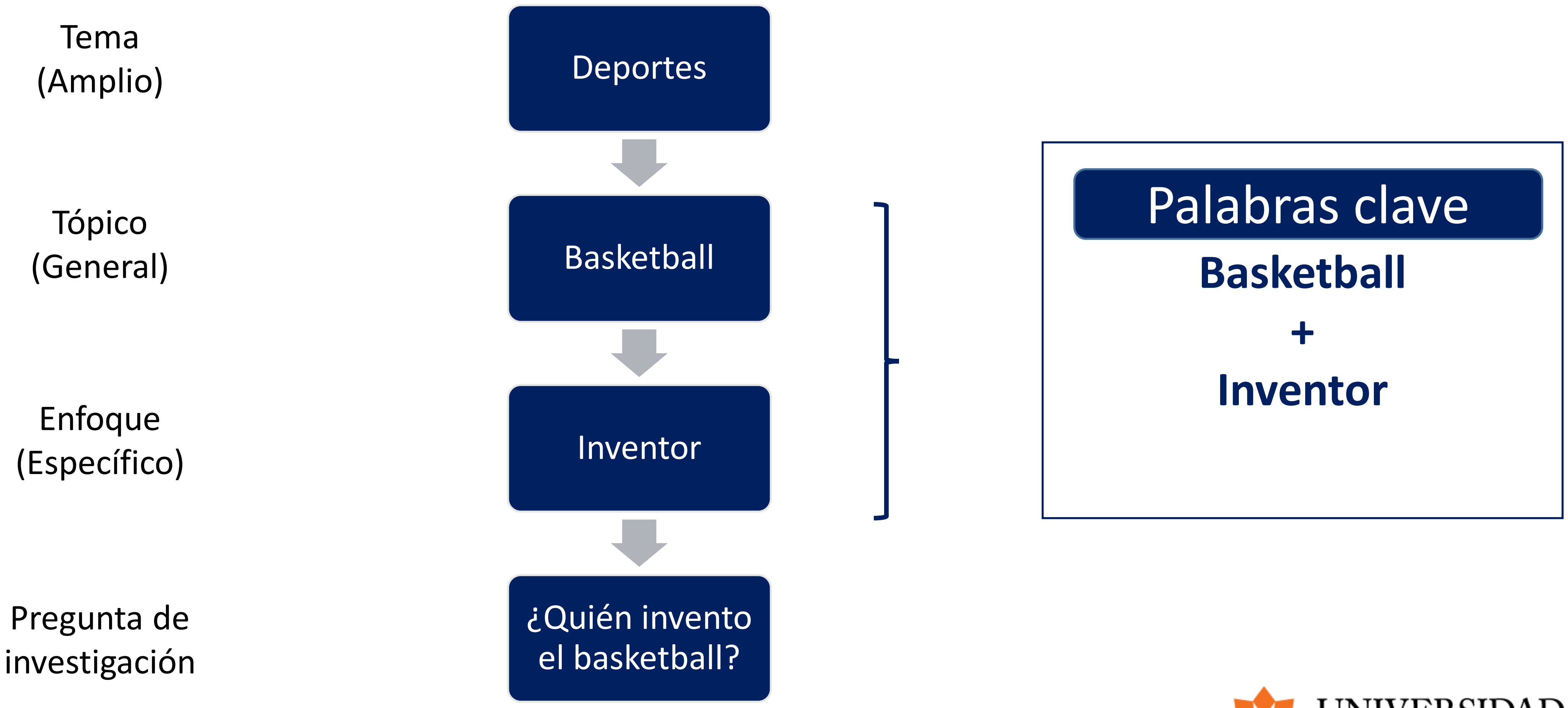
- Introducción
    - Motivación o Problemática
    - Revisión de literatura
    - Objetivo de investigación
- Marco Teórico
    - Hipótesis
- Metodología
- Resultados
- Discusión
- Conclusiones

Pregunta de investigación

¿Por qué es importante el tema de investigación?


