# ESTUDIO DE LAS TÉCNICAS DE PRIVACIDAD BASADAS EN AMBIENTES SENSIBLES AL CONTEXTO.

**MABEL YADIRA COGOLLO**

**Ingeniera de Sistemas – Especialista en Finanzas**


**UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA - UNAB**
**FACULTAD DE INGENIERÍA DE SISTEMAS**
**MAESTRÍA EN TELEMÁTICA - MODALIDAD INVESTIGACIÓN**
**GRUPO DE INVESTIGACIÓN -TECNOLOGÍAS DE INFORMACIÓN (GTI)**
**LÍNEA INVESTIGACIÓN TELEMÁTICA**
**BUCARAMANGA**
**2016**

# ESTUDIO DE LAS TÉCNICAS DE PRIVACIDAD BASADAS EN AMBIENTES SENSIBLES AL CONTEXTO.

**MABEL YADIRA COGOLLO**

**Trabajo de grado para optar al título de Magister en Telemática, en la modalidad de Investigación**

**Director: Ing. JOSÉ GREGORIO HERNÁNDEZ SÁNCHEZ M.Sc.**

**UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA -UNAB**
**FACULTAD DE INGENIERÍA DE SISTEMAS**
**MAESTRÍA EN TELEMÁTICA - MODALIDAD INVESTIGACIÓN**
**GRUPO DE INVESTIGACIÓN -TECNOLOGÍAS DE INFORMACIÓN (GTI)**
**LÍNEA INVESTIGACIÓN TELEMÁTICA**
**BUCARAMANGA**
**2016**

Nota de aceptación:

_____

_____

_____

_____

_____

_____

Firma del Presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bucaramanga, Enero de 2016

## DEDICATORIA

Quiero dedicar éste trabajo a Dios, por haberme permitido culminar los estudios y que por su amor infinito intervino cada día enviándonos su luz, sabiduría, amor y paz para recibir todas las bendiciones que nos tiene reservadas.

A mi hermosa familia, a mi amado esposo por su paciencia, comprensión y apoyo; a mis hijas, mis más preciados tesoros, por su admiración y respeto; y a mi madre querida, mi soporte incondicional, por sus oraciones, su voz de aliento y sabios consejos. Este logro también es de ustedes.

## AGRADECIMIENTOS

A la Universidad Autónoma de Bucaramanga, un profundo y sincero agradecimiento por su interés en capacitar y creer en sus docentes, por valorar mis capacidades, haciéndome becaria para el último semestre y así poder culminar mis estudios de la maestría en Telemática.

Igualmente, mi sincero agradecimiento a la Ingeniera Claudia Liliana Zúñiga, directora del anteproyecto, por su apoyo durante el desarrollo de la fase inicial de la investigación; al Ingeniero José Gregorio Hernández, director de proyecto, encargado de orientar los resultados de la investigación, para llevar a feliz término este proceso. De igual manera, quiero agradecer a los docentes de la Maestría, que a lo largo del programa compartieron sus conocimientos y con su cátedra, hicieron un gran aporte a la consolidación de éste proceso.

**CONTENIDO**

**Pág.**

## INDICE DE IMÁGENES

**Pág.**

## INDICE DE TABLAS

**Pág.**

## RESUMEN

**TÍTULO: Estudio de las técnicas de privacidad basadas en ambientes sensibles al contexto**

**AUTORES: Ing. Mabel Yadira Cogollo (Estudiante)**

© y M.Sc Claudia Liliana Zúñiga, (directora fase 1) Universidad Santiago de Cali

M.Sc José Gregorio Hernández (director fase 2) Universidad Autónoma de Bucaramanga

La presente investigación desea contribuir al desarrollo científico, tecnológico e innovación en la gestión de la privacidad del usuario en ambientes sensibles al contexto. En este documento se describen las políticas, los principios, los mecanismos y las técnicas de privacidad recomendadas por las autoridades mundiales en estandarización y telecomunicaciones - ISO, ITU, W3C y GSMA - , las ventajas de su implementación, desde la encriptación asimétrica, el software de gestión de datos, y las plataformas de acceso unificado, en sectores de productividad, incluyendo la educación.

Se hace mención de los programas exitosos de ciudades y *smart campus* a nivel nacional y mundial, teniendo en cuenta la adopción del programa BYOD y sus aplicaciones. Basados en lo anterior, se propuso un esquema donde se muestran los estándares para establecer técnicas y mecanismos de seguridad en ambientes sensibles al contexto, que permitan aumentar el nivel de privacidad del usuario. Para documentar la aplicación de la propuesta, se implementó una red piloto con NAC PacketFence, de tipo Open Source, que permitió valorar el modelo propuesto para un entorno urbano real; se realizaron pruebas en PC's, celulares y dispositivos móviles. Se obtuvieron resultados favorables en su ejecución,

destacándose la autenticación de usuarios, la implementación de VLANs por grupo y la viabilidad del programa BYOD en el Smart Campus de la Universidad Autónoma de Bucaramanga.

**Palabras Clave:** Privacidad, leyes de privacidad, principios de privacidad, técnicas de privacidad, estándares de privacidad, seguridad en redes, contexto, computación en entornos sensibles, aplicaciones sensibles al contexto, ciudades inteligentes, campus inteligentes, trae tu propio dispositivo, control de acceso a la red, NAC, PacketFence.

## ABSTRACT

The following research aims to contribute to the scientific, technological and innovative growth in user's privacy management in context-aware systems. Studied in various disciplines, in this document a description is made of all policies, principles, mechanisms and privacy techniques recommended by world standardization and telecommunications authorities, such as ISO, ITU, W3C and GSMA, taking into account the advantages of their implementation thanks to the exploitation of the technologies developed, like asymmetric encryption, data management software, unified access platforms, in diverse sectors of productivity, including education.

Also, successful programs in smart cities and smart campus are mentioned below, national and international experiences; the adoption of the BYOD and its applications were also taken into account. Based on these, a standards scheme was proposed to establish the security techniques and mechanisms in context-aware systems that allow the increase of the level of privacy for user's information. To supply documentary evidence of the application proposed, a pilot network was implemented using PacketFenceNAC, Open Source Type, which allowed the

assessment of the standards proposed for a real urban environment;; tests were executed on PCs, smartphones and mobile devices. Positive results were obtained during the tests execution, being user's authentication, VLANs group implementation and viability of BYOD program in the Smart Campus of the Autonomous University of Bucaramanga, UNAB, highlights of the project.

**Keywords:** privacy, privacy laws, privacy principles, privacy techniques, privacy standards, network security, context, context-aware computing, context-aware applications, smart city, smart campus, Bring Your Own Device, network access control, PacketFence.

**GRUPO DE INVESTIGACIÓN**: Tecnologías de Información - GTI – Línea de Investigación telemática

**PROGRAMA**: Maestría en Telemática
**UNIVERSIDAD AUTÓNOMA DE BUCARAMANGA - UNAB**

# INTRODUCCIÓN

Con el advenimiento de las tecnologías de la información y las comunicaciones, la privacidad ha pasado de ser comprendida como el derecho a la soledad, el respeto de la intimidad, convirtiéndose en un símbolo de la libertad individual para expresarse y ser reconocido en la complejidad de la interacción virtual. La privacidad ha pasado de ser una noción netamente sociológica a ser una solución tecnológica que basada en unos principios relacionados a la información de un individuo en específico, determina los cambios que se hagan sobre la percepción de los avances tecnológicos y las nuevas formas de interacción social.

La presente propuesta de investigación desea contribuir al desarrollo científico, tecnológico e innovador en los ámbitos de cómo se presenta la privacidad del usuario en los ambientes sensibles al contexto; asociado al uso de dispositivos móviles en los espacios donde la interacción de usuarios y dispositivos inteligentes forman parte de la vida cotidiana como es el campus de la Universidad Autónoma de Bucaramanga.

Con la introducción del concepto de Computación Ubicua, por Mark Weiser, en 1993, lo que en un principio era tan solo una propuesta, ahora es una realidad: la capacidad de los computadores personales se ha trasladado a los dispositivos móviles. No obstante, el crecimiento de este fenómeno es gracias a los avances tecnológicos en materia de infraestructura de redes; la conectividad ya no es un lujo de pocos, es un servicio común que está relacionado con cuán desarrolla es una comunidad, por lo tanto, la virtualidad ya no es un equivalente a la realidad misma, se encuentra por encima de ella, con prácticas incluyentes que tienden a anticipar los resultados de las actividades de cualquier individuo. Es entonces cuando la interacción con el dispositivo móvil se expande a todo entorno, dando lugar a ambientes inteligentes capaces de adquirir información y adaptarse a las

necesidades del usuario; ésta información es denominada *información contextual* y el entorno, como *contexto sensible*, generando una serie de datos como ubicación geoespacial, recursos cercanos y tareas, por lo tanto, los datos del contexto que pueden ser detectados, inferidos o ingresados por el usuario directamente, exigen mecanismos de recolección, almacenamiento, gestión y eliminación, convirtiéndose en la materia prima de todo sistema efectivo.

Con base en lo anterior, se presentó la propuesta de trabajo enfocado al cómo los datos sensibles de los usuarios pueden ser vulnerados y los niveles de seguridad brindados por los entornos inteligentes y las aplicaciones móviles utilizadas por los cibernautas, son tan bajos que infringen la privacidad de la información suministrada por los usuarios y su contexto. La relación entre las aplicaciones sensibles al contexto – contexto – usuario, se obtiene a través del dispositivo donde se ejecuta (donde un dispositivo puede ser un computador portátil, un Celular inteligente, un PDA,…..), la interacción del usuario con la aplicación, se realiza a través de la interfaz de la aplicación que sirve de medio para la comunicación ente el usuario y el dispositivo, esta comunicación se da en las dos vías.

Ahora bien, ¿qué tipo de técnicas y mecanismos de seguridad deben brindarse en un entorno inteligente para tratar de minimizar la vulnerabilidad a la privacidad de la información suministrada por los usuarios?

Para lo anterior, se propone un esquema de estándares para establecer técnicas y mecanismos de seguridad en entornos inteligentes, que permitan aumentar el grado de seguridad y privacidad de la información del usuario en ambientes sensibles al contexto. Y por ello, el proyecto se enfoca en hacer una revisión de las diferentes técnicas y mecanismos que existen para controlar la privacidad en ambientes inteligentes.

Esta realidad trajo consigo varios interrogantes relacionados con la seguridad en entornos inteligentes, en especial con la privacidad de los usuarios. Si bien la primera puede solucionarse como un aspecto técnico, la privacidad ha sido considerada durante siglos como un indicador fundamental de la personalidad individual. Este es el principal objetivo de este proyecto: ilustrar los grandes retos que deben superarse para ofrecer una plataforma robusta que garantice la seguridad y la privacidad de los usuarios de una red en un entorno sensible.

Existiendo tres capas para la ejecución de la minería de datos (*sensing, network, control & services*), la nube ha pasado de ser un recurso exógeno a ser el fundamento primordial de todas las plataformas activas que basan sus operaciones en el **Internet de las Cosas** (IoT), el modelo *Bring Your Own Device* (B.Y.O.D.) para mejorar el rendimiento y la eficiencia de los procesos al interior de la compañía, y la interfaz de experiencia de usuario, *User Experience*, (UX), todos los anteriores, presentes en el desarrollo de un *Smart Campus* para un entorno académico. En la actualidad, la minería de datos ha reducido las nociones de **seguridad y privacidad** a procedimientos y protocolos de acción, que han abierto las barreras de la interacción a través del concepto de la **compatibilidad**. Si la nube es el principal escenario para llevar a cabo todos los procesos necesarios para la integración de los usuarios en un entorno sensible, la viabilidad de la participación física de los mismos determina, de forma directa, el correcto uso que puedan dar los participantes de la red a la **privacidad** de sus datos, teniendo en cuenta el registro de un perfil.

Además, productos y efectos concretos de la investigación que permite que con la revisión de la literatura se realice un estudio diagnóstico de los estándares, técnicas y mecanismos de privacidad implementados en aplicaciones móviles para ambientes sensibles al contexto, para luego proponer un esquema de estándares de privacidad que permitan manejar grados de seguridad de la información del usuario.

Abordada desde varias disciplinas, en este documento se describen las políticas, los principios, los mecanismos y las técnicas de privacidad recomendadas por las autoridades mundiales en estandarización y telecomunicaciones, como la ISO, la ITU y la IEC, las ventajas de su implementación gracias al aprovechamiento de las tecnologías desarrolladas, desde la encriptación asimétrica, pasando por software de gestión de datos, hasta plataformas de acceso unificado, en diversos sectores de productividad, incluyendo la educación. De igual manera, se hace una descripción detallada de los programas exitosos de ciudades y campus universitarios inteligentes a nivel nacional y mundial, teniendo en cuenta su incursión en la adopción del programa BYOD y sus híbridos subsecuentes.

Al implementar los principios de privacidad en el contexto de la Universidad Autónoma de Bucaramanga, los usuarios son toda la comunidad universitaria en roles definidos como: empleados administrativo y docentes, estudiantes e invitados, autenticando sus dispositivos en la red con respecto a los criterios de seguridad, para que pueda acceder a los servicios de nuestro Smart Campus. Para documentar la aplicación de la propuesta presente, se implementó una pequeña red con NAC PacketFence que es *Open Source*, que permite el desarrollo y la ejecución de los estándares del modelo propuesto para un entorno urbano real, en este caso, el campus de la Universidad Autónoma de Bucaramanga como un *Smart Campus*. Con esto se desea aportar un recurso valioso a la modernización de nuestra alma máter, posicionándose como un referente académico en nuestro país.

El documento se estructura de la siguiente manera:

1. Marco Referencial
2. Proceso Investigativo
3. Datos encontrados
4. Resultado de la Investigación y Conclusiones y Recomendaciones.

# 1 PLANTEAMIENTO DEL PROBLEMA Y JUSTIFICACIÓN

El concepto de Ambientes Sensibles al Contexto, lleva también a pensar que en la sociedad del conocimiento y en el ecosistema digital, la información que se maneja en los ambientes inteligentes dependiendo del contexto en que se mueva el usuario, puede ser pública o privada. Esta propuesta de investigación tiene como propósito identificar las técnicas y mecanismos de privacidad que permitan a los usuarios sentir confianza en el manejo de su información a través de los dispositivos móviles y el tratamiento que recibirá por las aplicaciones que la requieran.

Los niveles de seguridad brindados por los entornos inteligentes y las aplicaciones móviles utilizadas por los cibernautas, pueden llegar a vulnerar la privacidad de la información suministrada por los usuarios en el contexto.

La relación entre las aplicaciones sensibles al contexto – contexto – usuario, se obtiene a través del dispositivo (donde un dispositivo puede ser un computador portátil, un Celular inteligente, un PDA), donde la interacción del usuario con la aplicación, se realiza a través de la interfaz que sirve de medio para la comunicación ente el usuario y el dispositivo.

Teniendo en cuenta lo anterior, la propuesta de investigación plantea lo siguiente:
¿Qué tipo de técnicas y mecanismos de privacidad deben brindarse en un entorno inteligente para minimizar la vulnerabilidad de la información suministrada por los usuarios?

Es importante definir que el establecimiento de técnicas y mecanismos de privacidad implementados en los entornos inteligentes permitirían disminuir problemas de seguridad y de vulnerabilidad en la información de los cibernautas.

En atención a ésta problemática, los modelos de entornos inteligentes se caracterizan por el uso de infraestructuras con tecnologías de información y de comunicaciones para obtener, almacenar, actualizar y emplear eficientemente la información; lo cual permite integrar servicios con los sistemas; además de mejorar la infraestructura de los contextos (privados: empresas, instituciones, etc; o públicos: entornos académicos, ciudades inteligentes, entro otros). Aunque las aplicaciones cuentan con esquemas de seguridad implementados para que el usuario sea quien disponga el activarlos o no, esos esquemas no son tan seguros y pueden ser vulnerados para conseguir la información del usuario.

Con el estudio de las técnicas de privacidad implementados y desarrollados para ambientes inteligentes, también se analiza el grado de confianza por parte del usuario al ser utilizadas por él; de igual manera se pretende establecer que tan vulnerables resultan ser la información tanto del usuario como de los sistemas de información en un entorno sensible de corte académico. Por lo tanto, es vital contar con técnicas estándares que permitan efectuar una valoración eficaz de los grados de seguridad y privacidad de la información en ambientes inteligentes, que conciban alto grado de confianza para que las aplicaciones que provean servicios, garantizando la seguridad y privacidad de la información del usuario.

# 2 OBJETIVOS

## 2.1 OBJETIVO GENERAL

Proponer un esquema de estándares para establecer técnicas y mecanismos de seguridad en entornos inteligentes, que permitan aumentar el grado de privacidad y seguridad de la información del usuario en ambientes sensibles al contexto.

## 2.2 OBJETIVOS ESPECÍFICOS

- Realizar una revisión de las diferentes técnicas y mecanismos actuales para controlar la privacidad en ambientes inteligentes.

- Realizar un estudio diagnóstico de los estándares, técnicas y mecanismos de privacidad implementados en aplicaciones móviles para ambientes sensibles al contexto.

- Proponer un esquema de estándares de privacidad que permitan manejar grados de seguridad de la información del usuario.

- Desarrollar una prueba de aplicación del modelo propuesto en un entorno urbano real.

# 3 MARCO REFERENCIAL

El marco referencial del presente proyecto se fundamenta en la privacidad de la información del usuario en el contexto, los mecanismos y técnicas de privacidad en entornos sensibles e inteligentes, teniendo en cuenta la estructura de la red ofrecida por el proveedor de servicios, las características del entorno y la información compartida por el usuario desde su dispositivo móvil.

## 3.1 LA PRIVACIDAD

### *3.1.1 Definición de Privacidad*

- El Diccionario de la real academia de la lengua española define la privacidad como el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión. (Real Academia Española, 2014), haciendo referencia a la propiedad individual que no pertenece a lo público.

- La privacidad entendida desde la disciplina jurídica ha sido considerada a lo largo de los años como una de las principales referencias en los derechos de los individuos. Se tiene conocimiento que en el acto de paz de la justicia Inglesa de 1361, el escuchar una conversación sin autorización podría ser considerada un crimen. (Langheinrich M. , 2005).

- Siglos más tarde, el parlamento Sueco ordenaba que cualquier información retenida por el gobierno debería ser utilizada para propósitos legítimos en 1776. A mediados del siglo XIX, en Francia se prohíbe la publicación de datos privados, decisión que fue adoptada, años más tarde, por el código

criminal de Noruega. Con la publicación del artículo "*The Right to Privacy*"[1] en 1890, la privacidad fue definida como el derecho a estar solo. Las apreciaciones dadas por sus autores, (Warren & Brandeis) estuvieron motivadas por oficio de los fotógrafos y los periódicos a quienes consideraban como una amenaza a la vida privada y doméstica.

Sin embargo, con la declaración universal de los derechos humanos la privacidad individual es protegida en el artículo 12, siendo entendida como el derecho a la protección de la ley contra cualquier interferencia o ataque que vaya dirigida contra la intimidad, la familia y el hogar de cualquier ser humano (ONU (United Nations Organization), 1948).

- En la computación, la privacidad ha recibido varias definiciones durante las distintas etapas históricas. Según (Westin, 1968), en su libro de "*Privacy and Freedom*"[2], la privacidad es la declaración de los individuos, grupos e instituciones para determinar por sí mismos, cuándo, cómo y en qué alcance de la información a cerca de ellos se comunica a los otros; esta es considerada como la primera y más acertada de las definiciones para comprender la relevancia de la misma en los diferentes niveles de procesamiento, análisis y publicación de la información.

### *3.1.2 Tipos de Privacidad*

Westin definió cuatro tipos de privacidad: Soledad, Intimidad, Anonimato y Reserva:

- **Soledad**: una persona está sola y está libre de la observación de los otros
- **Intimidad**: un pequeño grupo se separa de otros para estar solos
- **Anonimato**: cuando una persona está perdida en la multitud

[1] Derecho a la privacidad
[2] Privacidad y Libertad

- **Reserva**: establecimiento de las barreras sicológicas contra la intrusión.

La importancia del anonimato se ha ido incrementando dramáticamente con el crecimiento de la Internet, las redes sociales y las interacciones en línea.

Holvast y Rosenberg, hablan desde el punto de vista práctico donde muestran la privacidad desde los siguientes aspectos:

- **Privacidad Territorial**: es la protección de un área doméstica o física que rodea a una persona como el hogar, el sitio de trabajo, o espacios públicos.
- **Privacidad Corporal**: es la protección de una persona contra la interferencia indebida tal como pruebas genéticas, búsquedas físicas, testeo de drogas e información que viole el sentido moral del individuo.
- **Privacidad de la Información personal**: es el establecimiento de reglas para controlar los datos personales que puedan ser reunidos, almacenados, procesados o divulgados selectivamente.
- **Privacidad de la Comunicación**: se entiende como la cobertura de la privacidad y la seguridad de correo, teléfono, email, y otras formas de comunicación (protección de los datos) se ha convertido en uno de los aspectos más significativos de la privacidad.

### *3.1.3 La Taxonomía de la Privacidad*

En la taxonomía de la privacidad según (Solove), se acepta que tal vez haya razones válidas por las cuales la ley no debería estar involucrada o que los intereses compensatorios de la ley deberían prevalecer hasta cierto punto, esto es lo que se conoce como un reclamo del derecho absoluto a la privacidad, pero ésta flexibilidad es necesaria aun cuando un derecho absoluto es concedido. Muchos de los problemas de privacidad causados por la tecnología han de requerir involucrarse en esta clase exacta de balance de intereses, y si la privacidad es presentada en algo cercano al todo o nada, los consumidores a menudo escogerán nada.

De igual manera Solove, apoyándose en la perspectiva de Lillian BeVier, presenta la visión de la privacidad como una palabra cambiante según las circunstancias, usada denotativamente para designar un amplio rango de intereses salvajemente dispares, que van desde la confidencialidad de la información personal hasta la autonomía reproductiva, y connotativamente para generar benevolencia en nombre de cualquier interés que sea aseverado dentro su nombre. (BeVier, 1995).

Así mismo, Solove identifica cuatro grupos de actividades que forman parte del concepto general de privacidad y que constituyen riesgos y problemas para los ciudadanos: Recolección de la información, Procesamiento de Información, Divulgación de la información e Invasión de la Privacidad. Cada uno de ellos se divide a su vez en subactividades, donde se puede observar que la vida de las personas puede verse afectada negativamente.