AAAAAHHH!! THIS RESEARCH IS IMPOSSIBLE!!
latest journal issue.
Paper With Same Title You Were Going To Give Your Thesis
JORGE CHAM © 2006
AAAAAHHH!! SOMEONE ALREADY DID IT!!
WWW.PHDCOMICS.COM

¿Por qué es importante el tema de investigación?



Tema (Amplio) — Deportes

Tópico (General) — Basketball

Enfoque (Específico) — Inventor

Pregunta de investigación — ¿Quién invento el basketball?

Palabras clave

Basketball

+

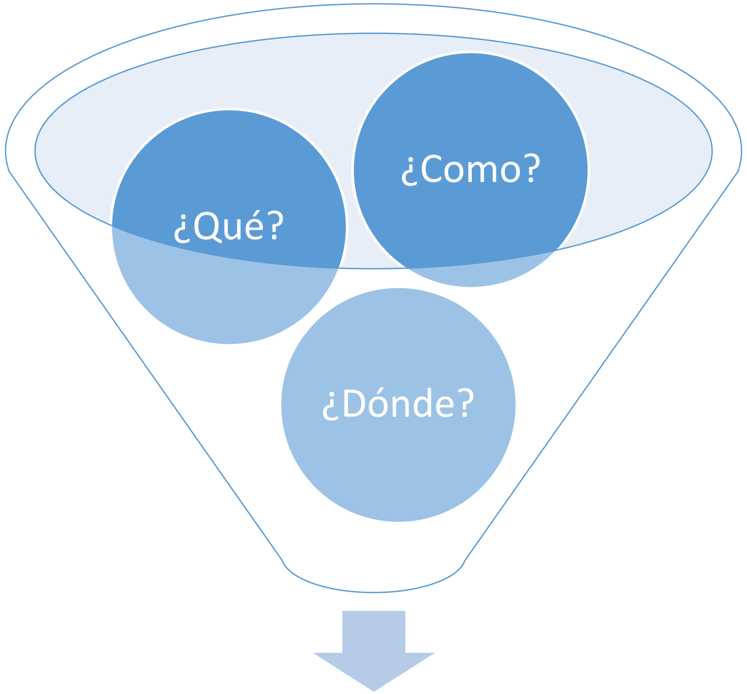
Inventor

Pregunta de investigación

- **Probablemente el ejemplo anterior no es una pregunta de investigación propiamente dicha pues no requiere de análisis…**
- **Es solo para efectos de ejemplo**

UNIVERSIDAD DE LIMA

¿Cómo paso un tema a una pregunta de investigación?



Pregunta de investigación

¿Qué?
¿Qué quieres saber del tema a investigar?

¿Cómo?
¿Cómo vas a llegar a la respuesta?
Tiene que ver con las técnicas de análisis

¿Donde?
¿Dónde vas a realizar el estudio?
¿De dónde vas a sacar la data?

UNIVERSIDAD
DE LIMA

Primer paso ¿Qué?

Riesgos

Información de salud

Android

Primer paso

Segundo paso ¿Cómo?

1. Determinar qué tipo de problema es
2. Cuál es nuestra variable dependiente
3. Determinar cómo se medirán las variables

UNIVERSIDAD DE LIMA

Tercer paso: ¿Dónde?

Aplicaciones Android de Telesalud
(Comparación de aplicaciones)

Mi pregunta de investigación es

¿Se analizan los riesgos y protege la información personal salud en las aplicaciones Android de telesalud?