#### *3.1.3.1 Recolección de la Información (Information Collection)*

Las entidades que recogen la información se denominan *Data Holders*, y la información puede ser recolectada por medio de la vigilancia y la interrogación. La primera puede llevar a la auto-censura e inhibición, ya que su propósito es mantener el control del comportamiento humano, sea por medio de limitaciones, monitoreo o incremento en las reglas y normas que un individuo deba cumplir. La interrogación, por otra parte, puede ser interpretada como la presión sobre los individuos a divulgar información propia o ajena. Esto puede representar varios beneficios para aquellos que quieren averiguar información que otros deseen conocer, sin embargo, éste método puede ser nocivo ya que a éste se le asocia con la coacción y la intimidación. A pesar de lo anterior toda interrogación sucede con pleno conocimiento del individuo mientras que la vigilancia puede ser clandestina, no consensuada y sin autorización. Otro aspecto a tener en cuenta es la gran capacidad de distorsión que la interrogación puede tener, ya que es el

resultado del control que el interrogador ejerza sobre la información que es obtenida, y la posterior interpretación que causa cualquier tipo de revelación.

En la computación, cualquier tipo de vigilancia e interrogación cumple con las características ofrecida en el párrafo anterior. La vigilancia ha llegado a extremos donde, bajo la premisa del interés común, se violan las libertades individuales; los recientes casos ocurridos en Estados Unidos, donde la Agencia Nacional de Seguridad (NSA) utilizaba la información provista por las grandes compañías de sus usuarios, para hacer seguimiento de posibles atentados, dejó en entredicho la viabilidad de una ley absolutista de seguridad, desconociendo los principios fundamentales de la 5ª enmienda. (BBC News, 2014), (The Huffington Post, 2013). La vigilancia con control excesivo sobre los individuos y la manipulación incorrecta de la información de los mismos, para fines distintos a los de la seguridad se distorsiona en el espionaje; si bien las naciones tienen leyes que facultan a sus agencias de seguridad para proteger a sus ciudadanos de cualquier amenaza interna o externa, el crecimiento desmedido de utilización de dispositivos móviles cuyas aplicaciones permiten rastrear la geolocalización de los usuarios, ha facilitado la percepción de que cualquier intento por mantener la privacidad de un individuo resulta en vano a pesar de los esfuerzos que el sistema jurídico y los mismos usuarios quieran hacer.

La interrogación puede ser ejercida de forma indirecta sobre un usuario al momento de que éste acepta los términos y condiciones de un servicio en la red; los protocolos de privacidad que un dispositivo móvil emplea pueden ser fácilmente vulnerados debido a la falta de compatibilidad entre las aplicaciones ejecutadas, lo anterior sumado al desconocimiento del usuario de los mismos, comprende una de las principales causas de la divulgación y manipulación de datos sensibles del usuario, de ahí que sea necesario establecer una uniformidad en los parámetros de diseño en las aplicaciones móviles cuyos servicios requieran la introducción de datos de alto nivel de privacidad. La creación de un perfil de

usuario se basa en la información esencial de un individuo, ésta información aparentemente es estática durante el tiempo que permanezca activo dicho usuario en el servicio; el nivel de protección que se pueda ofrecer al usuario debe de estar incluido en las políticas de calidad del servicio, haciendo de la interrogación un parámetro benévolo para el rescate y manipulación de la información, con preguntas de alto nivel que garanticen su privacidad.

#### *3.1.3.2 Procesamiento de la Información (Information Processing)*

Solove, la define como todo uso, almacenamiento y manipulación de los datos que hayan sido recolectados, la conexión entre los datos y las personas a quienes les pertenecen, con excepción de la divulgación, ya que la transferencia de cualquier dato no debe ser entendida como la revelación o publicación de la información a una persona distinta de su propietario. El procesamiento de la información incluye:

1. *Agrupación* (Aggregation) (pág. 505), es la colección de la información conjunta. Un solo dato no puede decir mucho a cerca de un individuo, pero el conjunto de datos y la capacidad combinatoria de los mismos describen el perfil del usuario. La sinergia que ocurre en la combinación de la información al momento de ser analizada y agrupada ha de revelar nuevos hechos que no son percibidos en un primer momento. Lo anterior abre la posibilidad de combinar varias piezas de información personal, haciéndolo más extenso y mucho más fácil de procesar en la era actual de la información en formas sofisticadas y robustas.

   En la actualidad, la agrupación representa un gran beneficio para determinar los comportamientos del usuario de acuerdo a su historial: empresas con servicios en líneas, bancos, incluso otras personas pueden tener una mayor comprensión de las preferencias y la experiencia del usuario. La agrupación comparte ciertas características con la vigilancia debido a la forma de

adquisición de la información, pero la agrupación es indirecta ya que ocurre mientras se procesa el dato recolectado.

La privacidad del dato agrupado puede ser vulnerada de forma inescrupulosa ya que al tener un registro completo de un individuo, por ejemplo en el caso financiero, puede llevar a que su vida se vea afectada por las decisiones que se tomen a partir de la información obtenida[3]. Solove lo denomina la *persona digital* (pág. 507), persona que puede tener serias repercusiones sobre el individuo en el espacio real, ya que el crecimiento de la persona digital es proporcional al crecimiento del espacio digital, entre más espacio haya para esa persona de compartir información, aumenta la capacidad combinatoria de los mismos, revelando facetas de su vida que en algunos casos puede ser mal interpretada o incompleta.

2. *Identificación (Identification).* Consiste en conectar la información a los individuos, esta sucesión de datos debe ser con un individuo en particular. Cole (2001) describe a la identificación como "la capacidad que nos permite verificar la identidad de un individuo que desee acceder a sus registros y que, ciertamente, sea el propietario de la cuenta o el asunto de los registros"; (Cole, págs. 4-5); lo anterior también permite confirmar si alguien comete una violación a la privacidad de la información de un individuo.

   Partiendo de la presunción de que toda información es verdadera, para identificar a la persona real no se necesitan grandes cantidades de datos agrupados; la proporción entre la identificación y la agrupación puede variar

[3] El pasado 28 de Julio de 2014 la Superfinanciera a través de la Carta Circular hizo un llamado de atención a las entidades bancarias recordándoles su obligación de "*Respetar el derecho fundamental de Habeas Data y la Regulación referida a la materia".* Fueron cuatro las fallas detectadas por la Superfinanciera: La no actualización de datos, los reportes sin autorización, la ausencia de notificaciones, y la falta de respuesta oportuna y diligente a las solicitudes y reclamos que hacen los clientes al detectar inconsistencias en su información. (Casa editorial El Tiempo, 2015)

debido a las actividades que un individuo realice en su día a día. Dentro de los beneficios que tiene la identificación está la reducción del fraude debido a la verificación de la identidad de las personas cuando éstas tienen varias cuentas. Lo anterior también representa un beneficio para la privacidad de la información de los individuos, ya que un vínculo efectivo entre la información y su propietario impediría la perdida fácil de datos sensibles y la suplantación de identidad.

3. *Inseguridad*, (*Insecurity).* La principal preocupación concerniente a la inseguridad es el robo de la identidad, la cual se ha hecho posible gracias a la gran cantidad de información personal almacenada en amplios depósitos, denominados *digital dossiers*[4] que a su vez son manipulados y sostenidos por varias instituciones y compañías. El robo de identidad está asociado a la agrupación de datos, ya que se pueden crear riesgos que pueden emerger de la protección inadecuada de los datos personales compilados, por lo tanto, la inseguridad es causada por la forma como nuestra información es manipulada y protegida. Dentro de las actividades relacionadas con la inseguridad se tienen: lapsus de seguridad, fallas técnicas, abusos y usos ilícitos de la información personal, convirtiéndose en una consecuencia posible de un error en la identificación del individuo. A pesar que el nombre de usuario y la contraseña con los identificadores biométricos han reducido dicha práctica delictiva, aún quedan espacios que se prestan para la identificación incorrecta de las personas, ya sea por divulgación de la información falsa o por exposición de datos sensibles. (pág. 517)[5]

[4] Expedientes Digitales

[5] Solove identifica las dificultades que tiene el sistema Americano al momento de prevenir cualquier robo de identidad o intromisión de la privacidad de un individuo. Para él, la ley Norte Americana reconoce que los resultados en la violación de la privacidad son altamente nocivos, sin embargo, las cortes son reacias a encontrar al almacenamiento de la información como la única causa de la inseguridad, resultando en la ignorancia de la inseguridad como un verdadero problema para los individuos y su privacidad.

4. *Uso secundario* (*Secondary use*). Las leyes y reglamentaciones sobre la privacidad, suelen advertir y sugerir a los usuarios tener presente preguntar cuál es la principal utilización que se le darán a los datos suministrados, sobre la información proporcionada. Cuando se habla del uso secundario es cuando los datos recogidos son utilizados para propósitos diferentes sin tener el consentimiento explícito del usuario; el uso secundario genera temor e incertidumbre en cómo la información de un individuo puede ser utilizada en el futuro, creando una sensación de impotencia y vulnerabilidad. El daño que se pueda sufrir surge de negar a las personas el control del uso futuro de sus datos, los cuales pueden ser utilizados de maneras que tengan efectos significativos en sus vidas.

5. *Exclusión* (*Exclusion*). La exclusión puede llevar a la divulgación de la información. Así como el uso secundario, la exclusión genera una sensación de vulnerabilidad en el usuario porque no tiene control total sobre sus datos, ya que no se le provee notificación sobre los usos que se le está dando a su información personal, así como los derechos para acceder a ésta y corregirla. Entre las normativas de privacidad se pueden relacionar los principios de:
   1. La información acumulada en bases de datos sobre las personas debe ser pública.
   2. Toda persona debe enterarse sobre su información almacenada en las bases de datos, qué información hay y para qué propósitos se está utilizando dicha información.
   3. Toda persona debe tener la propiedad de realizar modificaciones de su información cuando considera que hay datos erróneos en la base de datos.

   La exclusión se produce cuando los principios no se respetan.

*3.1.3.3 Divulgación de la información (Information Dissemination)*

La divulgación de los datos personales puede ocasionar daños en las personas y puede representar una amenaza que dicha información sea difundida. Solove identifica siete aspectos relacionados a la divulgación de la información: Violación de la confidencialidad, Divulgación, Exposición, Accesibilidad, Chantaje, Apropiación y Distorsión.

1. **Violación de la confidencialidad** *(Breach of Confidentiality*): Es la violación de la confianza en una relación específica sostenida entre el propietario del dato y quien lo administra. Esto no incluye que la información haya sido divulgada sino que el usuario haya sido traicionado.

2. **Divulgación** *(Disclosure):* La divulgación ocurre cuando cierta información verdadera acerca de una persona es revelada a otros. A diferencia de la violación de la confidencialidad, esta incluye el daño de la reputación de la persona. La protección de la información sobre la divulgación provee a las personas del poder para ocultar información acerca de ellas mismas que otro puede utilizar para perjudicarle.

   De acuerdo con Eugene Volokh, el derecho a la privacidad de la información es un derecho que controla la comunicación de información personal identificable. En otras palabras, es un derecho que impide que un tercero hable de un individuo sin su consentimiento. (1999, pág. 1049)

3. **Exposición** *(Exposure):* Es la exhibición de ciertos atributos emocionales y físicos de una persona. Dichos atributos son vistos como primordiales y la exhibición de los mismos puede traer vergüenza y humillación. Lo anterior hace daño a la integridad de la persona ya que hemos desarrollado prácticas sociales que ocultan ciertos aspectos de la vida como la desnudez, la sexualidad, las actividades fisiológicas, el dolor, el sufrimiento y el trauma. La dignidad es una característica de la civilización; la privacidad se considera

entonces como un referente de las relaciones sociales que sostenemos bajo las normas del decoro. La protección individual tiene serias repercusiones sobre el comportamiento colectivo, en palabras de (Miller), "un *espacio privado permite un espacio público civilizado".*

4. **Accesibilidad Incrementada** *(Increased Accessibility):* no implica una divulgación directa de la información, la información secreta no es revelada, la información ya disponible al público se hace mucho más fácil de acceder, esto conlleva a que una diferencia en la cantidad se convierte en una diferencia de la calidad y esto mejora el riesgo de los daños que tiene la divulgación. Es decir, la información abierta al público puede ser explotada para propósitos distintos a los cuales se hizo públicamente accesible, perdiéndose esa pequeña frontera entre la información completamente privada y la información completamente pública.

   El incremento de la accesibilidad a la información pública, las tecnologías de la información han permitido reforzar este problema apoyando que el usuario pueda consultar y acceder a su información a través de Internet, haciendo uso de las capacidades de los buscadores, derivándose problemas de explotación de la información para objetivos distintos de los previstos inicialmente.

5. **Chantaje** *(Blackmail):* El chantaje supone el control de una persona sobre otra y causa daño mediante la simple amenaza de divulgar su información, también involucra la información que es más propensa al ser exhibida y divulgada, sin embargo se caracteriza por ser una amenaza mas no la divulgación de la información.

6. **Apropiación** *(Appropriation):* Cuando alguien se apropia para su uso o beneficio particular del nombre o el parecido con otro, su reputación, su prestigio, su prestancia comercial o social, interés público y otros valores que

caractericen la identidad o personalidad de un individuo. Lo anterior está relacionado con los derechos de propiedad intelectual. Es necesario hacer una distinción entre los elementos tangibles e intangibles correspondientes a los agravios que pueda sufrir un individuo en su privacidad, ya que su identidad consiste en el dato primario, la información personal y las relaciones que sostenga dicho individuo con otras personas.

7. **Distorsion** *(Distortion):* Es la manipulación de la forma como una persona es percibida y juzgada por otros; la distorsión está relacionada con la difamación y a diferencia de la divulgación la información que se revela es falsa y engañosa. La distorsión tiene un impacto directo en la relación entre el individuo y la sociedad, ya que la reputación queda expuesta a cualquier tipo de manipulación que se quiera dar a la información.

#### *3.1.3.4* Invasión *(Invasion)*

Hay dos tipos de Invasión: Intrusión e Interferencia decisoria.

1. **Intrusión** *(Intrusión):* La Intrusión está relacionada con la divulgación. Esta se puede realizar por medio de la vigilancia, y el cuestionamiento, ya sea por incursión física o por proximidad. Lo anterior está relacionado con la posibilidad de ser objeto de control por periodos de tiempo prolongados a partir de prácticas invasivas en el comportamiento, la interacción y la información personal. La vulnerabilidad aumenta en entornos virtuales debido a los parámetros de exposición expuestos en párrafos anteriores. Ahora bien, el concepto de soledad aparece como un derecho que requiere protección y que la intrusión estaría violando en las esferas más privadas de un individuo; la visibilidad que un individuo quiera dar a su vida depende únicamente de él, pero las practicas intrusivas como la recepción de correos basura o ser objeto de publicidad no deseada afectan dicho concepto. De acuerdo con el filósofo Philip Koch, “La soledad permite que las personas descansen de la

presión de vivir en público o de desempeñar roles públicos". La protección de la privacidad de un individuo debe estar amparada en esta definición ofrecida por Koch.

2. **Interferencia decisoria** *(Decisional Interference):* Buena parte de la interferencia decisoria tiene relación con los problemas que trae la inseguridad, el uso secundario y la exclusión; estas prácticas afectan directamente el comportamiento y la percepción que tiene un individuo de sí mismo, debido al control, manipulación y posterior uso que tenga un ente superior sobre la información personal del sujeto en cuestión. Esta incursión no deseada en la información personal es ejecutada, principalmente, por el Gobierno, y tiene serias repercusiones sobre los intereses colectivos y las libertades individuales amparadas por la ley.

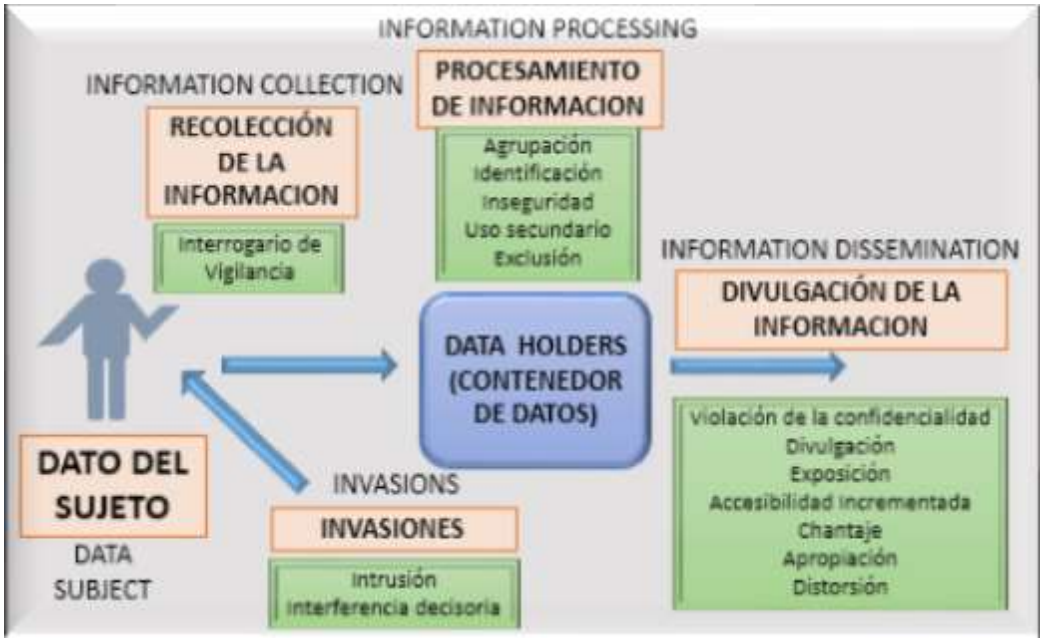
Aparece entonces una resignificación de la privacidad a partir de los usos que pueda dar el Gobierno a la información de los ciudadanos. Se refiere a la interferencia de los gobiernos en decisiones de los ciudadanos. En un sistema de gobierno democrático; si bien los gobernantes cumplen con periodos temporales por elección popular, la protección de la privacidad se convierte en una representación ilusoria, favoreciendo la noción de seguridad que debe tener un estado.

El sistema legal en una democracia debe considerar la privacidad como una forma de protección contra actividades problemáticas o actividades nocivas, esto no garantiza que las actividades que afectan la privacidad sean socialmente indeseables o que merezcan una sanción o prohibición, por ejemplo las prácticas comerciales de oferta y demanda.

La privacidad es lo que hace posible ejercer con confianza el derecho a intercambiar información y formas de pensar con otras personas, constituyendo

una de las bases de la democracia. El derecho a estar solos es lo que nos permite aprender cada día de nosotros mismos como personas, en Internet y la sociedad de la información podemos ver imposible la abstención a utilizar servicios debido a la evolución de la sociedad digital. En la siguiente imagen se puede observar de forma gráfica la taxonomía de la privacidad.

Imagen 1 : Taxonomía de la Privacidad




Fuente: (Solove, 2006)

### *3.1.4 Principios de la Privacidad*

Según Alan Westin, de la Universidad de Columbia, en Estados Unidos, son siete los principios de privacidad:

1. **Apertura y Transparencia**: No debe haber ninguna grabación secreta, esto incluye los datos recolectados como sus contenidos.

2. **Participación individual:** El sujeto de un registro debe ser capaz de ver y corregir el registro.

3. **Limitación en la recopilación:** La recopilación de los datos debería ser proporcional y no excesiva comparada con el propósito de la recopilación.

4. **Calidad del Dato:** El dato debe ser relevante a los propósitos por los cuales fue recopilado y debería mantenerse actualizado.

5. **Limitación de uso:** El dato debería ser utilizado únicamente para el propósito específico por el personal autorizado.

6. **Seguridad Razonable:** Adecuados guardas de seguridad debería ser puestos en lugar de acuerdo con la sensibilidad del dato recopilado.

7. **Responsabilidad:** Los guardianes de registros deben ser responsables del cumplimiento de los 6 principios anteriores.

La protección de la privacidad en la era del procesamiento del dato digital, ha llevado que exista una corriente Europea que está a favor de la liberación total de la información. Peter Cochrane de los laboratorios British Telecom, argumenta que: “La vida es mucho mejor sin privacidad”, afirma que desde el punto de vista tecnológico nunca hemos gozado de total anonimato en el pasado mundo de papel, entonces ¿por qué esperar que si sea posible en el mundo de los bits? Pensar en una legislación intencionada en la privacidad, sería más conveniente que el usuario sea quien decida qué compartir, con quién compartirlo y en qué entorno compartirlo (Langheinrich M. , 2001, pág. 277).

Quienes piensan que es mejor tener una libertad de la información sin privacidad presentan los siguientes principios para argumentar su propuesta en contra de la privacidad (Langheinrich M. , 2001, pág. 278):

1. **Viabilidad***:* Si no se es capaz de rastrear las violaciones de privacidad por medios legales o jurídicos entonces la responsabilidad dentro de las prácticas de la información justa se hace irrelevante.
2. **Conveniencia**: El libre flujo de la información pesa más que los riesgos personales en muchos casos. Al categorizar la información en pública, semi-pública y de alta sensibilidad (como es la de orientación sexual y religiosa, entre otras), solo esta última es la que merece verdadera protección.

3. **Comunitaria:** Las necesidades de la privacidad personal son inferiores al bienestar general de la sociedad; la sociedad podría supervisar los asuntos privados de la población, a través de instituciones de confianza, para mejorar la vida de la comunidad.

4. **Igualitaria:** Si todos tienen acceso a la misma información (deja de ser un arma para los pocos bien informados) nadie tiene control absoluto sobre la información de los demás. Cuando los que vigilan son vigilados, la información que ellos poseen de los otros es igual de valiosa a la información que los otros posean de ellos.

Los cambios que se hagan sobre la percepción de la privacidad estarán ligados a los cambios y avances tecnológicos; esto derivará en nuevas formas de interacción social y una ética que evolucione para hacer aceptables aquellas cosas que no lo eran en el pasado. Sin embargo, es importante tener en cuenta que las limitaciones sobre las prácticas de privacidad conciernen a los desarrolladores de aplicaciones, a los diseñadores de los dispositivos, a los usuarios, y a los procesadores o acumuladores de datos.

¿Cuántos de nuestros datos personales debe permitirse entregar por el bienestar de la conveniencia ante la sociedad y que nos prevenga del riesgo? ¿Cómo

podemos equilibrar el interés social contra nuestra protección personal? ¿A quién le estamos confiando nuestros datos de alta sensibilidad?

¿Cómo podemos influir en aquello que se constituya o no como el comportamiento social aceptable en el futuro, diseñando nuestros sistemas en una forma que apoye dicho comportamiento?

Ahora bien, lo que podemos hacer entonces es permitir que la gente que quiera respetar nuestra privacidad se comporte de dicha manera y, eventualmente, seremos capaces de construir una relación basada en la confianza y respeto mutuo, encontrando un buen balance de convivencia y control cuando interactuamos en infraestructuras ubicuas e invisibles.

### *3.1.5 Leyes de Privacidad*

La proteccion legal de la privacidad ha sido considerada por los sistemas juridicos occidentales como un elemento primordial del desarrollo del individuo, los primeros actos de proteccion de la informacion se remontan al siglo XIV, cuando el simple hecho de escuchar una conversacion privada era considerada un crimen en Inglaterra (Behrooz, 2010). Siglos después se reglamentó el uso de la informacion con propósitos legitimos, se prohibió la publicacion de hechos privados y asuntos domésticos, hasta que en la declaracion universal de los derechos humanos, la privacidad quedó consignada como un derecho que se establecía que nadie podía ser sometido a interferencia arbitraria con su privacidad, familia, hogar o su correspondencia, asi como nadie podía ser sometido a ataques en su honra y reputación. (ONU (United Nations Organization), 1948).

En la actualidad, la firma de abogados DLA Piper, con presencia en mas de 30 países, en los 5 continentes, publicó un compendio de leyes internacionales sobre la proteccion de datos en mas de 70 diferentes jurisdicciones (Halpert, et al, 2015). La Directiva de la Unión Europea de Octubre 24 de 1995, sentó el precedente mundial en la protección de los individuos en el procesamiento de sus datos

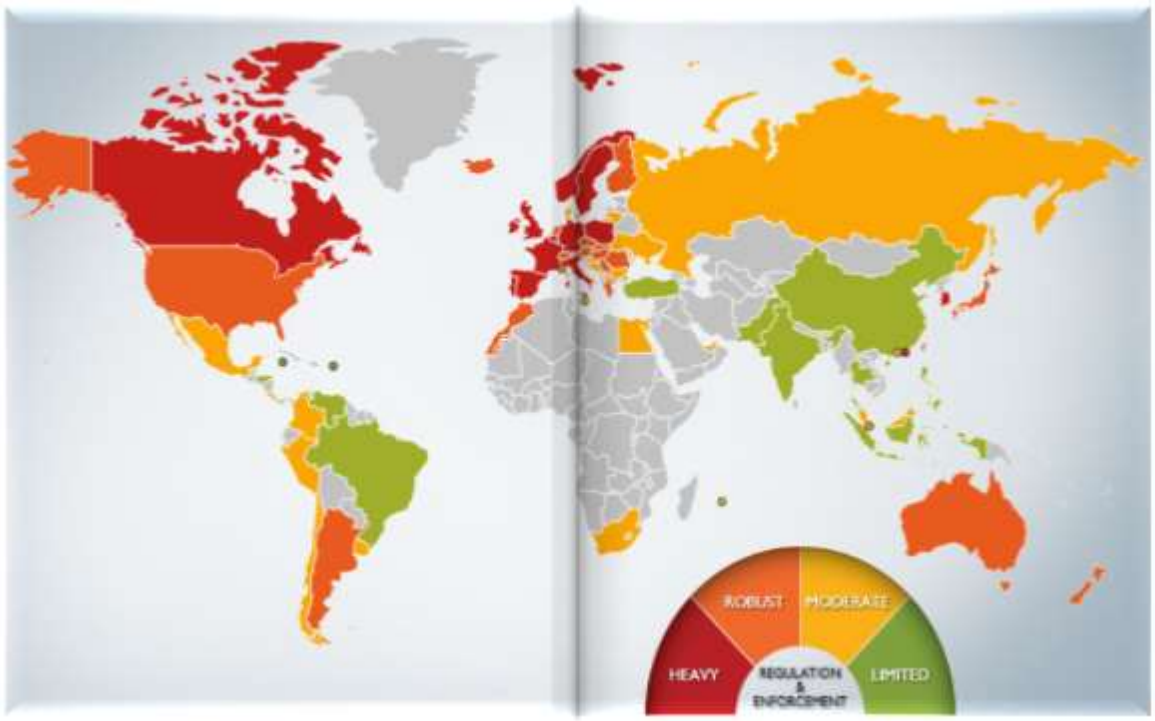
personales y el libre movimiento de los datos; a medida que las tecnologías progresan, así como la globalizacion, ha transformado la perspectiva que se tiene de los datos, los desarrollos técnicos están siendo correspondidos por leyes y marcos de trabajo más rigurosos, regulando la manipulación, almacenamiento y divulgacion de los datos personales, previendo las disposiciones futuras que los usuarios puedan hacer de los mismos. Los estados miembros de la Unión Europea han favorecido la política de responsabilidad que tienen aquellos que procesan los datos personales, sean compañías y organizaciones, así como la protección que deben recibir los datos bajo el consentimiento explícito de su propietario. La accesibilidad y la transferencia de los datos personales son servicios que deben ir acompañados de la notificación de violaciones en la seguridad de los datos. La búsqueda de una compatibilidad en las políticas de protección de datos empoderaría al usuario en la administración de sus datos personales ya que el almacenamiento de los mismos está sometido a la disponibilidad de espacio en la World Wide Web.

De acuerdo con el documento publicado por DLA Piper, se han identificado cuatro niveles de proteccion (Imagen 2) y Colombia se encuentra ubicada entre los países con un nivel de protección *moderado*.

DLA Piper clasifica la protección de la información en cuatro niveles, de forma descendente: Alto (Heavy), Robusto (Robust), Moderado (Moderate) y el Limitado (Limited). Se interpreta que dichos niveles de protección consisten en la convergencia de recursos técnicos y de infraestructura con políticas eficientes para garantizar al ciudadano que su información personal, incluyendo los datos sensible, es recolectada, administrada y manipulada cumpliendo con los principios mencionados en este documento, apartes arriba. Entre los de Nivel Alto (Heavy) se encuentran los paises de la Unión Europea, de Asia  están Corea del Sur y

Hong Cong, en America está Canadá. Entre Normativas más sobresalientes tenemos:

Imagen 2: Panorama mundial de los niveles de protección de datos




(Rojo = Alto Nivel de Protección(Heavy), Naranja = Robusto(Robust), Amarillo = Moderado(Moderate), Verde = Limitado (Limited); Fuente: (Halpert, Jim; et al, 2015)

### *3.1.5.1 La Unión Europea*

En 1995 el Parlamento Europeo publicó la Directiva 95/46/CE, relativa a la protección física y a la protección del tratamiento y libre circulación de los datos personales, (Access to European Union Law, 1995). El propósito de la directiva es velar por la protección de los derechos y las libertades individuales, en particular el Derecho a la Intimidad; la Directiva simboliza un nuevo giro en la historia de la legislación de la privacidad, así como en recalcar la relevancia de la protección de

la privacidad en la era del procesamiento del dato digital y la importancia de la cooperación internacional.

El objetivo es proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de los datos personales, estableciendo los principios referidos a la calidad de los datos, la legitimidad del tratamiento de los datos, las categorías especiales de tratamiento de los datos, el acceso a los datos, y la confidencialidad y la seguridad en el tratamiento de los mismos. El mayor impacto de la Directiva consiste en limitar la transferencia de datos que no son de la Unión Europea a aquellos países con un adecuado nivel de protección de privacidad; esto ha provocado que algunos países en el mundo revisen su legislación sobre la privacidad de los datos, como Estados Unidos. El resultado fue la creación de un Marco de Certificación, diseñado de manera conjunta entre los Estados Unidos y la Unión Europea, llamado Principios de Puerto Seguro (THE COMMISSION EUROPEAN, 2013), las políticas establecidas en que las empresas de Estados Unidos exportan y manejan los datos personales de los ciudadanos de la Unión Europea bajo los parámetros de la Directiva.

En segunda instancia, la Directiva depura e incluye prácticas de información justa, adicionando la noción de “Consentimiento Explícito” definido como: “El dato personal solo puede ser procesado si el usuario ha dado su consentimiento inequívocamente”, permitiendo excepciones para propósitos legales y contractuales.

La noción de Buen Gobierno de la información, introducida en la Directiva, genera nuevas perspectivas en el debate de la posesión real de la información; las relaciones que se establecen entre el usuario y el estado, el estado y el administrador de los datos, el usuario y el administrador de los datos, el usuario y el destinatario de los datos, conllevan diversos interrogantes sobre la relevancia de la privacidad original de la que se debe servir el usuario para tener pleno

control sobre la información que produzca o se produzca de él. Los principios sociales de la ética y la moral aparecen como los primeros portadores de la respuesta para solucionar cualquier dificultad que se presente en alguna de las relaciones mencionadas anteriormente, pero la ley tiende a ser una contramedida tardía para las dinámicas de interacción que sostienen los ciudadanos.

Una alternativa de gran aceptación para garantizar la calidad de los procesos en la recolección, almacenamiento, administración y liberación de la información, es la estandarización de los mismos en los lineamientos ofrecidos por la International Organization for Standardization, organización encargada de la publicación de las normas técnicas ISO, y que en nuestro país son implementadas por el ICONTEC. En las normas ISO[6] /IEC[7] 27018 – 2014 se establece criterios sobre controles y directrices a las medidas de Protección de Información Personal (P II8), de conformidad con los principios de privacidad en la norma ISO / IEC 29100 para entornos de trabajo con sistemas de almacenamiento público en la nube, se establece requisitos destinados a garantizar que los proveedores de servicios en la nube puedan ofrecer controles adecuados de seguridad de la información; el estándar ISO 27018 se apoya en la Directiva permitiendo la proyección en el mercado americano proporcionando confianza con respecto a servicios en entornos de almacenamiento en la nube (Normas-ISO.com, 2015).

Ahora bien, con lo expuesto arriba cabe destacar que la implementación de las políticas para la protección de la privacidad de la información de los usuarios tiene lugar de forma voluntaria. Si una organización adhiere a las políticas debe cumplir a cabalidad con las mismas, y si tiene sus protocolos propios y desea sincronizarlos con las medidas de orden internacional, estos deben estar sujeto a transformaciones que les permitan obtener los mismos beneficios. De alguna

[6] ISO: International Organization for Standardization (Organización Internacional de Normalización)
[7] IEC: International Electrotechnical Commission (Comisión Electrónica Internacional)
[8] Personally Identifiable Information

forma, esta adhesión se puede ver limitada, ya que las necesidades de cada estado corresponden a su desarrollo económico y nivel educativo, no obstante, la total transparencia de la implementación de los mismos debe favorecer el ejercicio ciudadano sobre la protección y la privacidad de los datos.

En lo concerniente a La Directiva de la Comisión del Parlamento y el Consejo de la Unión Europea, sus alcances y sus actualizaciones, profundizaremos en ella más adelante, en este documento.

*3.1.5.2 El caso Francia:*

En Enero 1978, con la ley 7817, Francia se convirtió en el primer país en Europa en proclamar una ley para la regulación y la protección de los datos en las tecnologías de información, denominada la ley como “Tecnología de la información, los Archivos de Datos y la Libertad Civil". Esta fue la base para la Directiva de la Protección de los Datos de la Unión Europea, 95/46/EC [9], implementada en Agosto de 2004.

Actualmente, cualquier regulación sobre el cumplimiento de la ley y la protección de los datos personales se encuentra bajo la supervisión de la Comisión Nacional de la Informática y de las Libertades, CNIL, por sus siglas en francés (Commission Nationale de l’Informatique et des Libertés), que ha definido dos categorías sobre el dato personal:

La primera categoría es la definición del dato personal que ofrece la ley 7817, del dato personal consiste en cualquier información relacionada a una persona natural que sea o pueda ser identificada, directa o indirectamente, por referencia de un número de identificación o uno o más factores específicos del individuo, como el nombre, número de registro civil, número de teléfono, entre otros.

[9] EC: European Commission

La segunda categoría que describe la ley determina el dato personal sensible; uno de sus mayores alcances es la consideración de cualquier dato que revele directa o indirectamente aspectos como la raza, orígenes étnicos, filosofías política o religiosa, afiliaciones a uniones de comercio o datos concernientes a su salud y su vida sexual, son datos que merecen un mayor nivel de protección y a los cuales se debe limitar el acceso, ya que corresponden a la caracterización de la identidad del usuario, y cualquier violación en la seguridad de los mismos dejan expuesta la vulnerabilidad del usuario.

La implementación de esta regulación, si bien es bastante posterior a las consideraciones iniciales de dicha ley, solo hasta la aparición de las Cookies, como programas de recolección automática de los datos, se hizo necesaria la adopción de la ley 7817 sobre los lineamientos sobre la Privacidad de los datos que establece que cualquier usuario de medios de comunicación electrónica debe estar al tanto de las disposiciones del controlador de los datos recolectados informando sobre el propósito de las cookies, ya sea para acceder a la información del usuario o almacenarla. De igual manera, el usuario debe tener la libertad de rechazar el servicio de las cookies y cualquier liberación o aplicación de las mismas sobre sus datos personales, debe estar bajo su consentimiento. Este consentimiento de usuario, descrito por la CNIL[10], debe ser libre, específico e informado; dicho consentimiento puede ser revocado en cualquier momento.

Además, esta ley fue la primera en especificar la regulación de los usos que pueda tener la información contenida en los datos personales, los cuales incluye el propósito de procesamiento de los datos, la identidad y la dirección del controlador de los datos, las interconexiones entre bases de datos, los tipos de datos personales procesados y las categorías de las personas encargadas del procesamiento, los destinatarios del dato procesado, el periodo de tiempo durante el cual el dato será almacenado, el departamento o las personas a cargo en

[10] CNIL: Comisión Nacional de la Informática y de las Libertades, sus siglas en francés (Commission Nationale de l'Informatique et des Libertés).

implementar el dato procesado, los destinatarios o categorías de destinatarios del dato personal, las medidas tomadas para garantizar la seguridad del procesamiento de los datos y la existencia de la transferencia de datos de un país externo a la unión europea. (Halpert, Jim; et al, pág. 115).

#### *3.1.5.3 Caso España*

Si bien España, como miembro de la Unión Europea, ha implementado la Directiva de Protección de Datos de la UE 95/46 / CE, la nación ibérica ya contaba con una Ley de Protección de Datos ("LORTAD"[11]), anterior a la adoptada por los países de la Eurozona. La posible incompatibilidad entre las dos leyes y la baja aceptación que tuvo la implementación de la Directiva llevó a las autoridades peninsulares a implementar la reciente LOPD[12], adaptándose al actual panorama de los avances tecnológicos y la gestión. En la actual ley, se define el derecho a la intimidad y a la privacidad de la información de todos los ciudadanos en todos sus trámites. Es decir, que todas las empresas que trabajen con bases de datos que contengan datos privados deben ajustarse a la ley LOPD y con esto preservar la privacidad del usuario. La compatibilidad con la Directiva de protección de datos de la UE 95/46 / CE y la efectividad de su ejecución ha hecho posible que el modelo español de protección a los datos sea un modelo ejemplar para las naciones en transición para adoptar medidas precisas para proteger la libertad de sus ciudadanos. Su última modificación se dio lugar en marzo de 2011, en una de las épocas más convulsas de esta nación, cuando la banca debió entrar en reestructuración para reforzar su capital, un año en el que el desempleo llegaba al 22%, un año de elecciones generales, dando por vencedor a Mariano Rajoy, quien recibía un país en una profunda necesidad de cambio y de adopción de medidas para el progreso.

[11] Ley orgánica de regulación del tratamiento automatizado de los datos de carácter personal
[12] Protección de Datos de Carácter Personal

### *3.1.5.4 Caso Canadá*

En su Monarquía Parlamentaria Federal, se reconocen veintiocho estatutos sobre la privacidad provincial y territorial, identificando tres áreas de control sobre la privacidad de los datos: el sector público, el sector privado y el sector salud. A pesar de las diferencias que se puedan presentar entre las jurisdicciones de sus diez provincias y sus tres territorios, todas disponen de un régimen que comprende la colección de los datos, el uso y la divulgación de la información personal. En cuanto a la propiedad del dato privado, son cinco los estatutos que mayor relevancia han tenido para la nación de la hoja de arce:

- Acto para la Protección de la Información Personal y Documentos Electrónicos (PIPEDA)
- Acto para la Protección de la Información Personal (PIPA Alberta)
- Acto para la Protección de la Información Personal (PIPA BC)
- Acto Respecto a la Protección de la Información Personal en el Sector Privado.

Este último, conocido como el Acto de la Privacidad de Quebéc, es reconocido colectivamente como Los Estatutos de la Privacidad Canadiense. La aplicación de los actos ya mencionados incluyen a las organizaciones que recolectan y revelan la información personal en el curso de una actividad comercial; las prácticas de información personal de la relación sostenida entre el Empleador y el Empleado, en organizaciones como bancos, compañías de telecomunicaciones, entre otras. Cabe destacar que debido a la organización política del territorio, cuando un ciudadano incurre en un delito informático, el proceso toma curso con los estatutos de la provincia lugar de su nacimiento a menos que los estatutos sean sustancialmente compatibles, de esta manera será procedente en la provincia donde se cometió el delito.

La diferenciación del sector salud respecto del sector público y el sector privado, en lo referente a la protección de la privacidad de la información, es debido a que

el sistema de salud es un sistema mixto entre ambos sectores, el público y el privado. Si bien el gobierno se encarga de financiar los servicios, es el sector privado el encargado de asistir a los pacientes con dichos servicios, por tal motivo, el dato personal y la información de los usuarios es más vulnerable ya que es manipulada desde los dos frentes. Gracias a la rigurosidad del sistema de protección a la privacidad y la separación, y posterior compatibilidad, entre los estatutos provinciales, el dato sensible cuenta con mayor vigilancia.

A modo de nota, cada uno de los Estatutos de la Privacidad Canadiense contiene estipulaciones diseñadas para exigir a las organizaciones, privadas y públicas, a tomar medidas técnicas, físicas y administrativas razonables para proteger la información personal contra la pérdida o el robo, acceso no autorizado, divulgación, copia, modificación y destrucción. El dato personal en Canadá es definido como toda información personal acerca de un individuo identificable, sin embargo, no hay una definición explícita para el Dato Sensible. De acuerdo con lo anterior, la no existencia de una distinción del dato sensible, Raw Data, impide que haya una polarización entre los estatutos provinciales sobre cuán íntimo o cuán público puede llegar a ser un dato, influyendo directamente sobre la manipulación y la seguridad que deban tener; que todo dato tenga un referente identificable caracteriza la legislación canadiense con el rasgo de la rigurosidad en la protección de las libertades individuales, desembocando en la posesión de un sistema robusto, modelo mundial, que va a la par de las necesidades y desarrollos de su sociedad.

Según DLA Piper, los países con el nivel Robusto (Robust) se encuentran Estados Unidos, Argentina, en Europa países como Suiza, Finlandia, Iceland, República Checa, Austria, Hungría, Rumania, Grécia, Servia, Mónaco, en Africa esá Marruecos, en Asia Japón, Taiwan y Singapure, además se encuentra Australia. Entre los casos más sobresalientes tenemos:

### *3.1.5.5 Caso Estados Unidos*

En el año 2000, la Comisión Federal de Comercio entregó al gobierno americano un reporte titulado “Privacy Online: Fair Information Practices in the Electronic Marketplace”[13], donde exponía la necesidad de asegurar el futuro del intercambio electrónico de la información personal. A pesar de la atención mediática que recibió, la administración Clinton se mostró poco complaciente con las sugerencias de la Comisión. En ese entonces, La Directiva para la Protección de los Datos, de la Unión Europea, ya había entrado en vigencia y había logrado permear parte del sistema jurídico norteamericano en las políticas de protección a la información, sin embargo, no era del todo efectiva y ejecutable (Halpert, Jim; et al, 2015).

En la actualidad, Estados Unidos tiene leyes sobre 20 sectores específicos medidas nacionales sobre la privacidad o de datos de seguridad, y cientos de dichas leyes entre sus 50 estados y sus territorios. Lo anterior puede entenderse como un gran avance en las políticas de protección a la privacidad de los datos, si comparamos con la ventaja que las naciones europeas le habían tomado desde la década de los ochenta. La definición del Dato Personal tiene dos connotaciones: la primera corresponde al contenido y la segunda, al uso que recibe el dato. Por tal motivo, el Dato Personal es entonces todo aquello que permita identificar, contactar o distinguir a un individuo, con excepciones en algunos estados que consideran que el Dato no es todo aquello que esté relacionado directamente con un individuo plenamente identificable. Ahora bien, en cuanto al uso que recibe el dato recolectado, diferenciando la relación del Individuo con el Sector Público y la relación del Individuo con el Sector Privado (Strauss & Rogerson, 2002).

El documento que valida las decisiones tomadas sobre la Privacidad de los Datos es la Política para la Privacidad de los Datos Safe Harbour[14], con el auspicio del

[13] La Privacidad en Línea: Prácticas de Información Justa en el Mercado Electrónico
[14] Safe Harbour (SH): Puerto seguro

Departamento de Comercio de Estados Unidos, DOC[15], y reconocida por la Comisión de la Unión Europea en un nivel de protección "adecuado", de acuerdo con los principios de La Directiva 95/46/EC, mencionada en el ítem 3.1.5.1 del presente documento (Dhont, Pérez Asinari, & Poullet, 2004).

#### *3.1.5.6 Caso Suiza*

La confederación Helvética es uno de los países que ha desarrollado una política de protección a la privacidad de los datos bastante robusta. Sus primeros acercamientos a este objetivo se dieron a mediados de la década de los setenta, paralelos a las actividades legislativas de la Comunidad Europea que en aquel momento buscaba implementar en los países miembros las políticas de transparencia y protección de la información de los ciudadanos. El trabajo de las comisiones expertas del Parlamento y el Consejo de la Unión Europea llevaron al Consejo Federal del Gobierno Suizo a producir en 1984 el primer borrador de lo que se convertiría en el Acto Federal de la Protección de Datos (DPA), con sus respectivas ordenanzas: Ordenanza para el Acto Federal de la Protección de Datos (DPO), y la Ordenanza sobre la Certificación de la Protección de Datos (ODPC) (Halpert, Jim; et al, 2015).

Al igual que Francia, se establecen dos categorías de dato personal: el Dato Personal y el Dato Personal Sensible. El primero corresponde a toda aquella información relacionada a una persona natural o jurídica que pueda ser o haya sido identificada. El segundo se encuentra dividido en cuatro subtipos: el de la dimensión ideológica, como la religión, filiación política y/o económica; el de la intimidad, como la salud, el origen racial y sus relaciones interpersonales; el de la dimensión de la seguridad personal y social; y el de la dimensión jurídica, donde se incluyen las procedimientos y las sanciones de orden administrativo o criminal.