UNIVERSIDAD
DE LIMA

Analizaremos la investigación

Risk Analysis of Residual Protected Health Information of Android Telehealth Apps (Miller et al., 2019)

Introducción

Problemática (Ejemplo)

The increasing reliance on technology is influencing almost every aspect of modern society, and healthcare is no exception. According to recent studies, 85% of healthcare providers use smart phones during work or training, and the majority of this time is spent using apps (Ozdalga et al. 2012). Almost half of adults in America own smart phones, and half of those adults report having used their phone for retrieving health information (Carroll et al. 2017). There are over 20,000 healthcare related apps across the various mainstream app markets, the majority of which are currently unregulated (Colorafi and Bailey 2016; Lewis and Wyatt 2014). While governing rules and regulations regarding technology currently exist, they are being outpaced by the capabilities of the technologies themselves. In a similar fashion, the healthcare industry has been slow to change and adapt to the robust technology capabilities. Fines for failure to follow HIPAA guidelines can range from $100 to $50,000 per violation and a mistake as simple as disabling a network firewall can cost $400,000 (Goldstein and Pewen 2013). While there are many risks inherent with technology use in healthcare, adoption is becoming more widespread (Washington et al. 2017), even as responsibilities become more diffuse and less clear (Larson 2018).

UNIVERSIDAD
DE LIMA

Revisión de literatura (Ejemplo)

Recent research in the field telemedicine/telehealth has focused on development of and integration mHealth apps (Azfar et al. 2015; Grispos et al. 2013, 2014; Plachkinova et al. 2015). This term applies to a wide variety of health related apps including those used solely for reference purposes or casual health tracking, such as fitness and calorie counting apps (Azfar et al. 2015; Plachkinova et al. 2015). Neither one of these types of apps appear to fall under regulatory guidance (Larson 2018; Washington et al. 2017). This section defines the terms telemedicine, telehealth, and mHealth (mobile health) and explores what laws, rules, and regulations apply to this type of technology.

Objetivo

- The goal of this paper is to examine the regulatory framework and regulatory guidance which applies to telehealth apps.

Marco Teórico

Marco Teórico

- The business associates rule expands the explanation of business associates, contracts, definitions, and responsibilities. These guidelines require that while it is the obligation of the healthcare provider to abide by the HIPAA privacy rule, any other business associations must meet the same security and encryption standards. These protections include providing security and training to guarantee the privacy, accuracy, and availability of ePHI (Goldstein and Pewen 2013). The regulation requires business associates and providers to form a Business Associate Agreement (BAA) that specifies how the data will be handled and protected (Allen et al. 2014).
- A legal example shows that not all technologies are permitted for use as telehealth. According to a news report (Lee et al. 2016), the Oklahoma medical board ruled in January 2014 that Skype could not be used by medical professionals for the purposes of treatment or diagnosis. This article explains that while Microsoft has some form of BAA, Skype is not included in the agreement. In this case, the provider faced reprimand for failing to obtain a BAA prior to using the service to provide care. This ruling reiterates the importance of having a BAA between the healthcare provider and the company providing the software, and that not all technology may be used in the course of providing healthcare. Researchers have published (Barmpatsalou et al. 2013) a review of mobile forensic practices and methods which showcased how data was acquired. These methods include manual, logical, and physical extractions. The authors also discuss differences in operating systems and types of data acquired from an analysis.

Hipótesis

Past research has shown that there is remains a regulatory gray area in the growing field of telehealth apps. The risks associated with end-user use of telehealth apps are currently not well understood. The majority of research has grouped all health-related apps together, under the umbrella term of mHealth. This grouping, while practical for creating taxonomies, does not capture or address HIPAA and FDA guidelines for covered apps. Specifically, three of the four categories of smartphone medical apps proposed by Özdalga et al. (Ozdalga et al. 2012), are reference or personal use. These apps which function as health apps for reference, education, or for the layperson for personal tracking purposes, do not contain ePHI (Larson 2018; Plachkinova et al. 2015). The category of patient care or monitoring, including those apps for diagnosis and treatment of medical conditions, has received the least amount of attention from forensic research literature despite the greater risks from the presence of ePHI.

Given that some apps do leave residual data on devices and some apps do handle ePHI, we pose the following questions:

1) How much residual data remains on an android device as the result of the use of a telehealth app?