[15] DOC: Department of Commerce US

Los Perfiles Personales también se encuentran protegidos por el DPA[16], y son definidos como la colección de los datos que permiten la identificación de las características esenciales de la personalidad del individuo.

La autoridad nacional para la protección de los datos es el Comisionado Federal para la Protección de los Datos y de la Información (FDPIC); las responsabilidades de los Oficiales de la Protección de los Datos están divididas en el Registro, la Recolección, el Procesamiento, la Transferencia, la Seguridad, la Notificación de Infracciones, el Mercadeo Digital, y la Privacidad en Línea. El DPA es ejecutado por la FDPIC[17] y está encargado de realizar las actualizaciones pertinentes, para garantizar la idoneidad del mismo, manteniéndose vigente en la regulación de la protección y transferencia de los datos (Halpert, Jim; et al, 2015).

Si bien el DPA representa un gran logro para la nación Helvética, las falencias que puedan presentarse en el documento no implican una omisión general de la ley de dicho país. Un ejemplo sencillo es el de la notificación en caso de violación de la seguridad y la privacidad; que esto suceda no implica una obligación explícita del DPA de notificar a los individuos afectados o a la autoridad de la FDPIC, pero el sistema jurídico determina que debe haber una evaluación individual de cada uno de los casos que se presenten y que las medidas que se deban tomar para garantizar la protección del ciudadano sean idóneas, como la obligación general para mitigar los daños y perjuicios sufridos, la observación de la buena fe en el procesamiento de la información personal y la instrucción de los individuos, si llegasen a ser víctimas, así como futuras medidas para prevenir y evitar ser sujeto de alguna violación a la seguridad y la privacidad de sus datos. La atención de los casos de forma individual favorece la evaluación acertada de las circunstancias, impidiendo que las formalidades generales no logren dar la solución requerida. Sin embargo, la no notificación de la violación a la seguridad y a la privacidad de los

[16] DPA: Acto Federal de la Protección de Datos
[17] FDPIC: Comisionado Federal para la Protección de los Datos y de la Información

datos es sancionada severamente, y cualquier evasión por parte de los Oficiales de la Protección de los Datos en notificar a los usuarios, es entendida como negligencia, y al ser un funcionario del estado, es vigilado por el código disciplinario establecido en el país (World Law Group, 2013).

#### *3.1.5.7 América Latina – Caso Argentina*

En el año 2003, después de trabajar comprometidamente en la protección de la información personal desde comienzo de siglo, Argentina recibió el aval de la Comisión Europea reconociendo que ofrecía un nivel adecuado de la protección de los datos personales, y que las disposiciones legales y jurídicas adoptadas por el país en la ley 25/326, Argentina se encontraba operando bajo los lineamientos de la Directiva de Protección de Datos (95/46/EC) de la Unión Europea.

La definición adoptada para el Dato Personal establece que “es cualquier tipo de información relacionada a individuos identificados o identificables o entidades legales”. La definición de Dato Personal Sensible se refiere a “toda información personal que revele el origen étnico o racial, postura política, creencias religiosas, postura filosófica y moral, afiliaciones o información relacionada con la salud y la vida sexual”. Uno de los grandes avances de la política Argentina es la creación de la Dirección Nacional de Protección de Datos Personales (DNPDP), donde yace el registro de cualquier base de datos pública o privada. Sin importar si el propósito de las bases de datos sea proveer reportes o transferencia de datos, siempre y cuando la base de datos no sea exclusiva de uso personal.

Dentro de los parámetros de regulación en el registro se encuentra: el nombre y la dirección del recolector de datos, caracterísiticas y propósitos de la base de datos, la naturaleza de los datos incluidos en la base de datos, métodos de recolección y actualización de los datos, individuos o entidades a quienes puedan ser transferidos los datos, los métodos de enlace para la información registrada, los

métodos utilizados para garantizar la seguridad de los datos detallando las personas que tengan acceso al procesamiento de la información, el tiempo de almacenamiento de los datos, y las condiciones bajo las que terceras partes puedan tener acceso a los datos relacionados a ellos y los procedimientos ejecutados para corregir o actualizar los datos. El consentimiento del usuario es uno de los factores más relevantes al momento de recolectar, procesar y disponer de los datos personales.

La DNPDP [18] establece que solo en cuatro casos no es necesario el consentimiento del usuario:

- Cuando la información es tomada de una base de datos públicamente accesible, estando el gobierno en ejercicio de sus deberes, o como resultado de una obligación legal.
- Cuando la base de datos está limitada a cierta información básica como el nombre, el número de identificación, número de recaudo tributario, fecha de nacimiento y domicilio.
- Cuando los datos personales derivan de una relación contractual, científica o profesional, y es utilizada únicamente en dicho contexto.
- Cuando la información es provista por instituciones financieras y que fuese requerida por los estrados, el Banco Central de Argentina, o la autoridad de recaudo tributario.

Sin embargo, en cualquier situación donde se exprese o no el consentimiento para entregar los datos personales, el usuario debe ser informado del propósito por el cual los datos son recolectados, quién puede llegar a disponer de dichos datos, la existencia de la base de datos, la identidad del recolector de los datos y su dirección de correo electrónico; de igual manera, debe conocer las consecuencias de proveer los datos, el rehusarse a entregarlos o el proveer información falsa e

[18] DNPDP: Direccion Nacional de Datos Personales

imprecisa, el motivo de acceso a los datos, y los derechos de rectificación y supresión de los datos. Es por eso, que los paises apuntan a sanciones mas severas sobre aquellos que violen la privacidad de los datos.

Argentina, es el único país de Suramérica que cuenta con el aval de la Comisión Europea en el alto nivel de protección de los datos. Uno de los principales factores de compatibilidad entre ambas agencias yace en la transferencia de datos fuera de su territorio. Las disposiciones de la DNPDP determina que “todo dato que sea transferido fuera de la nación debe hacerse en cumplimiento de los intereses legítimos de la transferencia de los datos y los destinatarios de los datos, y generalmente bajo el consentimiento previo del propietario del dato y que pueda ser revocado posteriormente”.

Según las disposiciones de la DNPDP, la transferencia internacional de los datos no requiere consentimiento cuando la recolección de los datos no lo requirió, cuando la transferencia de los datos es hecha entre agencias gubernamentales en el ejercicio de sus deberes respectivos; cuando los datos se encuentran relacionados a asuntos de salud y son utilizados para solucionar emergencias, ejecutar estudios epidemiológicos u otros propósitos de salud pública donde la identidad del usuario sea protegida, y cuando los datos han sido desidentificados y ya no corresponden a los sujetos correspondientes.

A pesar de los grandes avances que ha tenido la ley Argentina en cuanto a la protección de los datos, la nación aún no ha promulgado una regulación para la privacidad en línea. Este podría ser uno de los puntos débiles ya que una de las defincione dadas por la Ley de Protección de Datos Personales (PDPL) en la interpretación de la privacidad de los datos, está en el uso de las cookies y otros programas de recolección automática de datos. En la PDPL, dichos programas se consideran ajenos a la clasificación de dato personal ya que la información a la que tienen acceso corresponde a un dispositivo y no a un usuario específico.

El siguiente nivel de clasificación según DLA Piper, los países en el nivel Moderado (Moderate), se encuentran Rusia, Ucrania, Egipto, Malasia, Sudáfrica, y en América Latina se encuentran Perú, Chile, Uruguay, México, Costa Rica y Colombia; encontrandose por encima de potencias económicas como Brasil y Venezuela, pero muy por debajo de Argentina, país con un sistema jurídico de nivel alto en la protección de los datos.

### *3.1.5.8 Caso Colombia*

Nuestro país, a pesar de la aparición de la directiva a comienzos de siglo, la protección de la información solo ha tenido relevancia durante el más reciente gobierno. Si bien la privacidad y la intimidad personal se encuentran contempladas en el artículo 15[19] de la carta magna de nuestra nación, solo hasta el año 2009, con la sanción de la Ley 1341, que implicó la transformación del Ministerio de Comunicaciones en el Ministerio de las Tecnologías de la Información y las Comunicaciones, se desarrolló un nuevo marco normativo que promoviera el acceso y el uso de las TIC a través de la masificación, la posibilidad de la libre competencia entre los proveedores de servicio, la renovación de la infraestructura disponible y el uso eficiente de la misma, y el fortalecimiento a la protección de los derechos de los usuarios. Esta última disposición se reglamentó cuatro años después con el Decreto 1377, en el cual se normalizó, parcialmente, la Ley 1581 de 2012, conocida como la Ley Hábeas Data.

Los alcances de dicha Ley representan un gran avance para la percepción que tenían los ciudadanos respecto de su información personal. De acuerdo con el articulado de la misma, toda persona tiene derecho a conocer, actualizar y rectificar cualquier tipo de información que se haya recogido sobre ella en archivos

[19] "*Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas*" (Asamblea Nacional Constituyente (1991), pág. 15)

o cualquier base de datos de naturaleza pública o privada, exceptuando aquellas mantenidas bajo el uso personal o doméstico. De igual manera, aparece una nueva caracterización del ciudadano como Titular, definido como toda persona natural cuyos datos personales sean objeto de cualquier operación, ya sea de recolección, almacenamiento, uso, circulación o supresión. Esto último es definido como Tratamiento y opera bajo nueve principios aplicables de forma armónica, interpretado, en términos jurídicos, como la interrelación y la no contradicción entre dichos principios. Los principios contenidos en la Ley Hábeas Data son compatibles con las definiciones ofrecidas por Alan Westin, utilizando una terminología similar en algunos de ellos:

a. *Principio de Legalidad en Materia de Tratamiento de Datos:* cualquier tratamiento de información debe estar sometido a la ley y las disposiciones que en esta se desarrollen.

*b. Principio de Finalidad*: la finalidad del tratamiento de los datos debe ser legítima, de acuerdo con la constitución; el Titular debe estar informado.

c. *Principio de Libertad:* una vez el Titular haya sido informado y este haya dado su consentimiento previo, expreso e informado, puede ejercerse el Tratamiento de los datos; la obtención o divulgación de los datos no pueden ocurrir sin autorización del Titular o mandato legal que releve el consentimiento.

*d. Principio de Veracidad o Calidad:* el Tratamiento de datos parciales, incompletos o fraccionados, que induzcan al error, está prohibido. Toda información sometida a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.

e. *Principio de Transparencia:* a diferencia de la definición dada por Westin, el Titular tiene derecho a obtener del Encargado del Tratamiento de los datos, información acerca de la existencia de datos que le conciernan. Esto puede interpretarse como total apertura para con el Titular, sin embargo, el tipo de información que se recolecte de él puede recibir distintas tipificaciones, y se da por entendido que al regular las bases de datos se regula la información que estas contengan.

f. *Principio de Acceso y Circulación Restringida:* el Tratamiento de los datos sólo puede hacerse por personas autorizadas por el Titular o por las personas previstas en la Ley 1581 de 2012. Toda información que no sea de carácter público no puede estar disponible en Internet o cualquier otro medio de divulgación. El acceso debe ser controlable e incluso con conocimiento restringido para los titulares o terceros autorizados por la Ley mencionada.

g. *Principio de Seguridad*: toda información debe ser manipulada con las medidas técnicas, ya sean humanas o administrativas, que sean necesarias para otorgar seguridad a los registros. El propósito de este principio es evitar cualquier adulteración, fraude, pérdida, consulta, uso o acceso no autorizado. Esta medida es compatible con la propuesta por Westin, Seguridad Razonable; Westin propone que la seguridad de la que se debe disponer para proteger la información depende de cuán sensible sea. A partir de lo anterior, se habla entonces de los Niveles de Seguridad.

h. *Principio de Confidencialidad:* toda persona que intervenga en el Tratamiento de la Información está obligada a garantizar la reserva de la misma, aun cuando su labor esté terminada.

El séptimo principio propuesto por Westin, Responsabilidad, enmarca la ética profesional como la base fundamental para que estos principios de la privacidad

de la información puedan cumplirse. Cualquier vacío jurídico en la Ley es solucionado con la presunción de idoneidad en las personas a cargo del Tratamiento de la Información.

La presente Ley establece los Datos Sensibles como una categoría especial y los define como todo dato que afecta la intimidad del Titular, sean relativos a su ideología política, su salud, su vida sexual, y sus datos biométricos. Cualquier Tratamiento sobre los datos sensibles está prohibido con las siguientes excepciones: salvaguardar el interés vital del titular; si son necesarios para el reconocimiento, el ejercicio o la defensa de un derecho en un proceso judicial; si tiene una finalidad histórica, estadística o científica, para este caso, se debe suprimir la identidad de los titulares[20].

Desde su formulación, presentación y sanción, la Ley de Hábeas Data ha tenido que sortear difíciles escenarios. El primero de ellos fue en el año 2011 cuando la Corte Constitucional derogó tres de los treinta y cuatro artículos aduciendo vicios de forma; dichos artículos hacían referencia a la regulación en la certificación de antecedentes judiciales del desaparecido Departamento Administrativo de Seguridad, y el manejo de bases de datos de inteligencia y contrainteligencia, ya que la Corte consideró que debían ser objeto de otra ley. Acto seguido, los medios de comunicación no dudaron en hacer diversas comparaciones con las leyes de protección de la información en otros países enfocándose en situaciones cotidianas, como el ingreso a un conjunto residencial; comparaciones de este tipo solo ayudaron a generar mayor incertidumbre sobre la efectividad que tendría la Ley, si la sociedad colombiana estaba preparada para su entrada en vigencia y si había suficiente información sobre los derechos que esta Ley garantiza a los ciudadanos.

[20] Congreso de la República de Colombia, Ley estatutaria No. 1581, artículo 5

Sin embargo, una de las disposiciones más importantes de esta Ley es la creación del Registro Nacional Único de Bases de Datos, donde los Titulares tienen acceso a la cantidad de información que de ellos se posea, quiénes se encuentran encargados de su tratamiento, así como la notificación sobre el objeto de su uso. Para garantizar el control al manejo eficiente de los datos, la Superintendencia de Industria y Comercio quedó facultada con esta nueva ley para ordenar, investigar y sancionar, si es el caso, a quienes incurran en alguna falta o abuso de los datos de los Titulares. Una de las prácticas de mayor vigencia en la sociedad colombiana era el envío de mensajes al celular o al correo electrónico, con promociones u ofertas sobre servicios y productos no requeridos por los Titulares; con la entrada en vigencia de esta Ley, quedó reglamentado que si un Titular desea ser eliminado de alguna base de datos comercial, puede solicitarlo por medio de un derecho de petición. Este recurso facultó a cientos de usuarios para exigir su derecho a la privacidad. Las respuestas no se hicieron esperar. Antes que la Ley entrara en vigencia, las empresas recibieron un plazo de treinta días para notificar a sus usuarios sobre su permanencia en sus bases de datos, una vez terminado el plazo, si el usuario no respondía a la solicitud, este Silencio Positivo, autorizaba a las empresas a que los conservaran en su base de datos. Aunque la vía lógica del derecho permite pensar que esta medida era conveniente, algunos sectores mostraron su desacuerdo ante la misma ya que dicha figura sólo tiene validez para funcionarios públicos. El consentimiento debe ser previo, expreso e informado; así lo afirma la Ley de Hábeas Data. Si bien hubo descontento por esta primera etapa de transición a la entrada en vigencia de la Ley, la Superintendencia de Industria y Comercio ha logrado obtener buenos resultados en cuanto a la vigilancia y operación de las empresas con actividad en nuestro territorio. Dentro de las sanciones más sonadas están las que recibieron Movistar y Claro, dos de las empresas de telecomunicaciones que ofrecen servicios de telefonía, televisión e internet, con multas superiores a los ciento diecisiete millones de pesos, por la no notificación a los Titulares de la información sobre cómo sería manipulada y por robo de identidad, respectivamente.

Dentro de las últimas medidas que se pretenden implementar para fortalecer la Ley 1581, está el Proyecto de ley presentado en Octubre del presente año que pretende ampliar los procedimientos y sanciones para empresas que operan en el país, pero que no son domiciliarias locales y que, por tanto, no están cobijadas por la actual ley de protección de datos. (Periódico El Tiempo, 2015).

Tal es el caso de las empresas que prestan el servicio de redes sociales, como Facebook, Twitter, Amazon, entre otros, quienes también deben velar por la protección a la información personal y el derecho al buen nombre de sus usuarios, en las bases de datos físicas o digitales que posean, ya sea con información sensible o información de actividad comercial. Esta iniciativa puede generar una polarización en la percepción del verdadero alcance que puede tener una Ley más allá de sus fronteras territoriales, sin embargo, la Constitución Política de nuestro país establece que toda actividad comercial en el territorio colombiano está sujeto a las leyes que en él se sancionen.

### *3.1.6 Mecanismos de Privacidad y Organizaciones Internacionales*

Dentro de la literatura revisada, se identificaron los siguientes conceptos:

- Mecanismo de privacidad: es la herramienta empleada para garantizar la privacidad de la PII[21] en un ISMS[22]
- Técnica de privacidad: es el protocolo que se sigue para garantizar la privacidad de la PII en un ISMS
- Práctica de Privacidad: es toda medida de ajuste y configuración, anterior a cualquier mecanismo o a cualquier técnica de privacidad empleada para proteger la PII en un ISMS.

[21] PII : Personally Identifiable Information
[22] ISMS : Information Security Management System

### *3.1.6.1 International Organization for Standardization - ISO*

Desde el año 1947, la Organización Internacional de Estandarización, ISO, por sus siglas en inglés, se ha encargado de normativizar y dar las especificaciones mundiales para los productos, los servicios y los sistemas de los que se hacen uso, buscando garantizar su calidad, seguridad y eficiencia. En el área de informática y telecomunicaciones, la participación de la ISO ha sido determinante; debido a la revolución tecnológica, las compañías productoras de hardware y de software han tenido que atravesar duras pruebas para estar al nivel que demanda dicha institución. Sin embargo, existe un elemento que está más allá de los monopolios industriales en el emporio digital y está en esa delgada línea que separa lo público de lo privado; si bien Internet se encuentra bajo constantes controles de seguridad, desde los proveedores de servicio hasta los usuarios generadores de contenido han tenido que ver la dinamización del concepto de la Propiedad para favorecer la masificación del servicio. Es entonces cuando el ejercicio del modelo económico neoliberal encuentra en la red una de sus mejores facetas, no por la ejecución del libre mercado que oculta fácilmente los monopolios, sino por la despersonalización y la desaparición de una verdadera autoridad regulatoria y sancionatoria que pueda velar por la protección de los derechos de los usuarios y la seguridad y la privacidad de su información personal, en especial en la última década, donde la red se ha convertido en el escenario de distintas manifestaciones activistas, retratados en los medios como infractores de la ley, mientras las prácticas invasivas de un gran número de compañías son justificadas para lograr que sus clientes se hagan a sus productos y servicios, sean de su interés o no.

Dentro de las medidas de participación por la que ha optado la ISO ha sido la publicación de la serie de estándares ISO/IEC 27000, orientada a lo concerniente a la seguridad de la información. El primero de ellos, el estándar ISO 27001, apareció en el año 2005, consiste en la especificación de las operaciones de un

Sistema de Gestión de Seguridad de la Información, SGSI (en inglés: Information Security Management System, ISMS), encaminado a proveer los requerimientos para establecer, implementar y mantener un sistema de gestión eficiente en constante mejora, con un diseño atendiendo las necesidades, los objetivos, la estructura, el tamaño y los requerimientos de seguridad que tenga una organización en particular.

El siguiente en ser publicado fue el estándar ISO 27002, en el mismo año de publicación del anterior (actualizado en 2013), proveyendo los lineamientos para poner en marcha un ISMS. La versión más reciente contiene diecinueve controles menos que los propuestos en la publicada una década atrás; ha sido implementado en varios sectores de productividad, como el Sector Salud o el Sector Manufactura, por citar dos ejemplos, y su contenido describe las características de la estructura del Sistema, su política de Seguridad, la organización de la seguridad de la información, su control de acceso, su criptografía, las operaciones de seguridad, los activos de gestión, y los sistemas de adquisición, desarrollo y mantenimiento de la información, entre otros (International Organization for Standardization ISO, 2005-2013).

Tres años más tarde, en el 2008, con la publicación del estándar ISO 27003, por primera vez se presentaron las guías para la implementación de un ISMS destacando la pertinencia del método Plan-Do-Check-Act, PDCA (planificar-hacer-verificar-actuar o planificar-hacer-verificar-ajuste) (Gorenflo & Moran, 2010), para la eficiencia del sistema, un método iterativo utilizado en los negocios para el control y el mejoramiento continuo de los procesos y los productos. Algunas variantes del método incluyen la Observación convirtiéndolo en OPDCA. Las etapas consisten en establecer los objetivos y los procesos necesarios en concordancia con las expectativas de los resultados; implementar el plan y

ejecutar los procesos; estudiar los resultados obtenidos y compararlos con las expectativas planteadas; finalmente, si los resultados demuestran que el plan fue efectivo y preciso, se adopta como la nueva base de acción de la organización. La introducción de este método en los ISMS significó un nuevo punto de partida para las compañías que habían comenzado su proceso de gestión de seguridad; aunque se puede tomar como una herramienta para beneficiar dicho proceso también se incluyó el concepto de Factor de Éxito Crítico[23] relacionado con el Indicador Clave de Desempeño, llevando a que la orientación de los ISMS tuviera una notable marca del mundo empresarial, dando prioridad a las necesidades de los proveedores de servicios sobre los usuarios. Estas primeras medidas de la ISO son tardías comparadas con los avances que los sistemas jurídicos en Europa en cuanto a la protección de la PII y el dato sensible. Muestra de lo anterior es que un año después se publicó el estándar ISO 27004, que provee la guía para el desarrollo y uso de medidas para la evaluación de la efectividad de un ISMS.

En 2011 se publica el estándar ISO 29100, el cual provee un marco para la privacidad donde se especifica la terminología común para la privacidad, se definen los actores y sus roles en el procesamiento de la Información Personal Identificable, PII, por sus siglas en Inglés; se describen las consideraciones para salvaguardar la privacidad, y se ofrecen las referencias para conocer los principios de privacidad en las Tecnologías de la Información. Dicho estándar es aplicable a toda persona natural u organización que tenga su campo de desempeño en sistemas y servicios de las TIC. Tres años más tarde, en 2014, después de los escándalos de Wikileaks y las revelaciones de Edward Snowden, se publica el estándar ISO 27018 en el que se establecen los objetivos, controles y lineamientos comúnmente aceptados para implementar medidas de protección de la PII, de acuerdo con los principios de privacidad publicados en el estándar ISO 29100, en el entorno público de computación en la nube. Según Radic, la

[23] En Inglés es CSF: Critical Success Factors

adopción voluntaria del estándar implicaría la adopción de nuevos controles de protección de la PII durante la implementación de un ISMS en la nube (2015); dentro de los aportes de este nuevo estándar se destaca que toda información personal o dato sensible deben ser tratados de conformidad con las disposiciones del usuario, la prohibición de exigir el consentimiento del usuario para usar su información personal con fines publicitarios o de mercadeo a cambio de poder acceder a los servicios en la nube, las medidas sobre la divulgación de información a terceros y la eliminación de los datos personales. La relevancia de esta normativa también está dada por la revelación al usuario de los posibles lugares donde pueda ser almacenada y procesada su información así como las posibles organizaciones o personas que estarían a cargo de dichos procesos.

La ISO ha publicado hasta el momento más de veinticinco mil estándares en sus sesenta y ocho años de existencia. La serie 27000 ha contribuido a mejorar los niveles de eficacia de seguridad y privacidad de la PII en ISMS, ahora en la nube.

#### *3.1.6.2 International Telecommunications Union – ITU*

Otra de las organizaciones internacionales que ha abordado la seguridad y la privacidad en las TIC ha sido la Unión Internacional de Telecomunicaciones, ITU, institución asociada a las Naciones Unidas encargada de controlar las frecuencias radioeléctricas y las órbitas satelitales, elaborar las normas técnicas que aseguren la interconexión de las redes y las tecnologías, concentrando parte de sus esfuerzos en mejorar el acceso a las TIC en las comunidades menos favorecidas (2013). Activa desde 1865, con presencia en ciento noventa y tres países, y más de setecientos miembros a nivel mundial entre reguladores, universidades, instituciones para la investigación y el desarrollo, organizaciones regionales e internacionales, y compañías líderes en telecomunicaciones, internet, emisiones y transmisiones, satélites, desarrollo de software, e industrias de tecnología de la

información, convierten a la ITU en una autoridad mundial en ISMS. En 2012, el buró para la estandarización de las telecomunicaciones de la ITU, publicó un reporte titulado Privacy in Cloud Computing, identificando el gran reto que exige procesar la información personal en la nube ya que esta puede tornar obsoleta cualquier noción de privacidad. Cloud Computing, computación en la nube, es referida como la habilidad para acceder y manipular información almacenada en servidores remotos utilizando una plataforma habilitada para internet, incluyendo los teléfonos inteligentes (2013). Las ventajas económicas en la reducción de costos debido a la posibilidad de compartir recursos de almacenamiento y computación, combinadas con un modelo *pay-per-use*, pagar por usar, trae consigo diversas inquietudes sobre los mecanismos tradicionales de seguridad, confianza y privacidad; esta última es definida como el derecho a la autodeterminación, es decir, el derecho de los individuos a saber que se sabe de ellos, ser consciente de la información almacenada sobre ellos, controlar cómo esa información es comunicada y prevenir cualquier tipo de abuso con la misma. Esta concepción de la privacidad va más allá de la confidencialidad de la información, ya que cada individuo, para la ITU, deber tener el control de que su información personal sea pública, privada o profesional; debido a la facilidad con la que los datos pueden manipularse en la nube, es igual de fácil perder el control de los mismos, por tal motivo, la compatibilidad de los políticas, técnicas, mecanismos y protocolos de privacidad son fundamentales para la ITU, empezando por la utilización de una herramienta global llamada estándar, ítem del cual pudimos hacer una breve revisión en el apartado anterior. Cabe destacar que la ISO es una institución que ha trabajado muy de cerca con la ITU para diseñar sus estándares.

- El término acuñado por la Unión Internacional de Telecomunicaciones para la protección de la PII es PET, abreviatura de Privacy-Enhancing Technologies (Tecnologías de Privacidad Mejorada), tecnologías encargadas de la

privacidad, protegiendo los datos personales previniendo su procesamiento innecesario e indeseado pero haciendo al usuario consciente de sus datos almacenados, su procesamiento y los flujos de datos relacionados. La estandarización al interior de las empresas favorece esta práctica (International Telecommunication Union - ITU, 2012).

- Para implementar una PET en una empresa, la ITU recomienda seguir los principios de *Privacy by Design*, empezando por la Transparencia; la descripción del flujo del procesamiento de los datos es vital para hacer las precisiones necesarias en la evaluación de los riesgos que puede correr la información.

  Para ello, la ITU propone tener en cuenta las siguientes categorías en el análisis que se haga del flujo de los datos:

  - Tipo de Dato
  - Personas con derecho[24] a procesar los datos personales.
  - Plataforma Operativa
  - Aplicación de Procesamiento
  - Propósito del Procesamiento de los Datos
  - Modo de Protección
  - Tiempo de Almacenamiento y Medidas de Eliminación
  - Destinatario del Dato
  - Si el Dato es transferido fuera del país, indicar el país destino.
  - Esta propuesta va acorde con el ciclo de vida de los datos: recolección, transferencia, uso, almacenamiento, confidencialidad[25] y eliminación.

[24] El término en inglés es *entitled*, su traducción en español es *con derecho a*. Otro término válido es *titular*, sin embargo se prefirió no utilizarlo para evitar confusiones con la terminología empleada en la Ley Hábeas Data de nuestro país.
[25] El término en inglés es *sharing*. Su traducción también incluye términos como reparto, partición y compartir. Se optó por el de confidencialidad ya que es una acepción válida en el contexto de la PII.

Ahora bien, una vez establecida la guía para hacer protección efectiva de la información en la nube, el paso a seguir consiste en mitigar las dificultades que puedan presentar casos específicos utilizando la lógica caso-a-caso en relación con los servicios prestados en la nube. Debido a que los proveedores del servicio de la nube y los desarrolladores de la nube trabajan bajo la noción de interoperabilidad, la depuración de grandes bloques de información haría prácticamente imposible sentar una base operativa a partir de la caracterización individual. Para cumplir con parámetro de globalización que tiene la computación en la nube, las PET deben ser implementadas a partir de los principios de privacidad que toda arquitectura debe cumplir.

La primer PET que todo ISMS debe tener es aquella encargada de recolectar la mínima cantidad de información necesaria para un propósito dado, conservar el anonimato en estos casos es de gran utilidad. Los Anonymizer[26] son un tipo de tecnología empleada para este principio de *Proporcionalidad*, funcionan ocultando la información real en línea reemplazándola con una identidad temporal no rastreable, haciendo uso de seudónimos, direcciones IP aleatorias, direcciones de correo electrónico descartables; el usuario recibe una credencial de anonimato con cuya posesión demuestra ser el propietario de su PII, trabajando en un entorno interoperativo entre organizaciones. La credencial de anonimato puede revelar información selectiva de algunos atributos del Titular para que se le garantice el acceso a servicios específicos, como la edad; de igual manera, la credencial de anonimato protege la identidad del proveedor de servicio de computación en la nube, reduce la cantidad de información rastreable en cada una de sus operaciones o transacciones que puedan tornar vulnerable su privacidad. Para un efectivo funcionamiento de la credencial de anonimato, esta incluye pruebas de validez, también entendidas como Derecho de Acceso, requeridas para hacerse a

[26] PET que procesa la PII de un usuario, otorgándole a este el anonimato, impidiendo que la información real sea revelada.

los servicios en la nube, obtener un espacio de almacenamiento, o acceder a contenidos digitales bajo demanda.

Otra de las propuestas que incluye la ITU en su reporte es la Encriptación. Es una PET de gran acogida debido a que permite aislar los datos y sus respectivas políticas de privacidad en ambientes de múltiples inquilinos (también llamados ambientes sensibles), característica de la computación en la nube. Sin embargo, el consumo de poder de computación es elevado y los beneficios de la computación en la nube se ven reducidos. Este es uno de los mayores retos a superar en los años venideros, ya que el proceso de encriptación puede llegar a tornarse poco práctico para cumplir con el principio de confidencialidad, principio que a su vez es una obligación de mantener y respetar, incluso después del cese de la relación establecida entre el proveedor de servicios y el Titular de la información. Dentro de los últimos avances de la encriptación está el desarrollo de estrategias tipo SES[27]. Son mecanismos diseñados para garantizar la confidencialidad de la PII de cualquier usuario que elija almacenar sus datos en la nube sin perder rastro de ellos, aún si el proveedor de servicios no es del todo confiable. A partir del principio de encriptación asimétrica, el Titular recibe un *token* con el cual puede encontrar su información almacenada en la nube. El *hashing* es otra de las técnicas de encriptación muy útil para proteger las contraseñas de los usuarios, siendo bastante confiable para notificar posibles violaciones a la seguridad en un ISMS; al final, lo importante es que el Titular pueda rastrear su información encriptada y que no pierda el control sobre ella.

Otra de las propuestas valoradas por la ITU para cumplir con el principio de Control de Acceso a los Datos, es la del gigante Google Inc., ahora Alphabet Inc., llamada Google Dashboard. A pesar que el Titular tiene en este Panel de Control

[27] Abreviatura para Searchable Encryption Scheme. Traduce en español Estrategia de Encriptación Rastreable

el conocimiento de toda su información activa en los servicios de Google, que van desde correo electrónico a telefonía móvil, esta aplicación no es del todo compatible con las leyes que cada país sancione para proteger la PII de los ciudadanos. Un claro ejemplo de lo anterior es la Directiva de la Unión Europea: desde el año 2012 están haciendo seguimiento a las políticas de privacidad del gigante de la computación, liderado por la CNIL[28].

Existe también una alternativa dentro de las tecnologías valoradas por la ITU y es que los ISMS funcionen bajo un lenguaje estándar para configurar sus políticas de privacidad. El consorcio OASIS, liderado por IBM y Microsoft, desarrolló XACML manejando un algoritmo basado en la delegación; la principal función de esta PET consiste en soportar una administración descentralizada de las políticas de privacidad en un ISMS, de esta manera, se crea un nuevo nivel de accesibilidad a la información, sin necesidad de modificar las políticas de privacidad raíz en el sistema. Las características de este lenguaje se asemejan al método PDCA, mencionado en apartados anteriores, debido a la relevancia que tiene el comportamiento de los usuarios para determinar las dinámicas de privacidad necesarias en un sistema. Al ser un lenguaje desarrollado entre Microsoft e IBM, la compatibilidad se ve reducida a sus productos, limitando la versatilidad de XACML a otros OS[29].

#### *3.1.6.3 The World Wide Web Consortium W3C*

Fundado en 1994 por Tim Berners-Lee, el Consorcio de la World Wide Web, es una comunidad internacional encargada de desarrollar estándares para la WEB (W3C, 2015), actualmente cuenta con más de cuatrocientos miembros entre

[28] Commission Nationale de l'Informatique et des Libertés. Autoridad para la protección de los Datos en Francia
[29] OS : Operating Systems (SO: Sistemas Operativos)

organizaciones y personal de tiempo completo. El W3C tiene su oficina central en el Instituto de Tecnología de Massachusetts, MIT[30], con oficinas subsidiarias en el Consorcio Europeo de Investigación para la Informática y las Matemáticas, ubicado en Francia, y en las Universidades de Keio y Beihang, ubicadas en Japón y China, respectivamente.

El W3C contempla en su misión el llevar a la World Wide Web a su máximo potencial, desarrollando protocolos y lineamientos para asegurar el crecimiento a largo plazo de la Web. Son dos los principios de diseño que el W3C: la Web para todos y la Web todas las cosas; en el primero se destaca el valor social de la Web ya que posibilita la comunicación, el comercio y el intercambio de conocimiento, siendo su objetivo el de garantizar la disponibilidad para la mayor cantidad de personas sin importar el hardware, el software, la infraestructura de la red con la que cuentan, así como su idioma nativo y su ubicación geográfica.

El segundo principio consiste en ampliar la presencia de la Web en las actividades cotidianas de cualquier individuo. Con el acelerado crecimiento en la producción de teléfonos inteligentes, asistentes personales digitales, sistemas de televisión interactivos, sistemas de respuesta de voz, electrodomésticos con conexión a redes inalámbricas, el consorcio ha decidido promover el concepto de "*One Web*". Para el W3C, la disponibilidad de la web para cualquier dispositivo va más allá de los factores relevantes para la conectividad, también es importante asegurar la mejor experiencia usuario[31], con arquitecturas multimodales, permitiendo que las aplicaciones puedan adaptarse a nuevos modos de interacción. A partir de lo anterior, se podría entender la disponibilidad propuesta en el concepto de la *One Web*, como la disponibilidad de conectividad que debe tener todo dispositivo para aprovechar al máximo sus aplicaciones y tener mayor eficiencia en su

[30] MIT - Massachusetts Institute of Technology
[31] UX: User Experience, por sus siglas en inglés.

funcionamiento; sin embargo, la conectividad de los dispositivos, sea a través de nodos fijos o de forma inalámbrica en entornos sensibles, la disponibilidad también atiende a la información y los contenidos que el usuario desea acceder desde su dispositivo.

Para el W3C, las preocupaciones sobre la seguridad y la privacidad de la PII no son un asunto reciente. En 1996 fueron presentados los estándares de XML[32] para su funcionamiento y su combinación con los lenguajes de HTML, RSS y KML. Este primer avance en la seguridad se vio fortalecido, dos años después, con el desarrollo del Proyecto de la Plataforma para las Preferencias de la Privacidad, P3P [33], diseñado para promover la privacidad y la confianza en la Web, permitiendo a los proveedores de servicio divulgar sus prácticas sobre la información, y habilitando a los individuos a tomar decisiones informadas sobre la recolección y el uso de su PII (W3C NOTE, 1998). La noción de confianza a la que atiende el W3C con esta plataforma consiste en el entendimiento mutuo al que deben llegar las partes, proveedor de servicios y usuario. Este es el primer protocolo que incluye un apartado sobre la manipulación de la PII y la privacidad de los niños en la Web. Para describir su funcionamiento, P3P ha incluido las siguientes definiciones relativas a los participantes en los procesos de seguridad y privacidad de la PII (W3C NOTE, 1998):

- **Información Personal (PII):** es todo dato relacionado a un usuario identificado o identificable, que ha sido transferido a un servicio o que ha sido almacenado bajo P3P.

- **Preferencias:** es el conjunto de reglas que determina qué acción tomará o permitirá el agente de usuario, durante una negociación o una interacción

[32] *Extensible Markup Language*, lenguaje que describe un tipo de datos denominados *XML Documents*, que consisten de unidades almacenadas llamadas *entidades*, los cuales contienen datos que son o no, analizados sintácticamente. Además, provee un mecanismo para imponer restricciones en la disposición del almacenamiento y su estructura lógica.
[33] Platform for Privacy Preferences Project

con un servicio específico. Las preferencias van encaminadas a reflejar la actitud del usuario respecto al uso y la divulgación de su PII.

- **Propuesta:** es una serie de declaraciones de P3P que describen las prácticas y los términos relacionados a la privacidad bajo la cual un servicio pretende interactuar con un usuario o un agente de usuario.

- **Proveedor de Servicio:** es la persona u organización que ofrece información, productos o servicios para un sitio web, recolecta información y es responsable por las representaciones hechas en una declaración de práctica sobre la seguridad y la privacidad. El anterior proveedor de servicio descrito no es el mismo proveedor de internet, *ISP*, por sus siglas en inglés.

- **Usuario:** es el individuo o el grupo de individuos, que actúan bajo una entidad, que acceden a un servicio y del cual existe PII.

- **Agente de Usuario:** es el programa que actúa en representación del usuario, sobre sus preferencias de privacidad, confidencialidad, filtración de contenidos y toda actividad relacionada con la manipulación de su PII.

A partir de lo anterior, entran en juego las siguientes variables para que la plataforma P3P sea implementada eficientemente (W3C NOTE, 1998):

1. **Aviso y Comunicación:** el Proveedor de Servicio debe notificar periódica y efectivamente a los usuarios sobre sus prácticas y sobre la PII, así como los Agentes de Usuario deben procurar herramientas efectivas a los usuarios para que puedan acceder a dichas notificaciones y tomar decisiones basadas en las mismas.

2. **Elección y Control:** el usuario debe estar habilitado para hacer elecciones significativas sobre la recolección, uso y divulgación de su PII. De igual manera, el usuario debe tener control sobre la misma y decidir las condiciones de confidencialidad bajo las cuales va a ser almacenada.

3. **Legitimidad e Integridad:** el Proveedor de Servicio debe hacer tratamiento de la información del usuario únicamente para el propósito declarado y por el tiempo que sea necesario, asegurando su precisión, completitud y actualización.

4. **Seguridad:** aunque la plataforma P3P no incluye un mecanismo de seguridad en sí misma, sí debe operar en conjunto con las herramientas de las que disponga el Proveedor de Servicio y el Usuario. P3P es una plataforma que permite ser compatible con cualquier protocolo de seguridad y privacidad, ya que opera bajo el principio de *One Web*, mencionado arriba.

La característica fundamental de la operatividad de la plataforma P3P es que utiliza descripciones legibles para la máquina al momento de describir la recolección y el uso de los datos, esto logra que los sitios que la implementan hagan sus prácticas sobre los datos y la PII más explícitas. Para generar una interacción más sencilla entre los usuarios y la plataforma, los navegadores pueden generar interfaces inteligentes, ayudando a desarrollar un comportamiento predecible en el usuario, de esta manera, podrá bloquear el contenido no deseado de una forma más eficiente.

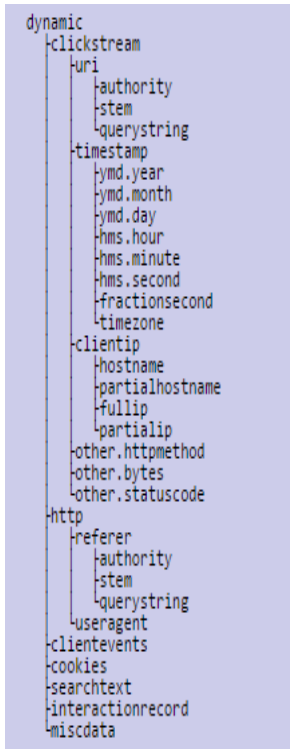
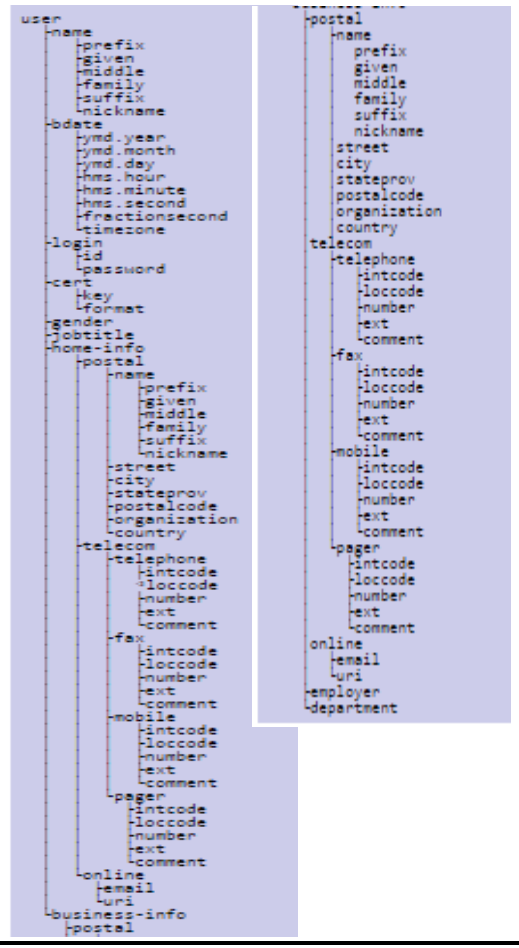
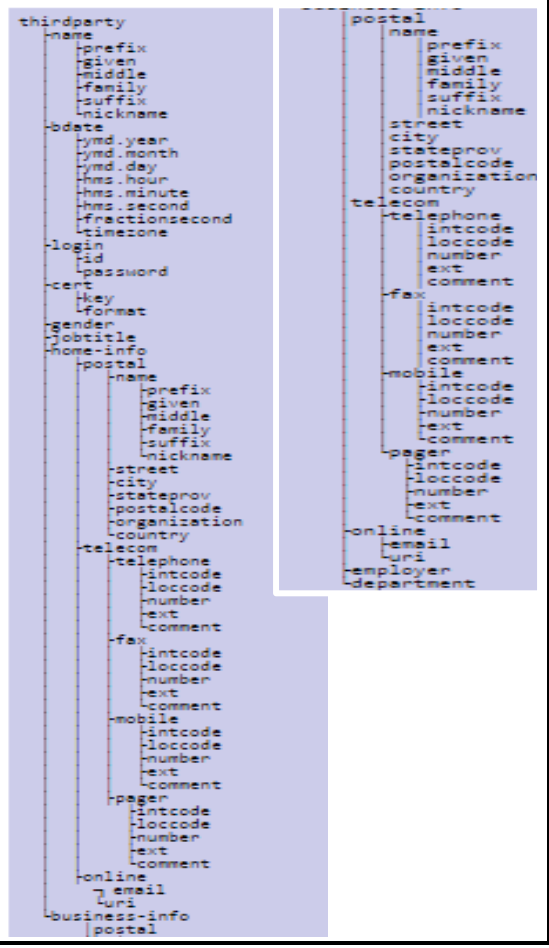
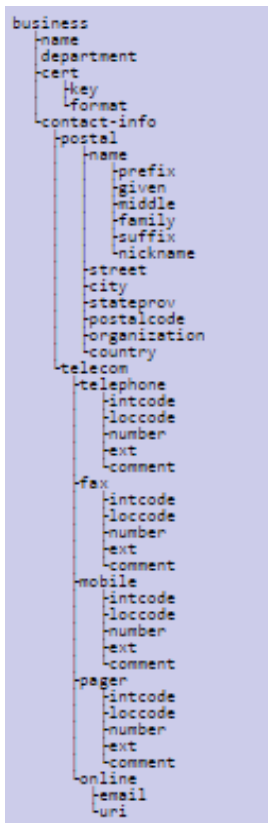
Cuatro años más tarde de su liberación, la plataforma recibió su primera actualización, denominada *P3P 1.0.* Funcionando bajo las premisas anteriores,

esta nueva versión (W3C Recomentation, 2002), habilita a los Sitios Web a que expresen sus prácticas de privacidad en un formato estándar que pueda ser recuperado e interpretado fácilmente por los agentes de usuario. Aunque P3P provee un mecanismo técnico para asegurar que los usuarios puedan ser informados de las políticas de privacidad de los sitios antes de liberar su PII, P3P carece de un mecanismo para asegurarse que los sitios actúen de acuerdo a las preferencias de usuario, así como tampoco dispone de mecanismos para transferir o asegurar datos en tránsito o en almacenamiento.