2) What components of this information directly violates HIPAA and how? Methodology

According to legislative guidelines and related works in mobile forensics, telehealth apps should be covered by various rules governing ePHI [7, 8, 13, 16, 33]. As such, our hypotheses are:

H1: Telehealth apps leave artifacts on android devices.

H2: The artifacts left after the use of a Telehealth app include legally protected ePHI.

Metodología

Metodología (Diseño de investigación)

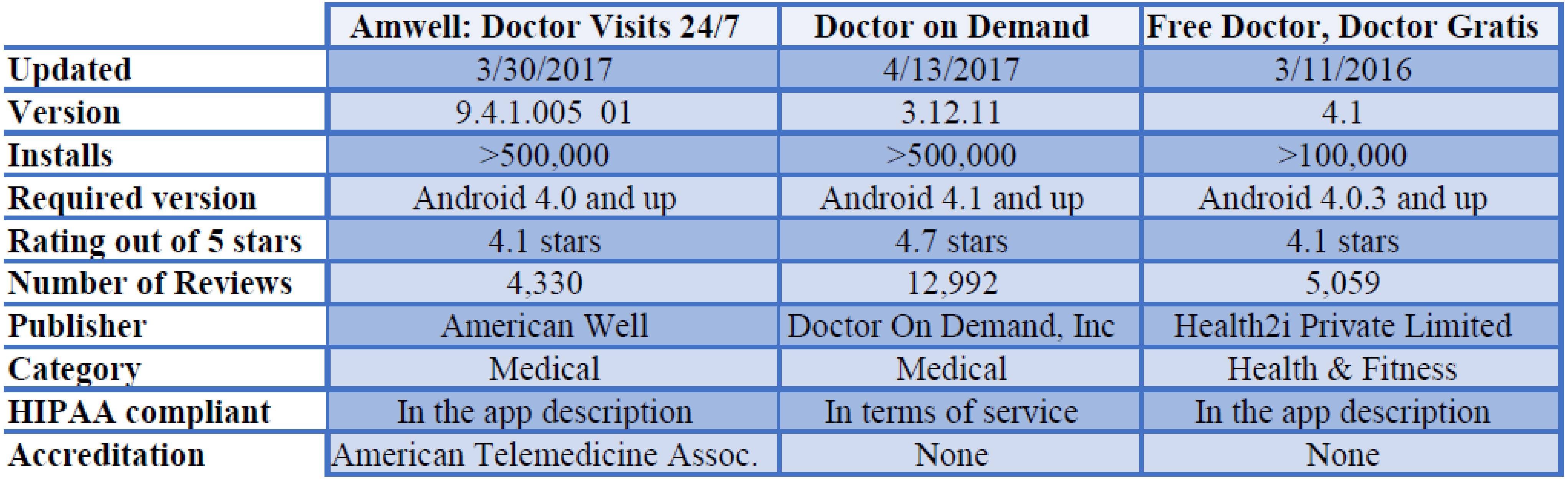
To test the hypotheses, **a forensic analysis on three apps was. The study consisted of a forensic analysis of an Android smart phone loaded with three Telehealth apps. The process was broken into four stages, which include: 1) preparing the smartphone device and installing the health app; 2) loading a data set into the application; 3) process the device using the XRY forensic device to extract the files and artifacts from the resulting memory dumps; and 4) accessing the phone via a standard USB file transfer method. We utilized a Samsung SM-G920T Galaxy S6 LTE-A (carrier: T-Mobile, unlocked) with an operating system of Android 6.0.1 to perform our tests. Prior to performing the case study** steps, a factory reset was performed on the phone to remove any extraneous, or user downloaded apps or residual data not related to the present study.

Three apps were selected from the Google Play store based on a variety of criteria. The criteria include a minimum of 100,000 downloads, a minimum of 4 out of 5-star rating, and a statement that the app is explicitly designed to allow communication with a doctor or other healthcare provider. **These apps include Amwell: Doctor Visits 24/7; Doctor on Demand; and Free Doctor, Doctor Gratis.** The technical details for each of the three apps are given in Table 1.

Técnica de medición

¿Cómo medirás tus variables o darás respuesta a tu pregunta de investigación?

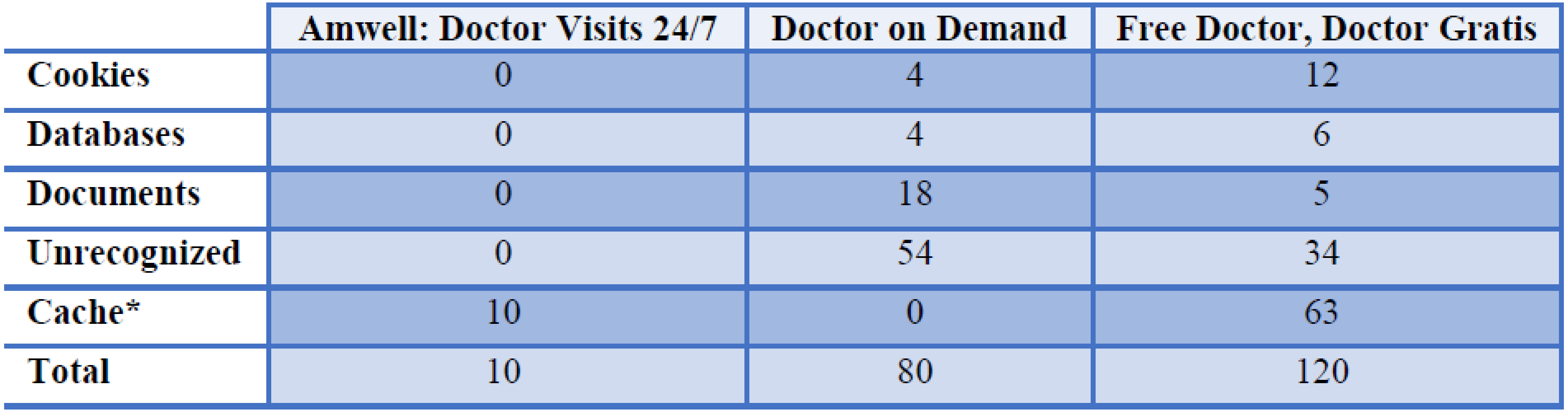
Metodología (Diseño de investigación)



	Amwell: Doctor Visits 24/7	Doctor on Demand	Free Doctor, Doctor Gratis
Updated	3/30/2017	4/13/2017	3/11/2016
Version	9.4.1.005_01	3.12.11	4.1
Installs	>500,000	>500,000	>100,000
Required version	Android 4.0 and up	Android 4.1 and up	Android 4.0.3 and up
Rating out of 5 stars	4.1 stars	4.7 stars	4.1 stars
Number of Reviews	4,330	12,992	5,059
Publisher	American Well	Doctor On Demand, Inc	Health2i Private Limited
Category	Medical	Medical	Health & Fitness
HIPAA compliant	In the app description	In terms of service	In the app description
Accreditation	American Telemedicine Assoc.	None	None

Table 1. App Details

Resultados (1/2)