En 2006 la plataforma liberó una nueva versión, *P3P 1.1.* Esta nueva especificación (W3C Working Group Note, 2006) define la sintaxis y la semántica de las políticas de privacidad de P3P, así como los mecanismos para asociar sus políticas con las de los recursos Web. Dichas políticas consisten en declaraciones hechas usando el vocabulario P3P para expresar las prácticas de privacidad. Una de las fortalezas, y a la vez falencia de la segunda versión de la plataforma, es su *Data Base Schema*[34]; este es un conjunto de elementos de datos, organizados de manera jerárquica en cuatro tipos de diagrama: Diagrama de Datos Dinámico, Diagrama de Datos de Usuario, Diagrama de Datos de Terceros y Diagrama de Datos de Negocios. A pesar de tener una espina dorsal mucho más robusta, la falencia a la que se hace referencia es que no es fácilmente legible para el usuario. La siguiente tabla (Tabla 1) presenta los gráficos del resumen de la jerarquía del esquema de la base de datos mencionada (W3C Working Group Note, 2006):

[34] Diagrama de Base Datos

Tabla 1 : Data Base Schema

| Diagrama de Datos Dinámicos | Diagrama de Datos de Usuario | Diagrama de Datos de Terceros | Diagrama de Datos de Negocio |
|---|---|---|---|
|  |  |  |  |

Resumen de la jerarquía del esquema de la base de datos de la W3C; Tomados de http://www.w3.org/TR/P3P11/#dynamic_data

El estado actual de la Plataforma P3P no cuenta con una versión posterior a la liberada en 2006. Las críticas recibidas por sus falencias han hecho que el proyecto haya adoptado un carácter de mayor impacto debido al creciente número de producción y compra de dispositivos móviles, aumentando el número de usuarios y su relación proporcional con la cantidad de contenidos y de información sensible en la web. Sin embargo, la priorización del desarrollo de P3P 1.2., conserva su estatus inicial debido a la compatibilidad que esta plataforma presenta con otros protocolos y técnicas disponibles para garantizar la privacidad de la PII en un ISMS.

## 3.2 SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD INFORMÁTICA

La seguridad es uno de los pilares fundamentales en cuanto a la gestión de cualquier tipo de recurso. Siendo la información un activo valioso en la red, diversas definiciones han sido presentadas por las autoridades mundiales en telecomunicaciones y estandarización para abordar la seguridad de forma precisa. Según la ITU-T, la seguridad es la prioridad de reducir al mínimo las vulnerabilidades de los activos y recursos en una red específica; lo anterior es compatible con la apreciación de la ISO, con la publicación del estándar ISO/IEC 27000 cuyo objetivo es el ofrecer los parámetros para gestionar adecuadamente la seguridad de la información, convirtiéndose en un marco de referencia para establecer, implantar, gestionar y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI)[35], dirigido a las técnicas, operaciones de seguridad, prácticas de controles de seguridad de la información y hace especial énfasis en que la información es un activo que hay que proteger, ya que es esta la que define y da sentido a la empresa, por lo tanto se debe tener control de acceso a ella y sobre todo conocer quién, el para qué y el cómo la procesan.

[35] ISMS por su sigla en inglés SGSI.

### *3.2.1 Seguridad de la información*

En el caso específico de la información, diversos autores han definido la **seguridad de la información,** como la protección de la confidencialidad, integridad y disponibilidad de la información (Costas Santos, 2014). Las anteriores características se definen como:

- **Confidencialidad**: consiste en garantizar que solo pueda acceder a la información que está protegida quien esté autorizado.

- **Integridad**: consiste en avalar solo a quien esté autorizado para modificar, añadir o suprimir información protegida, certificando que la información y sus procesos son exactos y completos.

- **Disponibilidad**: es una variable temporal, definida como el acceso a la información protegida en un momento específico, por el personal autorizado dependiendo del nivel de seguridad y tipo de aplicación utilizada para acceder a la misma. Es una prioridad que la información se encuentre disponible, de no ser así, puede ocasionar riesgos en el sistema.

### *3.2.2 Seguridad Informática*

Basados en lo anterior, **la seguridad informática**, consiste en proteger la información a ser almacenada o transmitida en función de lo que se quiere proteger y del momento en que tiene lugar la protección. Para alcanzarla, se han identificado distintos tipos de seguridad de acuerdo a su propósito; el primero se entiende como *lo que se quiere proteger:*

- **Seguridad física**: es la protección física del sistema ante amenazas como robos, incendios, etc.
- **Seguridad lógica:** son los mecanismos que permiten proteger un sistema informático, por ejemplo la criptografía, la cual permite proteger datos,

aplicaciones y sistemas operativos. La seguridad lógica también se ha definido como el conjunto de medidas destinadas a la protección de los datos y aplicaciones informáticas, así como garantizar el acceso a la información únicamente por las personas autorizadas. (Escrivá, G. G., et al, 2013)

El segundo tipo comprende *el momento en que tiene lugar la protección*, siendo dos*:*

- **Seguridad activa**: son las medidas preventivas que se encargan de evitar, detectar y alertar cualquier incidente en los sistemas de información.
- **Seguridad pasiva**: son las medidas correctivas que se encargan de minimizar las consecuencias de un acontecimiento que viole la seguridad informática en un sistema.

### *3.2.3 Políticas de Seguridad*

Toda empresa debe establecer normas claras que permitan conocer al usuario qué le está permitido, qué no le está permitido y los alcances de su acceso en una red. El conjunto de normas y protocolos de seguridad a seguir, definidos al interior de cualquier compañía, son denominados como políticas de seguridad informática corporativa. Dentro de los estándares presentados en las secciones preliminares, algunas medidas que se pueden establecer como mecanismos de seguridad son:

- **Autenticación de usuarios**: es una práctica básica que permite comprobar la identidad del usuario, por medio de un nombre de usuario y una contraseña.
- **Lista de control de acceso:** son los procedimientos que permiten controlar usuarios, roles o grupos de usuarios, a lo que pueden acceder y qué pueden hacer sobre los recursos.
- **Criptografía**: es la técnica que transforma un mensaje comprensible en un mensaje cifrado para evitar que personas no autorizadas tengan acceso y modifiquen la información.

- **Certificados digitales**: son todos los documentos digitales identificados por un único número en un periodo determinado, mediante el cual se acredita la identidad de su propietario.
- **Firmas digitales**: son los datos asociados a un usuario que pueden ser utilizados como identificación del firmante.
- **Cifrado de unidades de disco o sistemas de archivos**: es la práctica criptográfica que permiten proteger la confidencialidad de la información a partir de la transcripción a palabras claves, implementadas en un algoritmo de encriptación.

La clave para mantener la seguridad y confidencialidad de la información es establecer perfiles o roles de usuario; cuando la creación de VLANs tiene lugar, se debe hacer a partir de los tipos de preferencias, definidas a partir de los roles de usuario. Cada perfil tiene una categoría con autorizaciones específicas al acceso de la información. La utilización inapropiada de la autorización para acceder a determinada información está fuera del alcance del personal encargado de la gestión de los Sistemas de Información y depende del usuario únicamente.

### *3.2.4 Importancia de la Seguridad*

La evolución de las redes en la última década ha resignificado su concepto inicial; en la actualidad, debido a su auge y las amenazas detectadas, la seguridad de una red debe pensarse empleando soluciones puntuales como Firewalls y mecanismos de encriptación, permitiendo que las nuevas tecnologías sean aplicadas para identificar, prevenir y proteger todo tipo de vulnerabilidades posibles en ella. Las capacidades y las complejidades de las redes de información deben ser estimadas basadas en las limitaciones de las organizaciones que las usan, esto con el propósito de adoptar las medidas apropiadas para proteger su información; esta prioridad está también presente en la seguridad de las distintas herramientas informáticas, diseñadas para satisfacer las necesidades de los

entornos corporativos. Teniendo en cuenta los principios de seguridad de la información, la disponibilidad, continuidad y escalabilidad masiva de las redes, han ampliado y agilizado enormemente las capacidades de millones de usuarios en la gestión de sus datos; los beneficios de una red segura trascienden los imperativos de eficiencia y operatividad, ya que están pensados para favorecer la experiencia de usuario.

### *3.2.5 Control de Acceso a la Red (NAC)*

Basado en el estándar 802.1X de la IEEE, parte de la familia de protocolos para acceso a redes, los NAC, Control de Acceso a la Red, son una solución integrada que provee un mecanismo de autenticación para los dispositivos que deseen conectarse a una red de tipo LAN o WLAN (Congdon, 2000). Los primeros de su tipo se remontan a los orígenes de la Ethernet en la década de los setenta, pero solo hasta el nuevo milenio, con el incremento del uso de las redes LAN en lugares públicos y semipúblicos, se hizo visible la necesidad de asociar la identidad del usuario con el puerto de acceso a la red, estableciendo un acceso autorizado, habilitando los mecanismos de facturación y responsabilidad[36], y personalizando el entorno de acceso a la red, en una infraestructura de tipo AAA[37]. En una red LAN, los beneficios de un NAC incluyen el reconocimiento de los usuarios, sus dispositivos y sus roles en la red; el soporte de los dos protocolos de autenticación para plataformas AAA, RADIUS[38] y TACACS+[39], respectivamente; el cumplimiento de las políticas de seguridad consiste en la protección de las

[36] Los términos empleados son *Billing* y *Accountability*; ambos son del ámbito financiero. Se entiende que su uso es debido a la gestión de los datos y de la información en la red.
[37] AAA - *Authentication, Authorization and Accounting.*
[38] El protocolo de servicio de usuario de acceso telefónico de autenticación remota fue desarrollado por Linvingston Enterprises, Inc., como un protocolo de autenticación del servidor de acceso y de contabilidad. En RADIUS, la autenticación y la autorización están unidas. Si se encuentra el nombre de usuario y la contraseña es correcta, el servidor RADIUS devuelve una respuesta de Acceso-Aceptar e incluye una lista de pares de atributo-valor que describe los parámetros que deben usarse en esta sesión.
[39] Terminal Access Controller - Access Control System es un protocolo utilizado en infraestructuras AAA para los servicios y dispositivos de red, el cual tiene mayor uso en la administración del acceso a los dispositivos de red como Routers o Switches.

terminales, la infraestructura y la productividad del empleado, determinando los niveles de riesgo en los ambientes internos y el acceso de invitados; se minimiza la necesidad de actualizaciones para la infraestructura con opciones de despliegue flexible y compatible con aplicaciones de gestión de terceras partes; mitigando los riesgos de virus, gusanos y accesos no autorizados, reduciendo las irrupciones a gran escala, facilitando una alta eficiencia en TI (CISCO, 2014), (Tacacs, 2011), (Cisco, 2015).

Las redes inalámbricas cuentan con un alcance aproximado de cien metros a la redonda y corresponden a las especificaciones ofrecidas en los estándares de la IEEE 802.11 (Parekh, 2014) y el hiperLAN2 del ETSI (ETSI, 2000), en Europa. En una red inalámbrica los nodos se comunican entre sí, de forma directa; al momento de iniciar la transmisión entre los nodos, a través del punto de acceso, se logra el acoplamiento coordinado entre la red cableada y la red inalámbrica. La implementación del NAC en una WLAN ha tenido gran aceptación ya que permite integrar la autenticación de la red, el control de acceso y no repudio[40], y tiene por objeto garantizar un entorno de red seguro con la autenticación del usuario final establecido en el cumplimiento de políticas de seguridad. De igual manera, permite el acceso a la red basado en la evaluación del comportamiento de los dispositivos en las terminales y restringe el acceso de los dispositivos que no cumplen las normas de acceso.

Con lo anterior se puede evidenciar que un NAC no es un producto, es un proceso. Su enfoque es la gestión de riesgo y de usuarios (Robinson, 2007). Los operadores de red pueden definir políticas, en cuanto a los roles de usuario, nivel de acceso y áreas de red en la que se les permite el acceso. Los controles de acceso a la red de pueden clasificar de la siguiente manera:

[40] No repudio: evitar que cualquiera que envía o recibe información alegue ante terceros que no envió o no recibió

- **Basado en hardware**: requiere de un equipo que tendrá que estar instalado en casi cualquier ubicación donde sea preciso contar con un NAC. Puede ser "in-line"[41] o "out-of-band"[42].
- **Basados en agentes software**: son pequeños programas residentes en los PCs y dispositivos, donde el NAC controla los sistemas con agentes en cada uno de ellos. Su función consiste en escanear y monitorear el dispositivo, generalmente enviando los resultados al servidor central, controlando el acceso a aquellos sistemas que no cumplen con los requisitos. Así mismo se les envían algún tipo de medida correctora para que cumplan las directivas de seguridad.
- **Sin agentes software**: los NAC sin agentes, es otra de las variantes y consiste en partes de software que se ejecutan puntualmente. Con esta configuración, un agente temporal escanea el cliente periódicamente en búsqueda de vulnerabilidades o incumplimientos en la política de seguridad. Los resultados del escaneo son enviados al servidor central de políticas, y se ejecuta una acción en caso de que el sistema no cumpla con los requerimientos. Cuando el proceso se completa, el agente se descarga
- **NAC dinámico.** En este proceso solo se utilizan agentes en un porcentaje determinado de equipos. También se conoce como NAC peer-to-peer, siendo una opción que no requiere cambios a nivel de red o software que deba ser instalado en cada equipo. Los agentes, que en ocasiones pueden llegar a ser obligatorios, son instalados en sistemas seguros (WatchGuard Technologies Inc., 2008).

### *3.2.6 Motor de Servicios de Identidad – Cisco ISE*

Las soluciones NAC permiten a los departamentos de TI definir e implementar políticas de seguridad, tipos de PCs, y roles de tipos de usuarios con acceso a la

[41] En línea con el tráfico de usuarios
[42] Fuera de banda para permitir a los clientes atraviesan solo la red Clean Access durante la vulnerabilidad, evaluación y remediación. (evaluación de la postura).

red. Los dispositivos NAC permiten el acceso basándose en comparar identidades de usuarios autenticados, para usuarios finales de equipos portátiles y móviles.

Cisco cuenta con un motor de servicios de identidad ISE[43], que reduce los ataques que surgen a través del control de acceso; dentro de las ventajas que CISCO muestra al trabajar con plataformas NAC están:

1. La completa visibilidad de puntos finales, proporcionando un acceso uniforme y seguro a usuarios finales e identificación de dispositivos más precisa.
2. La incorporación de contexto sensible en la plataforma NAC.
3. La integración con otras plataformas de seguridad para mejorar la eficacia de las defensas del perímetro.
4. La detección de comportamientos sospechosos de los usuarios de la red.

ISE de CISCO reduce los ataques que surgen controlando el acceso y previniendo movimiento lateral no autorizado en la red. Basado en la información contextual recolectada, el Motor de Servicios de Identidad, ISE, crea una política de control de acceso basada en el rol RBAC[44], al hacer una evaluación de los terminales y los perfiles de usuario. En caso que un terminal se encuentre comprometido por alguna amenaza, el ISE notifica al administrador y puede cambiar la política de acceso para contenerla o ponerla en cuarentena. Otra ventaja del Motor de Servicios radica en la incorporación de la tecnología Cisco TrustSec, integrada en los Routers y Switches para reforzar la política de seguridad a través de la red.

Además. Cisco ISE provee un monitoreo completo, reporte y alarmas para todas sus funciones desde el panel de control NAC, evaluación por perfiles AAA, invitados BYOD y acceso MDM. El servicio de alimentación dinámica de dispositivos es continuamente actualizado y si un servidor se ve comprometido y

[43] Identity Services Engine- Motor de Servicios de Identidad.
[44] Role – Based Access Control - RBAC por su sigla en inglés.

empieza a reenviar el tráfico como servidor SMTP[45] ilegitimo, el ISE puede reclasificar el dispositivo y cambiar su nivel de acceso a partir de los sondeos realizados por NetFlow. Un instrumento propio del sistema operativo de Cisco, encargado de caracterizar la operatividad de la red.

La integración del ISE con la sensibilidad en el contexto ocurre cuando la visibilidad de un terminal se intersecta con señales de otra infraestructura de red, aplicaciones y defensas de seguridad. El ISE usa el contexto para centralizar y unificar el control de acceso transmitido en la política de acceso a la red segmentándolo dinámicamente sin la complejidad de múltiples VLANs y sin cambiar la arquitectura de la red. Al contar con una plataforma robusta de acceso compartido pxGrid, se acelera la eficacia de la red y las soluciones de seguridad. La anterior plataforma también funciona para integrar el NAC con otras plataformas de seguridad para acelerar las características de sus soluciones e identificar, mitigar y remediar las amenazas en la red. Estas mejoras de seguridad expandidas ofrecen nuevas posibilidades como la detección avanzada de amenazas en la red, ATD[46], el fortalecimiento de los Firewalls y el reforzamiento de los antivirus.

## 3.3 EL CONTEXTO

La definición precisada por la Real Academia de Española (RAE, 2014), indica que es todo entorno lingüístico del cual depende el sentido y el valor de una palabra, frase o fragmento considerados. El valor al que hace referencia proviene del carácter relacional que tiene el lenguaje, donde la interacción entre los elementos del discurso permite que este se pueda dotar de sentido, cuya dependencia a los valores de tiempo y espacio es absoluta; el resultado de este

[45] Simple Mail Transfer Protocol – SMTP por su sigla en Inglés
[46] Advanced Threat Detection - ATD por su sigla en inglés.

fenómeno es la consideración de que todo discurso se comporta como una unidad de significado y sentido completo. El contexto permite que el contenido y efecto del discurso sea comprensible, atendiendo las variables de tiempo, ubicación geográfica, mencionadas anteriormente, así como el entorno sociocultural y psicológico. (Manzano, 2005)

Según Pablo Haya, en su escrito lo define como una parte fundamental de la comunicación humana, que actúa para establecer el significado de la palabra, simplifica la comunicación y que permite dar sentido al mensaje. (2006)

Este concepto tiene gran relevancia para el desarrollo de las redes de computación y su posterior evolución en la computación ubicua, computación en la nube y los entornos sensibles. Varios autores han abordado su definición, aplicada a la computación ubicua, buscando una aproximación precisa para sus objetivos: Dey y Abowd, profesores asociados a la Universidad de Carnegie Mellon, lo definen desde el punto de vista del software, la definición más aceptada es la que brinda (Dey A. K., 2001): “el contexto es cualquier información que puede ser usada para caracterizar la situación de una entidad. Una entidad puede ser una persona, un lugar o un objeto que es considerado relevante para la interacción entre el usuario y la aplicación; incluyendo al usuario y la aplicación misma”.

Paul Dourish, catedrático asociado a la Universidad de California, sugiere que la noción de contexto tiene un origen dual: uno de carácter técnico y otro que corresponde a las ciencias sociales (Dourish, 2004). El primero ofrece a los desarrolladores de sistemas de computación ubicua nuevas maneras de conceptualizar la acción humana y la relación entre dicha acción y los sistemas computacionales para soportarla; la segunda, el contexto provoca la atención

analítica de aspectos determinados en el marco de los comportamientos sociales. Dourish afirma que una de las principales dificultades para el diseño de sistemas que operan en entornos sensibles son las conjeturas que se han generado a partir del *contexto*, para sustentar su operatividad en dichos sistemas (2004, pág. 20):

- ***El contexto es una forma de información**:* el contexto es algo de aquello que se conoce y todo lo que se conoce puede ser codificado y representado como cualquier otro tipo de información.
- ***El contexto es definible**:* es posible definir lo que cuenta como contexto de las actividades que una aplicación de un sistema soporta, desde las exigencias del sistema.
- ***El contexto es estable**:* las entidades que permiten la representación del contexto pueden variar de aplicación a aplicación, pero no varían durante la ejecución de una actividad en el sistema.
- ***El contexto y la actividad son divisibles**:* toda actividad tiene lugar en el contexto ya que este describe las características del entorno en el cual la actividad tiene lugar. Sin embargo, estas características del entorno se pueden separar de la actividad.

En el año 2009, Kaiyu Wan, profesora del Departamento de Ciencias de la Computación e Ingeniería del Software de la Universidad Xi'an Jiaotong-Liverpool, publicó un artículo académico donde definía al contexto como un concepto rico y a la vez vago. Para ella, la participación de distintas disciplinas en la precisión del mismo, como la lingüística, la filosofía y las ciencias de la computación, han interpretado su significado de acuerdo a los objetivos propios de cada una de ellas sin lograr una precisión definitiva del término (Wan, 2009). Sin embargo, en lo que compete al desarrollo de sistemas, Wan propone que más allá de una definición totalizadora del concepto, es necesario hacer una descripción del conjunto finito de las entidades que intervienen en él, identificando el conjunto de propiedades para cada una de ellas, teniendo presente aquellas propiedades que se

entrecruzan de entidad a entidad. La elección de entidades, la elección de las propiedades, y la notación utilizada para interrelacionarlas son cruciales; esta percepción de contexto puntualiza las posibles interpretaciones a las que se pueda ver sujeto durante la puesta en marcha de un sistema, eliminando las ambigüedades.

Proyectando el crecimiento que tendría la computación ubicua en la segunda década del nuevo milenio, Gideon Gartner, fundador y actual presidente ejecutivo de Gartner Inc., empresa consultora y de investigación en tecnologías de la información, en un reporte del año 2010 (Macdonald & et.al), define al contexto como las circunstancias dentro de las cuales algo existe o sucede, y que puede ayudar a explicarlo o entenderlo. El enfoque principal de esta compañía es el análisis y la interpretación del negocio de las TIC, lo anterior sumado a sus investigaciones en el campo de la seguridad en la computación en entornos sensibles, uno de sus más importantes campos de acción (Gartner Enterprise); basados en lo anterior, Gartner, al igual que los catedráticos citados en este apartado, identifica la entidad como la base para tomar decisiones respecto de la seguridad en una red, identificando las siguientes siete categorías: Proceso, Contenido/Información, Identidad, Aplicación, Sistema Operativo, Dispositivo, Red, que a su vez incluyen entidades físicas o lógicas como los paquetes de datos, la máquina, las aplicaciones, los servicios, los usuarios, los grupos de usuario, las transacciones entre otras actividades que tienen lugar en un entorno sensible en la Red. El aporte de Gartner prioriza el paradigma de la infraestructura del sistema, caracterizando las dinámicas que tienen lugar en este, gracias a las entidades que participan en el contexto.