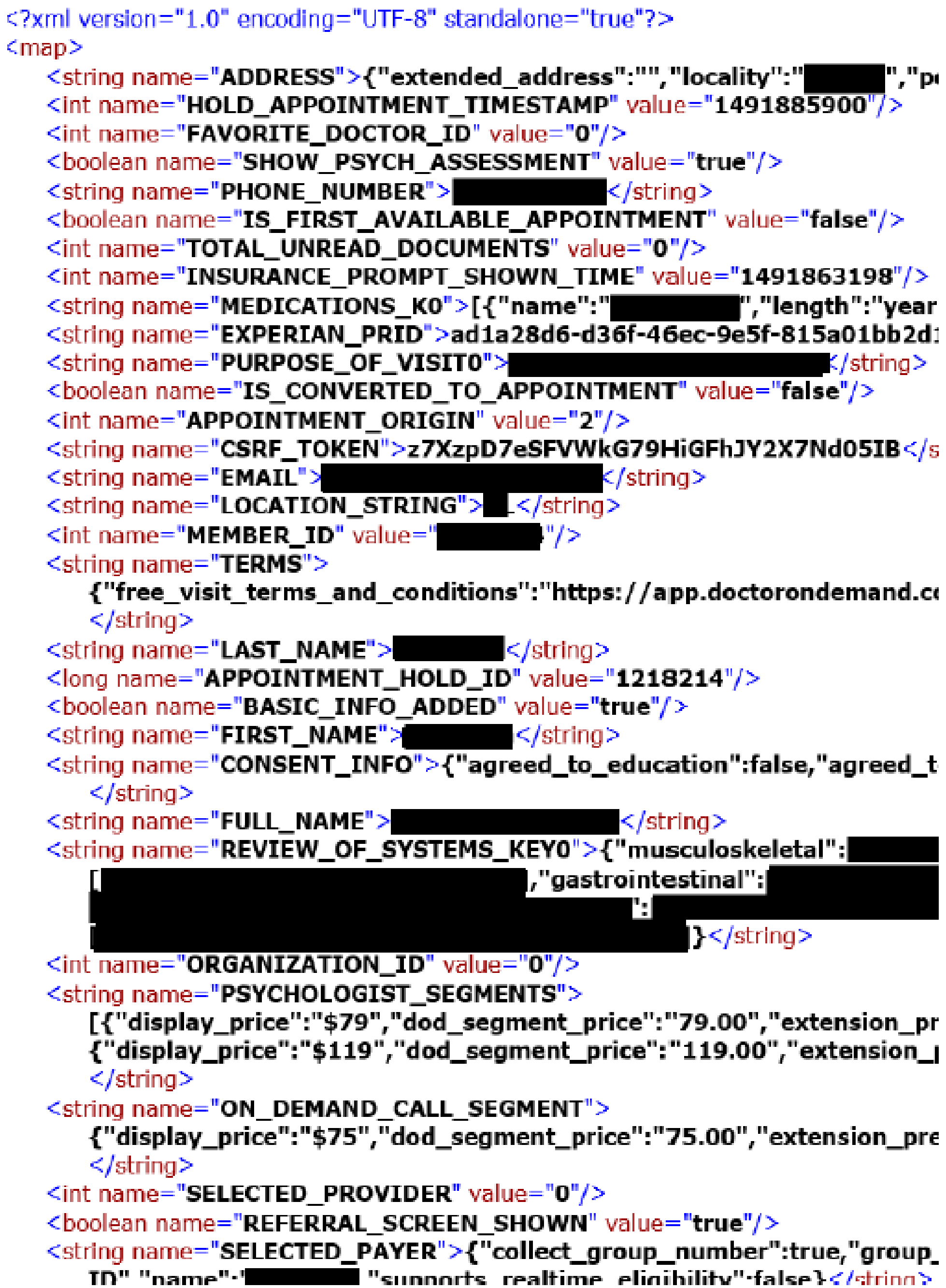


	Amwell: Doctor Visits 24/7	Doctor on Demand	Free Doctor, Doctor Gratis
Cookies	0	4	12
Databases	0	4	6
Documents	0	18	5
Unrecognized	0	54	34
Cache*	10	0	63
Total	10	80	120

Table 2. File count from XRY extraction

Resultados (2/2)

- While sensitive information from the Free Doctor, Doctor Gratis app was not found, the app itself did not comply with HIPAA standards. The app did not request the same level of user information as the other two apps. Despite the lack of account creation initially, this app, was possibly less private and secure than the other two. When attempting to contact a healthcare provider, the app showed a long disclaimer. The app initially stated it was HIPAA compliant in the app’s description, but this disclaimer states that the app is not. The disclaimer includes a warning that any information asked on the app can be visible to the public via a health-based social media site. The contradiction between the app’s store description and the disclaimer can lead to false expectations of privacy by the user and confusion about the app’s purpose.



```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
<map>
    <string name="ADDRESS">{"extended_address":"","locality":"[redacted]","p
    <int name="HOLD_APPOINTMENT_TIMESTAMP" value="1491885900"/>
    <int name="FAVORITE_DOCTOR_ID" value="0"/>
    <boolean name="SHOW_PSYCH_ASSESSMENT" value="true"/>
    <string name="PHONE_NUMBER">[redacted]</string>
    <boolean name="IS_FIRST_AVAILABLE_APPOINTMENT" value="false"/>
    <int name="TOTAL_UNREAD_DOCUMENTS" value="0"/>
    <int name="INSURANCE_PROMPT_SHOWN_TIME" value="1491863198"/>
    <string name="MEDICATIONS_K0">[{"name":"[redacted]","length":"year
    <string name="EXPERIAN_PRID">ad1a28d6-d36f-46ec-9e5f-815a01bb2d
    <string name="PURPOSE_OF_VISIT0">[redacted]</string>
    <boolean name="IS_CONVERTED_TO_APPOINTMENT" value="false"/>
    <int name="APPOINTMENT_ORIGIN" value="2"/>
    <string name="CSRF_TOKEN">z7XzpD7eSFVWkG79HiGFhJY2X7Nd05IB</s
    <string name="EMAIL">[redacted]</string>
    <string name="LOCATION_STRING">[redacted]</string>
    <int name="MEMBER_ID" value="[redacted]"/>
    <string name="TERMS">
        {"free_visit_terms_and_conditions":"https://app.doctorondemand.c
        </string>
    <string name="LAST_NAME">[redacted]</string>
    <long name="APPOINTMENT_HOLD_ID" value="1218214"/>
    <boolean name="BASIC_INFO_ADDED" value="true"/>
    <string name="FIRST_NAME">[redacted]</string>
    <string name="CONSENT_INFO">{"agreed_to_education":false,"agreed_t
        </string>
    <string name="FULL_NAME">[redacted]</string>
    <string name="REVIEW_OF_SYSTEMS_KEY0">{"musculoskeletal":[redacted]
        [redacted],"gastrointestinal":[redacted]
        [redacted]":[redacted]
        [redacted]}</string>
    <int name="ORGANIZATION_ID" value="0"/>
    <string name="PSYCHOLOGIST_SEGMENTS">
        [{"display_price":"$79","dod_segment_price":"79.00","extension_pr
        {"display_price":"$119","dod_segment_price":"119.00","extension_
        </string>
    <string name="ON_DEMAND_CALL_SEGMENT">
        {"display_price":"$75","dod_segment_price":"75.00","extension_pre
        </string>
    <int name="SELECTED_PROVIDER" value="0"/>
    <boolean name="REFERRAL_SCREEN_SHOWN" value="true"/>
    <string name="SELECTED_PAYER">{"collect_group_number":true,"group_
        ID","name":"[redacted]","supports_realtime_eligibility":false}</string>
```

Figure 1. XML file with patient information

Discussion

- While all three apps claim to be HIPAA compliant, only the first app, Amwell: Doctor Visits 24/7, appeared to completely comply with the standards of security necessary for the storing and transmission of ePHI. While encryption in particular is not necessary to protect the data, however, the data should be protected in some way to prevent accidental or inappropriate disclosures [7, 13]. The worst offender for protecting patient information was the Doctor on Demand app. Figure 1 shows the XML text for the user data file com.android.doctorondemand.xml. This file contains personal health data such as current medications, insurance number, full address, symptoms, and more in plain text. This file also shows personally identifiable demographic data such as name, address, and phone number.