### *3.3.1 Tipos de Contexto*

Con las definiciones ofrecidas en el apartado anterior, se pueden identificar cuatro tipos de contexto, que adquieren mayor relevancia sobre los demás en la praxis de

la computación ubicua, estos son: *lugar, identidad, actividad y tiempo*. El primero corresponde a la capacidad relacional que tienen las entidades entre sí, de acuerdo a las propiedades individuales de cada una de ellas. El segundo, basado en el tipo anterior, es una forma cercana a la información pero está dotada de sentido gracias a la caracterización de los roles que tiene la *identidad* en cualquier actividad que esté teniendo lugar en el sistema, ya que todo contexto puede ser definible y limitado, sin ser del todo estático. Ahora bien, todo contexto es activamente producido, sostenido y representado por la actividad en cuestión (Dourish, 2004). El atributo temporal del contexto se da gracias a la finitud de su definición y la limitación de la actividad ejecutada en el mismo, convirtiéndose en un evento ocasional, con dinámicas específicas para propósitos específicos en un tiempo determinado. Es decir, cada uno de los tipos de contextos expuestos responden a los interrogantes de *dónde, quién, qué* y *cuándo* tiene lugar un evento en una red.

### *3.3.2 Context-Aware Computing: Computación Sensible al Contexto*

El surgimiento de las tecnologías de la computación pervasiva o ubicua ha transformado significativamente la forma de trabajar con las TIC, funcionando bajo el paradigma de la computación en cualquier momento, en cualquier lugar, para cualquier persona. El término *ubicuidad*, relacionado directamente con Dios, presente en todo momento y en todo lugar (RAE, 2014), ha permitido que la movilidad y la portabilidad de la información de los usuarios deje de estar sometida a un dispositivo específico para poder acceder a ella. La Computación Ubicua se vale de varios recursos para funcionar eficientemente, sin embargo, sigue siendo una materia de estudio para las ciencias de la computación debido a la constante expectativa en las mejoras y en los alcances que puede llegar a tener, tanto en materia de desarrollo como en materia de seguridad. Lo que en un principio se percibió como un *reto*, ha adoptado la connotación de *riesgo*, y siendo un sistema dinámico, cambiante y evolutivo, el día a día parece convertirse en una pequeña

fracción de segundo: un oxímoron de costo-beneficio, en un escenario limitado y adaptable.

La primera investigación que se hizo en torno a la *Computación Sensible al Contexto* [47] fue la de Olivetti Active Badge, en 1992, quienes utilizaron comunicación por medio infrarrojo, entre las placas de los usuarios y los sensores ubicados en las instalaciones de la compañía, para monitorear el movimiento y la ubicación de sus empleados para reenviar las llamadas telefónicas (1992). En 1993, la compañía norteamericana XEROX, pone en marcha el experimento PARCTab[48], cuyo principal objetivo era clarificar los problemas en el diseño y la aplicación involucrada en la construcción de un sistema de computación móvil dentro de un edificio de oficinas. El sistema estaba basado en computadores inalámbricos tipo tableta y la comunicación por infrarrojo, enlazando los computadores, unos con otros, y a computadores de escritorio, con terminales fijas, a través de una red de área local, LAN. La proyección del sistema ideal consistía en un mecanismo de rastreo, en tiempo real, que obtuviera las ubicaciones y el estado operativo de muchos de los componentes del sistema, y utilizar ese contexto para enviar mensajes inteligentemente. Debido a las dificultades de espacio y poder de los dispositivos, las dos tecnologías disponibles para acometer la comunicación inalámbrica fueron la radio y el infrarrojo, optando por este último debido al bajo consumo de energía y las velocidades de comunicación de 9600 a 19200 baudios, y las ventajas que traía trabajar con un sistema que no se encontraba regulado bajo licencia de operación como la emisión de ondas de radio. Estos primeros pasos en la computación ubicua, significaron grandes aportes, no solo a los futuros avances tecnológicos sino también a la filosofía de una computación abierta, ilimitada y portable. (Diciembre, 1995., pág. 28).

[47] En Inglés *Context- Aware Computing.*
[48] La abreviatura PARC significa *Palo Alto Research Center*; *Tab*, es una abreviación utilizada en inglés para las tabletas, *small Tablet computer*.

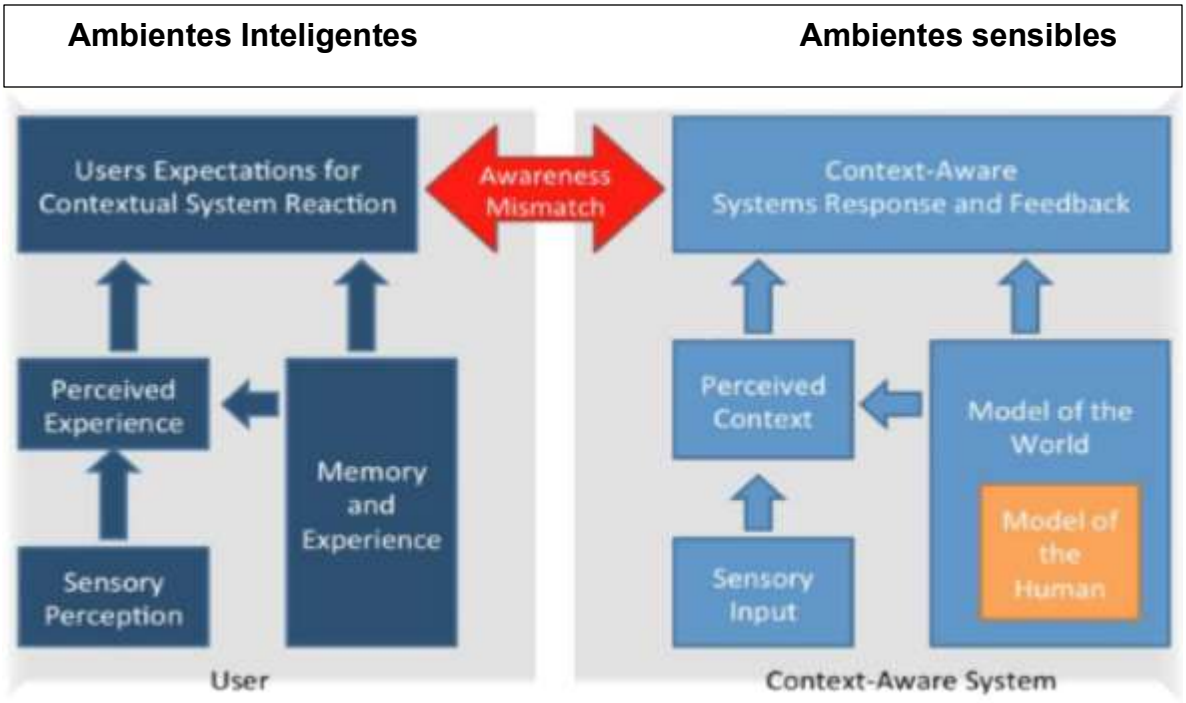
Sin embargo, los primeros en introducir el término fueron Schilit y Theimer; lo definieron como todo software que se adapta de acuerdo a la ubicación de su uso, el grupo de personas y objetos en sus alrededores, así como los cambios de dichos objetos en el tiempo (1994).

En la actualidad, el concepto de *Computación en un Contexto Sensible* se ha convertido en sinónimo de otros términos como *adaptabilidad, reactividad, grado de reacción, situado, y ambientalmente orientado.* Las definiciones ofrecida por Hull describe este tipo de computación como la habilidad que tienen los dispositivos para detectar y sentir, interpretar y responder a los aspectos del entorno local del usuario y del dispositivo (1997). Otros autores lo definen como la habilidad de proveer el máximo de flexibilidad de un servicio computacional (Salber D, 1998) o la automatización del sistema de un software basado en el conocimiento del contexto del usuario (Dey A. et al., 1999). La definición de mayor aceptación fue la que Abowd ofreció en el Primer Simposio Internacional de Computación Ubicua y Portátil, en Londres: "*Todo sistema que use el contexto para proveer información o servicios relevantes al usuario, cuya relevancia depende directamente de la tarea que el usuario esté desempeñando"* (2012). Se considera que esta definición es una de las más precisas ya que también permite a inclusión de entornos académicos, objeto de estudio del presente documento, y que será revisado en apartados posteriores.

### *3.3.3 Información Contextual*

Caracterización del conocimiento de la situación del usuario en un momento dado. (Dey A. K., 2001), y el punto más importante es determinar la información contextual que debe suministrar el usuario al sistema para lograr una interacción natural.

Imagen 3 : La percepción Modelo Usuario - Contexto (UCPM




Donde se describe el desequilibrio entre la percepción del usuario y un entorno sensible. Fuente: (Schmidt, 2015)

Entorno en el que los usuarios interactúan de forma transparente por medio de sus dispositivos, que se encuentran interconectados y a Internet, permitiendo intercambiar información y servicios.

### *3.3.4 Aplicaciones Sensible al Contexto (Context-Aware Applications)*

Una aplicación es un software que le permite al usuario completar tareas, por ejemplo: crear documentos, hojas de cálculo, bases de datos, publicaciones, hacer búsquedas en línea, enviar correos electrónicos, realizar negocios, entre otras, ya que están diseñados con el objetivo de mejorar la productividad de un individuo. Cada aplicación cumple una tarea específica y responde a las necesidades implícitas del usuario durante el desarrollo de la misma. Cuando se

habla de *Aplicaciones Sensibles al Contexto*, la adaptabilidad de la aplicación es uno de los parámetros fundamentales para un funcionamiento eficiente, este tipo de aplicaciones cambia dinámicamente o adapta su comportamiento basado en el contexto de la aplicación y del usuario, proveyendo información o ejecutando procesos en tiempo real cuando es detectado por los sensores.

Pascoe, por su parte, propuso una taxonomía que apuntaba a identificar las características fundamentales del Contexto Sensible. Basado en este primer paso, las aplicaciones debían tener la habilidad de detectar información contextual y presentarla al usuario, aumentando su sistema sensorial. Este atributo se definió como *Sensibilidad Contextual*. La segunda característica, definida por el autor como *Adaptación Contextual,* es la habilidad de ejecutar o modificar un servicio automáticamente basado en el contexto inmediato (1998.). Toda aplicación también debe tener la posibilidad de localizar y explotar los recursos y servicios que son relevantes para el contexto del usuario, definido como *Descubrimiento del Recurso Contextual*. La última característica propuesta por Pascoe es la de *Aumentación Contextual,* descrita como la habilidad de toda aplicación para asociar el dato digital con el contexto del usuario, presentando información relevante, incluyendo el contexto.

Otra apreciación sobre las aplicaciones sensibles al contexto la muestra Dey donde las define de la siguiente manera: “Un sistema es sensible al contexto si utiliza el contexto para proveer información y/o servicios relevantes para el usuario, donde la relevancia depende de la actividad del usuario” (2001)

Según Haya Coll, define Aplicación sensible al contexto como aquella que emplea el contexto como medio para ofrecer al usuario información y/o servicios, dependiendo qué necesita el usuario en un momento dado, (2006) y pueden ser clasificadas en:

- **Presentación de Información**: son aplicaciones que muestran información personalizada según el contexto del usuario.
- **Ejecución Automática**: es la ejecución de un servicio dependiendo del contexto.
- **Etiquetado del Contexto**: rotula un contexto para que el usuario pueda consultarlo en otro momento y observar cambios en él.
- **Aplicaciones Activas**: son aplicaciones que se adaptan a la actualización del contexto automáticamente, modificando su comportamiento.
- **Aplicaciones Pasivas**: son aplicaciones que reaccionan a los cambios del contexto a petición del usuario, guardando los cambios para ser recuperados posteriormente.

Se ha encontrado otras diferentes propuestas de categorización del contexto, por lo tanto existen diferentes puntos de vista sobre las características de las aplicaciones para ser consideradas como sensibles al contexto. Según Hervás Lucas & Bravo Rodriguez muestra que son cuatro requisitos los que determinan si una aplicación es sensible al contexto (2009):

- **Percepción contextual:** Es la capacidad de adquirir la información del contexto y poder mostrarla a los usuarios. Es la habilidad más básica que debe tener una aplicación consciente de contexto**.**
- **Adaptación Contextual:** Capacidad de reaccionar adecuadamente a los cambios en el contexto, que pueden ser provocados por las propias acciones de los usuarios, por cambios en las propiedades físicas, disparadores de sucesos, etc.
- **Detección contextual de recursos:** Las aplicaciones tienen que ser capaces de conocer el estado y acciones de las distintas entidades presentes, tanto usuarios como dispositivos.

- **Amplificación Contextual:** Es la capacidad de combinar las tres anteriores para ofrecer servicios implícitos al usuario.

El progreso en los últimos quince años en el diseño y desarrollo de Aplicaciones Sensibles al Contexto, el crecimiento en su uso, así como la incursión de los ambientes inteligentes en distintos escenarios, como el sector laboral, el sistema de salud, incluso en la misma vivienda, han generado la necesidad de profundizar más en la comprensión del concepto de adaptabilidad, evaluando el impacto del cambio. Ya que las aplicaciones responden al comportamiento de los usuarios, al uso que hagan de ellas, a las actualizaciones y personalizaciones para afrontar nuevos requerimientos de los sistemas a los que se conecten. Las dinámicas del contexto se han convertido en las determinantes en el rendimiento de cualquier aplicación. Estos cambios a los que se hacen alusión pueden ser internos o externos, y está en el desarrollador de las aplicaciones, encontrar la forma de anticiparlos a través de un Análisis de Impacto de Cambio –CIA[49], teniendo en cuenta que pueden ocurrir cuando se hacen modificaciones en el código del programa, o cuando el contexto del usuario o las circunstancias del sistema inteligente evoluciona. Con esta nueva tendencia, se puede hacer una mejor evaluación y seguimiento de las propiedades de coherencia, seguridad, privacidad y fiabilidad de las aplicaciones sensibles al contexto (Preuveneers & Joosen, 2015).

El profesor Albrecht Schmidt, asociado a la Universidad de Stuttgart y encargado de la cátedra de HCI[50], en una entrevista concedida a la Interaction Design Foundation (2015) aportaba a los planteamientos de Preuveneers que uno de los principales objetivos de los desarrolladores de aplicaciones sensibles al contexto consiste en “diseñar un sistema interactivo fácil de manejar, creando experiencias de usuario que se fijen en los pequeños detalles para hacerla mucho más

[49] *Change Impact Analysis*, *CIA,* por sus siglas en inglés.
[50] HCI - Human-Computer Interaction

relevante, teniendo en cuenta las dinámicas y la arquitectura del Contexto Sensible". Parte de la causa para que las aplicaciones presenten dificultades en el desempeño, cuando se encuentran funcionando en contexto, según Schmidt, consiste en que la computación en Contextos Sensibles no funciona a un 100%, no es perfecta. A lo anterior se suma que los sistemas pueden comportarse de una forma aleatoria, y a menudo los usuarios pueden encontrarse con casualidades al momento de interactuar en un entorno sensible, a diferencia de uno que no lo es, ya que su comportamiento es más fácil de mensurar debido a que funciona de una forma determinística. En cierta medida, este tipo de comportamiento hace mucho más comprensible su funcionamiento a diferencia de la computación en contextos sensible. Debido a que en la computación en contextos sensibles, los sistemas pueden presentar un comportamiento aleatorio, siempre van a traer dificultades para generar un nivel de satisfacción en los usuarios, ya que los sistemas se adaptan constantemente: identificando elementos del mundo real y asignándoles un rol dentro del sistema.

En la computación en contextos sensibles, los entornos deben estar al servicio de la eficiencia de los procesos, con alta precisión, aumentando la pro actividad de las personas; esto último se logra cuando el sistema hace que sean sencillos los procesos dejando más tiempo libre para que las personas se enfoquen en su crecimiento intelectual; los usuarios deben estar al tanto, entonces, de los parámetros que influyen en el comportamiento del sistema. En otras palabras, para que las aplicaciones alcancen su máximo rendimiento, cumpliendo con las tareas que le son asignadas, acometiendo procesos de alto o bajo nivel, el entorno de un Contexto Sensible debe funcionar bajo la premisa de la sencillez al servicio de la eficiencia. La anterior apreciación es de gran valor para el propósito del presente documento, teniendo en cuenta nuestro enfoque en la computación en contextos sensibles bajo la figura de Smart Campus, concepto que se abordará en apartados posteriores.

### *3.3.5 SMART CITIES*

#### *3.3.5.1 Definición*

Con la llegada del nuevo siglo, distintas organizaciones a nivel mundial empezaron a hacer énfasis en la necesidad de retomar la ruta hacia la sostenibilidad ambiental; el reto consistía en disminuir las emisiones de carbono con el uso de nuevas fuentes de energía renovable, acercar a las habitantes en condiciones de pobreza a los servicios básicos para llevar una vida digna, la generación de fuentes de empleo que estuvieran a tono con la proyección de crecimiento poblacional, la necesidad de implementar nuevas políticas para la distribución equitativa del territorio, brindando oportunidades de acceso a las clases menos favorecidas a una vivienda, el mejoramiento del sistema de transporte y una disposición eficiente de los desechos que se producen diariamente en la ciudad. El crecimiento del uso de las tecnologías para la gestión de la información (TIC's), la aparición de los entornos sensibles y la expansión de los servicios en el Cloud, llevaron a que naciera una nueva perspectiva de la ciudad con el concepto de *Smart City*[51]*.* El objetivo del mismo es propiciar un escenario de intercambio de ideas que propendan por el mejoramiento de la calidad de vida de todos los habitantes del mundo, con estrategias diseñadas para las características individuales de cada una de las ciudades. Los catedráticos de diversas universidades quisieron estudiar los alcances del término, coincidiendo en la noción de *sostenibilidad*. Una ciudad es inteligente si cuenta con un sistema sostenible.

A continuación, algunas definiciones pertinentes:

- Los rudimentos de lo que constituye una *Ciudad Inteligente Sostenible* con los cuales definimos a una ciudad son aquellos que surgen cuando las TIC's están ensambladas con las infraestructuras tradicionales, mientras la ciudad

[51] *Ciudad Inteligente,* por su traducción en español.

es coordinada y está integrada a las nuevas tecnologías digitales (Batty , Et.al, 2012).

- Una *Ciudad Inteligente* es aquella que monitorea e integra las condiciones de todas sus infraestructuras físicas incluyendo caminos, puentes, túneles, vías, vías subterráneas, aeropuertos, comunicaciones, agua, abastecimiento de energía, edificaciones, y puede optimizar mejor sus recursos, planear sus actividades de mantenimiento preventivo y monitorear aspectos concernientes a la seguridad, mientras maximiza el acceso de los servicios a sus ciudadanos (Braverman, Et.al, 2014-2015).

- Una *Ciudad Inteligente* se refiere al centro urbano del futuro que es seguro, ambientalmente verde y eficiente, con infraestructuras avanzadas cuyos sensores, dispositivos electrónicos y redes estimulan el crecimiento de la economía y una alta calidad de vida. (Schaffers, Et.al, 2012)

- Una *Ciudad Inteligente* es una ciudad con un buen desempeño en la proyección de sus seis características: economía, habitantes, gobernabilidad, movilidad, entorno y estilo de vida; construida en la combinación inteligente del legado y las actividades de ciudadanos conscientes, independientes y decididos. (Braverman, Et.al , 2014-2015)

- El concepto de *Ciudad Inteligente* hermana todas las características asociadas con el cambio organizacional, tecnológico, económico y desarrollo social de una ciudad moderna. (González & Rossi, 2001)

- El concepto de Ciudad Inteligente Sostenible es un marco de referencia para una visión específica del desarrollo urbano moderno. Este concepto reconoce la vital importancia de la información y las tecnologías de comunicación como los conductores de la competitividad económica, la sostenibilidad ambiental y

la habitabilidad de la misma. La infraestructura correcta para las TIC afectará la manera en que cada ciudad será creada y evolucionará (Lucent, 2011.).

La urgencia por la sostenibilidad se plantea por las cifras correspondientes al incremento de la migración hacia las ciudades; de acuerdo con el informe publicado en 2008 por United Nations Population Fund[52], 3.3 mil millones de personas vivían en áreas urbanas y se estimaba que para el año 2030 el número aumentaría a 5 mil millones. Y la cifra parece no variar mucho, en la más reciente campaña de la ISO, la ITU y la IEC: (ISO -IEC, 2015), se anunciaba que más del 50% de la población mundial reside en áreas urbanas, proyectando un incremento del 70% para mediados de siglo. El objetivo de esta campaña era generar un escenario para aportar ideas en el desarrollo de estándares que permitan construir ciudades inteligentes donde se pueda hacer gestión inteligente de los recursos para reducir el impacto ambiental; siendo los estándares un lenguaje común para las organizaciones internacionales, la necesidad de tener ciudades más eficientes e interconectadas es mayor.

### *3.3.5.2 Casos de Estudio*

Algunas ciudades operan exitosamente bajo el paradigma de *Smart City*, aprendiendo progresivamente de sus prácticas y de las de sus homólogas. El Foro de Comunidades Inteligentes, *ICF* (2015)[53]*,* anualmente galardona a las veintiuna ciudades que tengan un desempeño de alto nivel en los siguientes cinco factores: *Conectividad de ancho de banda, Conocimiento de la Fuerza Laboral, Inclusión Digital, Innovación, Mercadeo y Promoción*. Luego se seleccionan las mejores siete, siendo escogidas como modelos ejemplarizantes para incentivar al desarrollo urbano sostenible a nivel mundial. El escalafón anual ofrecido por el ICF

[52] Fondo de Población de las Naciones Unidas
[53] Intelligent Community Forum por su sigla en inglés

es una de las mejores alternativas para analizar las decisiones y los procedimientos que adoptaron las ciudades nominadas en su propósito de convertirse en un lugar mejor para vivir.

En el 2015, de las siete ciudades ubicadas en el *Top 7*, cinco están en el continente americano[54], una en Asia[55] y una en Oceanía[56]. Para 2016, Canadá y Taiwán se posicionan como los países líderes en ciudades inteligentes ( Intelligent Community Forum (ICF), 2015). En nuestro continente, parte de ese liderazgo se debe a los esfuerzos conjuntos entre las administraciones locales y organizaciones internacionales como el Banco Interamericano de Desarrollo, con su Iniciativa de Ciudades Emergentes Sostenibles (BID, 2015), con la implementación de la Metodología ICES.