Conclusión

- There are several issues with the regulatory landscape relating to healthcare apps. The first problem is that the guidelines are being written by different governing agencies with different motivations. These guidelines do not always line up with one another, creating gaps and conflicts. The second problem relates to roles. Vendors, healthcare providers, business associates, and patients all have differing responsibilities, and not all of them are covered under HIPAA and related regulations (Goldstein and Pewen 2013). These different roles can lead to confusion regarding whose responsibility is to protect ePHI, and how that role can be enforced.
- The results of the case study portion illustrate the vast differences in how patient information is being handled and stored. Our examination of these apps support the first hypothesis. All the apps left some residual data on the phone. The second hypothesis is less clearly supported. The first app, Amwell: Doctor Visits 24/7, does not support the hypothesis that residual ePHI exists from usage of the app. The second and third apps, however, do support this hypothesis. Patient information, including ePHI, was found.
- The case studies demonstrate the need for clearer regulatory guidance in healthcare-based apps. While the most detailed information was found from the Doctor on Demand app, it was the Free Doctor, Doctor Gratis app which is the most significant example of the privacy issues with unregulated telehealth apps.

Contribution

- ¿Qué aporta tu investigación? ¿A quien le sirve?

Rubrica para paper

Rúbrica	Satisfactorio (4 puntos)	Aceptable (2 puntos)	Deficiente (1 punto)
Introducción	El estudiante redacta claramente la motivación, revisión de literatura (estado del arte) y el o los objetivos de investigación	El estudiante solo redacta claramente dos aspectos de la introducción (motivación, revisión de la literatura y los objetivos).	El estudiante solo redacta claramente un aspecto de la introducción.
Marco Teórico e Hipótesis	El estudiante define claramente el marco teórico y las hipótesis	El estudiante define de manera clara solo marco teórico o las hipótesis	El estudiante define con poco fundamento el marco teórico y las hipótesis
Metodología	El estudiante define de manera satisfactoria la metodología incluyendo claramente el objeto y sujeto de estudio y como lo medirá	El estudiante define de manera aceptable la metodología incluyendo el objeto y sujeto de estudio y como lo medirá.	El estudiante define de manera deficiente la metodología incluyendo el sujeto de estudio y como lo medirá.

Rubrica para paper

Rúbrica	Satisfactorio (4 puntos)	Aceptable (2 puntos)	Deficiente (1 punto)
Resultados y Discusión	[redacted]	El estudiante define claramente los resultados y remediaciones de acuerdo con los objetivos planteados	El estudiante define de manera muy general los resultados y/o las remediaciones.
Conclusiones y Contribución	[redacted]	El estudiante define de manera consistente las conclusiones y su contribución a la literatura.	El estudiante define de manera deficiente las conclusiones y la contribución.
Uso de APA	[redacted]	El estudiante utiliza APA para las citas y referencias; y por lo menos 15 referencias.	El estudiante utiliza poco APA para las citas y referencias; y usa menos de 10 referencias.
Exposición	[redacted]	El estudiante expone claramente paper y conoce al detalle su tema.	El estudiante conoce de manera general su tema pero no profundiza en su explicación.

UNIVERSIDAD
DE LIMA

Indicaciones adicionales

- Seguir el formato entregado.
- El *paper* será un trabajo experimental.
- Entrega parcial: antes de la primera sesión de la semana 6 (Introducción y Marco Teórico e Hipotesis).
- Entrega Final: antes de la primera sesión de la semana 12.
  - El paper debe tener ***como mínimo 10 paginas máximo 12*** incluido referencias.

UNIVERSIDAD DE LIMA

Temas

- Smart Cities
- Blockchain
- Telemedicina
- Smart Building
- Wearables
- Drones
- Ciberinteligencia
- Dark Net
- Smart Cars
- BioHacking
- Móviles