En Colombia, la Financiera del Desarrollo Territorial S.A., FINDETER, actualmente se encuentra liderando el Programa de Ciudades Sostenibles y Competitivas, cuyo principal objetivo es promover en las ciudades una alta calidad de vida a sus habitantes, reduciendo el impacto sobre el medio natural, generando espacios de amplia participación ciudadana, promoviendo el crecimiento económico. Este programa cuenta con el apoyo del BID y funciona en el marco de la ICES desde 2012, utilizando como modelo la metodología implementada en ciudades como Goiâna (Brasil), Trujillo (Perú), Santa Ana (Salvador), Puerto España (Trinidad y Tobago) y Montevideo (Uruguay). El primer paso fue la creación de la Plataforma de Ciudades Sostenibles y Competitivas (CSC), contemplando las siguientes cuatro dimensiones:

- Sostenibilidad Ambiental y Cambio Climático.
- Sostenibilidad Urbana.

[54] Estados Unidos: Arlington County, Virginia; Columbus, Ohio; Mitchell, Dakota. Cánada: Surrey, British Columbia. Brasil: Río de Janeiro.
[55] Taiwan: New Taipei City.
[56] Australia: Ipswich, Queensland.

- Sostenibilidad Fiscal y Gobernabilidad.
- Sostenibilidad Económica y Social.

Acto seguido, se identificaron quince ciudades intermedias de acuerdo al factor poblacional y el acelerado crecimiento demográfico y económico, entra las que se encuentran Bucaramanga, Manizales, Pereira y Pasto.

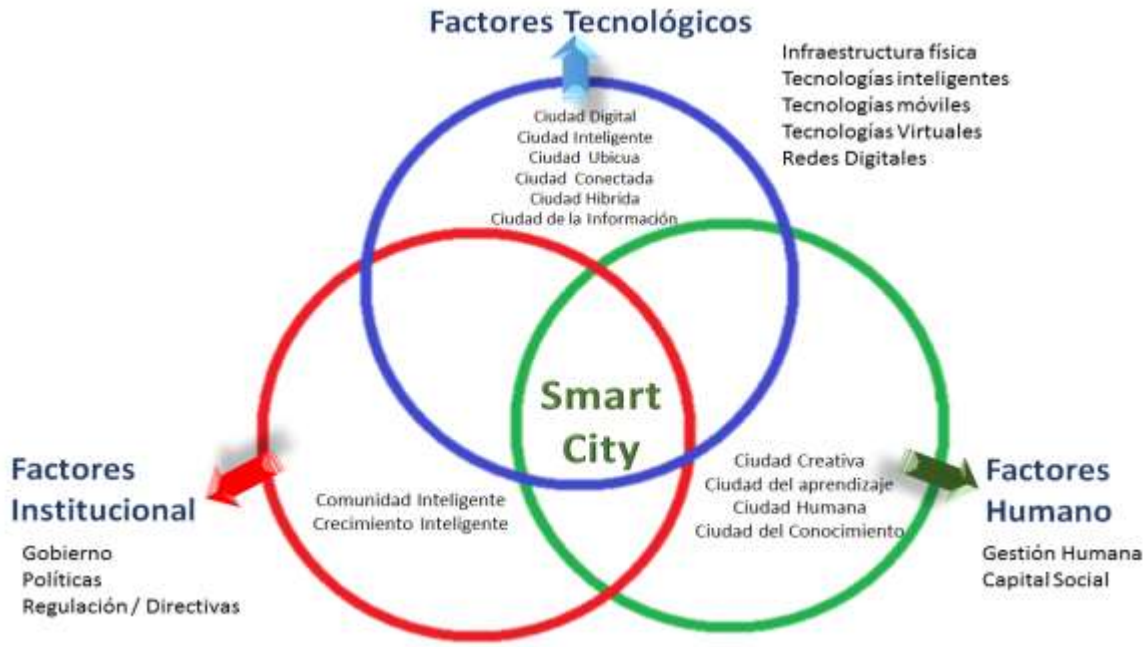
El ejemplo de mayor relevancia entre la innovación en las ciudades de nuestro país es Medellín. En el concurso organizado por el Citigroup y el Departamento de Servicios de Mercadeo del Wall Street Journal, en colaboración con Urban Land Institute ULI, buscaba determinar cuál ciudad era la más innovadora del mundo, basado en su progreso y su potencial, el premio de la que se hizo acreedora *La Ciudad de la Eterna Primavera*, fue gracias a la unión y el trabajo conjunto entre el gobierno local, la empresa privada, las organizaciones comunitarias y las universidades, para dar solución a los problemas de movilidad, sostenibilidad ambiental y la violencia. Entre los programas que destacaron para recibir el galardón está el de *Presupuesto Participativo*, donde los ciudadanos podían definir las prioridades de inversión. En 2013, la ciudad más innovadora del mundo según (Patiño Sedan), comprendió la necesidad de la transformación del sistema educativo, fortaleciendo los centros de investigación en las universidades e introduciendo una política de estímulos a la creatividad y al emprendimiento para los estudiantes de la media básica y secundaria. El cambio en la mentalidad de los futuros residentes del *Valle de Aburrá* va acompañado de la inversión en infraestructura y la construcción de centros de innovación y negocios como el edificio de la corporación *Ruta N* (2012), adscrita a la alcaldía municipal, y que cuenta con laboratorios de ciencia y tecnología, con capacidad para albergar empresas extranjeras.

Si el modelo de progreso Medellín es uno de los ejemplos a nivel mundial, sus avances hacia la consecución del grado de *Smart City* son parciales. A pesar que

las políticas adoptadas llevan a la ciudad por buen camino, aún dista de figurar en el escalafón mundial del ICF.

Nam & Pardo, en su intervención en la conferencia Internacional sobre Investigación de Gobierno Digital, categoriza el núcleo en tres dimensiones o factores de las ciudades inteligentes, como se muestra en la siguiente figura: (2011, pág. 286).

Imagen 4 : Factores fundamentales de una Ciudad Inteligente (Smart City)




Fuente: Tomado de Conceptualizing Smart City with Dimensions of Technology, People, and Institutions, 2011

*3.3.5.3 Infraestructura: Seguridad y Privacidad en Smart Cities*

Las *Smart Cities* son una conjunción perfecta entre tres dimensiones que llevan al desarrollo urbano sostenible: la Dimensión Humana, la Dimensión Institucional y la

Dimensión Tecnológica (NAM, 2011.). Desde 1990, el movimiento de las *Comunidades Inteligentes* empezó a tomar forma, teniendo como fundamento el trabajo cooperativo entre los miembros de la comunidad para transformar las condiciones de habitabilidad haciendo uso de las TIC. Sin embargo, el concepto *Smart City* también cuenta con nociones adyacentes:

- Digital City (Yovanof, 2009): una ciudad digital es una comunidad conectada que combina una infraestructura de comunicaciones de banda ancha; una infraestructura de computación orientada a servicios, flexible, basa en los estándares de la industria abierta, y servicios innovadores para enfrentarse a las necesidades de los gobiernos y sus empleados, ciudadanos y negocios. El objetivo de este tipo de ciudades es crear un entorno sensible para compartir información, permitir la interoperabilidad y trabajo colaborativo, con experiencias de usuario para cualquier habitante de la ciudad.

- Intelligent City (Malek, 2009): es el resultado de una hibridación entre la sociedad del conocimiento y la *Digital City*. Esta tiene toda la infraestructura y la *infoestructura* (Cornella, 1999) de la IT y la última tecnología en comunicaciones. La característica de este tipo de ciudad es que tiene la habilidad de soportar el aprendizaje, el desarrollo tecnológico y los procedimientos de innovación.

- Virtual City (Boulton, 2011): las funciones de la ciudad son implementadas en la nube, consistiendo de una realidad con sus entidades físicas y habitantes reales con sus contrapartes virtuales, de esta manera, lo que se busca es eliminar las distancias entre las actividades que tienen lugar en la ciudad.

- Ubiquitous City (Lepouras, 2007): las *U-city* surgieron como una extensión del concepto de las ciudades digitales, cuyo propósito es hacer la computación ubicua disponible para los elementos urbanos como su

infraestructura, sus construcciones, sus habitantes y sus espacios abiertos. Esta viene siendo, a su vez, una implementación a gran escala de los entornos sensibles permitiendo el acceso a cualquier servicio en cualquier lugar en cualquier momento a través de las aplicaciones de los dispositivos móviles. Mientras una *Virtual City* reproduce los elementos de la ciudad para ser visibilizados en el espacio virtual, la U-city se genera a partir de los sensores insertados en esos elementos urbanos.

- Information City (Sairamesh, 2004): se refiere a los entornos digitales que recogen información de las comunidades para después destacar los indicadores, factores y variables de funcionamiento de la ciudad y sus diversos sectores de desarrollo.

Con el crecimiento poblacional experimentado en la última década, una verdadera *Smart City* debe valerse de la integración efectiva de los anteriores tipos de ciudad. Actualmente, en la era del Big Data, cientos de posibilidades se han abierto para que los usuarios puedan hacer varias tareas en simultánea por medio de sus dispositivos móviles. Si bien la infraestructura se ha robustecido por las tendencias impuestas por las redes sociales y la generación de contenidos, las plataformas para sostener la demanda de infraestructura están empezando a modelarse, gracias a la integración de diversas prácticas de computación ubicua al interior de las empresas, los centros de investigación y las universidades. Anticipando la transformación de los centros urbanos, la ISO recientemente publicó el estándar ISO 37120 en colaboración con la ITU y el IEC. El principal objetivo es el ofrecer un marco de trabajo para la obtención de indicadores que midan el desempeño para mejorar la calidad de vida y la sostenibilidad ambiental (ISO, 2014). En general, los indicadores existentes, a menudo compilados dentro del Big Data, al no estar estandarizados hacen difícil el trabajo comparativo temporal en el progreso de las ciudades.

Cuatro de las ciudades beneficiadas con el ISO 37120, son Melbourne, Minna, Rotterdam y Johannesburgo. La medición de resultados parciales, en las estrategias implementadas para el desarrollo y el crecimiento de los centros urbanos, ha sido positiva. El trabajo está inacabado ya que las dinámicas sociales y económicas varían constantemente, dependiendo de la interacción interna entre sus habitantes, y la interacción externa con las demás ciudades de su país, al igual que su posicionamiento a nivel internacional (Lazarte, 2015). En la actualidad, la organización internacional encargada de certificar a las Smart Cities en la implementación del estándar es el *World Council on City Data* (Cities for Cities, 2014), el cual cuenta con el listado de las ciudades reconocidas internacionalmente que cuentan con su certificado ISO en alguna de sus cinco categorías: Aspirational, Bronze, Silver, Gold, Platinum[57]. En el año 2014, Bogotá recibió la certificación en la categoría Aspirational, obteniendo un puntaje entre 30 y 45, en los indicadores base. De las doce ciudades que cuentan con una certificación *Platinum* seis se encuentran en el continente americano[58], tres son europeas[59] y las tres restantes están en el continente asiático (Bartoli, Et.al, 2011).

El razón por la cual las anteriores ciudades son líderes a nivel mundial se debe a que cuentan con un modelo basado en proveer una estructura para la implementación de servicios para el monitoreo de infraestructuras críticas y para la organización y la gestión de las bases de datos de *Smart City*. Toda arquitectura (Bartoli, Et.al, 2011) cuenta con cuatro unidades principales que cubren casi todas las redes, los procesos, las aplicaciones y un sinnúmero de actividades asociadas en diferentes tendencias:

- ***Unidad de Aplicaciones***: las aplicaciones están relacionadas a valores físicos de monitoreo utilizando tecnologías de vigilancia como la imagen

[57] *Aspirante, Bronce, Plata, Oro, Platino*, por su traducción en español.
[58] México: Guadalajara y León; Estados Unidos: Los Ángeles y Boston; Canadá: Toronto y Vaughan.
[59] España: Barcelona; Holanda: Rotterdam; Inglaterra: Londres.

satelital. Estas tecnologías permiten que operen aquellas que se encuentran relacionadas con los procesos de seguridad de la ciudad, el monitoreo industrial, la construcción de sistemas de gestión de la información y los sistemas de automatización. De igual manera, bajo esta unidad funcionan los circuitos cerrados de televisión (CCTV), la televisión de acceso comunitario (CATV) y los sistemas de información geográfica (GIS).

- ***Unidad de Información***: es de vital importancia para que puedan funcionar las aplicaciones mencionadas anteriormente. La mayoría de las unidades de información se encargan de monitorear el comportamiento de los habitantes, los estudios de factibilidad, la demanda de mercados, las actividades comerciales y la circulación de nueva información referente a los mercados emergentes.

- ***Unidad de Gestión***: la gestión de procesos es de gran importancia debido a que define la relación, las reglas, las estrategias y las políticas entre las aplicaciones y la unidad de información. La seguridad y la privacidad reciben especial atención en esta unidad ya que el beneficio de una ciudad interconectada está en la garantía de la protección del Big Data y el PII, con la integración eficiente de los distintos ISMS presentes en la ciudad.

- ***Unidad de Protocolo de Integración de Comunicaciones***: está encargada de conectar los tres principios anteriores, utilizando redes convencionales de cableado o usando cables de fibra óptica para los sistemas que dependen de conectividad física. Si bien las tecnologías inalámbricas, Bluetooth, Wi-Fi y GSM son una solución más práctica y factible para una Smart City, es importante destacar que si la seguridad de las redes se convierte como una mera alternativa, dependiendo si son públicas o privadas, los procesos ejecutados por las unidades anteriores se verán entorpecidos. Un ISMS

robusto sumado al rigor de las políticas de privacidad harán de los centros urbanos, el escenario de la transformación social.

De forma que los sistemas de control sean más sofisticados, las Smart Cities requerirán un alto grado de conectividad en sus redes. La proporción es directa con la vulnerabilidad, por esta razón, uno de los retos más grandes que enfrentan las ciudades del futuro es la seguridad. Cuando se habla de protección en la red, no se refiere únicamente a atender ataques aislados únicamente, también están aquellos que provengan de empleados inconformes, espionaje industrial, ciberterrorismo, errores inadvertidos en el uso que hagan los usuarios de sus dispositivos, fallas en el funcionamiento de los dispositivos y desastres naturales (Bartoli, Et.al, 2011). Las vulnerabilidades en la red pueden permitir que el sistema sea desestabilizado, en algunas ocasiones, de forma impredecible. En cuanto a la privacidad, todo servicio tiene opciones de configuración, dependiendo de las preferencias o expectativas del usuario, ya sea que reciban una caracterización como ciudadano, comunidad o área urbana. No obstante, cuando se hace una completa caracterización de las preferencias y el comportamiento de los habitantes de una ciudad pueden ser considerados como una amenaza. El consentimiento puede ser relativo pero para conseguir que la aprobación sea total, debe haber una integración eficiente entre los ISMS y las PET, poniendo al usuario al tanto de las políticas y procedimientos a los que está sujeta su información cuando hace parte del entorno sensible de una Smart City.

### *3.3.6 SMART CAMPUS*

#### *3.3.6.1 Definición*

La incursión de los entornos sensibles en el sector educativo es uno de los puntos cruciales para el desarrollo de las TIC y crecimiento en la oferta de servicios en el *Cloud*. El desarrollo de un *Smart Campus* en los espacios académicos está

involucrado con el desarrollo de las Smart Cities y su origen está en la necesidad de integrar el progreso económico a las dinámicas sociales para tener una mejor percepción de la sostenibilidad. Existen varias aproximaciones al término de *Smart Campus*, entre las que se destacan:

- Un Smart Campus corresponde a una forma de pensamiento y no un producto, con claros beneficios en la interacción y la experiencia del estudiante, mejores resultados en el proceso de aprendizaje, y mayor proximidad a las habilidades de la economía digital, permitiendo el desarrollo de estrategias para la eficiencia operativa del espacio físico, y la creación de alianzas con la industria (Pandey, 2015).

- Son tres las funciones que debe cumplir un Smart Campus: debe haber *una comunidad creadora de servicios* para satisfacer sus necesidades académicas; debe *funcionar como un laboratorio* para experimentar e innovar en soluciones para las TIC; y debe ser una *plataforma socio-técnica* para la creación y entrega de servicios en el campus (De Angeli, 2013).

- Son entornos sensibles encargados de la creación de servicios *con* y *para* los estudiantes, basados en el concepto de *Smart Community,* dónde los esfuerzos para usar las IT son conscientes, para transformar la vida y el trabajo en un espacio específico de forma cualitativa, más allá de ser netamente cuantitativa (Pistore, 2015).

Las anteriores definiciones nos acercan a los modelos de ciudades inteligentes, estudiados en el apartado anterior. Al hacer una comparación con el mundo natural, los Smart Campus funcionarían como pequeñas células de un sistema más complejo, las Smart Cities, siendo de igual manera, sistemas en sí mismos. En otras palabras, el concepto de Smart Campus apunta a ser una ciudad, con

una población definida, con comodidades y activos que son formados por su valor, sus expectativas y las transformaciones requeridas por sus *ciudadanos* (BHERT, 2015).

Imagen 5 : Modelo de Smart Campus;


Se debe aprovechar la innovación del Internet de las cosas (IoT) para construir el campus inteligente y sostenible Fuente: (Round Table Business/Higher Education, 2015)

### *3.3.6.2 Casos de Estudio*

Las universidades se están haciendo más fuertes con la entrada del IoT, diseñando nuevas estrategias para desarrollar al máximo su capacidad de innovación en áreas como la salud, el transporte, la economía, la agricultura y los recursos de la educación. El paradigma de *todo y todos conectados* (BHERT, 2015), ha ampliado la percepción de la capacidad digital de la educación. Que exista una apertura en los espacios físicos para la interconexión hacen del recurso virtual la materia prima para resignificar la información procesada en dichos espacios. Para que haya, entonces, un verdadero crecimiento debe haber el

sentido cooperativo entre el desarrollo de las *Smart Cities* con los *Smart Campus*, por ejemplo: mientras las universidades inteligentes atraigan los mejores investigadores y puedan contar con un estudiantado selecto, las ciudades inteligentes atraerán mayor inversión, generando nuevas formas de empleo, consolidando su infraestructura, con aplicaciones para el desempeño eficiente de las actividades que día a día tienen lugar en la vida de sus habitantes. No obstante, una contradicción salta a la vista con el interrogante: ¿si una ciudad es más productiva, es una ciudad más humana?

Revisemos algunos casos. En Trento, Italia, el potencial de convertirse en un laboratorio de Comunidad Inteligente fue valorado en los ciudadanos y empresas comprometidas con la ciudad para identificar y solucionar los problemas, para lo cual, la universidad abre sus sistemas, sin vulnerar la seguridad y la privacidad de los datos, para acelerar la innovación, haciendo disponibles una nueva generación de servicios disponibles para la ciudad. Los requerimientos planteados para lograr este objetivo establecieron la necesidad de invertir en la educación de acuerdo con la visión de *Educar la Ciudad* (Pistore, 2015), iniciando desde la secundaria, con mayor impacto en la vida universitaria. Es entonces desde la universidad que se pueden tejer las estrategias académicas con el progreso de la ciudad.

India es uno de los países de más habitantes (United Nations, 2014), con una fuerte tendencia al crecimiento en su densidad poblacional, cuenta con el 32% de su población ubicada en centros urbanos. Se estima que para mediados de siglo las ciudades albergarán alrededor de 843 millones de personas (Maidan, 2015). La estrategia planteada para superar las exigencias del futuro es la construcción de cien nuevas ciudades inteligentes en la periferia de las ciudades de mayor población, funcionando como pueblos satélites con un comportamiento inteligente en el uso de los recursos naturales, sistema de transporte, gobierno e infraestructura para las TIC. En la actualidad, las universidades de Bangalore y Delhi figuran entre las doscientas mejores universidades del mundo, de acuerdo

con el ranking mundial de Quacquarelli Symonds, junto con otras catorce universidades e institutos que se encuentran entre las mejores universidades del escalafón, ubicadas en las ciudades de mayor población. La misión de estas universidades ha sido contribuir a la investigación de ciudades inteligentes implementando en sus campus las políticas e infraestructura para sostener un sistema de redes abiertas para la innovación en el desarrollo de programas para mitigar las problemáticas de sus ciudades.

Un *Smart Campus* debe facilitar la integración de los datos y su modelo no dista del utilizado en una *Smart City*; para llegar a ser un sistema eficiente debe cumplir con cuatro fases propuestas (Pandey, 2015): en la primera se debe integrar la industria con la academia, definiendo las condiciones de seguridad de las redes y las políticas de privacidad en la gestión de la PII, haciendo uso correcto de las PET; a continuación debe enfocarse en el fortalecimiento de los protocolos de movilidad y de interconexión en las aulas de clase, eliminando las barreras del espacio físico para hacer aprovechar los recursos intelectuales de su comunidad educativa. La tercera fase consiste en la adopción de *Cloud* para expandir su presencia y su incidencia en los procesos de transformación de sus alrededores, así como su vinculación a proyectos internacionales, diseñando un Sistema de Gestión de Aprendizaje, *LMS* (Know, 2015), que permita tener una descripción clara de los resultados obtenidos en el modelo de competitividad implementado para alcanzar la excelencia académica. Finalmente, la cuarta fase corresponde al robustecimiento de las capacidades operativas del Smart Campus y las técnicas de seguridad, siguiendo los estándares internacionales de calidad propuestos por la ISO, la ITU y la IEC. Un *Smart Campus* que progrese en las cuatro fases descritas puede tener gran influencia en los procesos de transformación y desempeño de una ciudad, en su camino a hacer un uso más eficiente de sus recursos, en sus tres dimensiones de desarrollo, bajo el imperativo de las *Smart Cities* que necesita el mundo para evitar el próximo colapso generacional.

El recurso intelectual está al servicio de su comunidad, con la implementación de un *Smart Campus,* dicho recurso puede ser orientado efectivamente para suplir las necesidades y requerimientos presentes en su comunidad.

## 3.4 BRING YOUR OWN DEVICE (BYOD).

### *3.4.1 Definición*

El programa BYOD, *Bring Your Own Device*[60], consiste en involucrar a los empleados utilizando sus propios dispositivos móviles de comunicación para llevar a cabo sus labores incluso con asistencia remota a su área de trabajo (Cavoukian, 2013). La implementación del BYOD en los compañías tiene como único propósito mejorar la productividad de sus empleados, de tal forma que puedan ejecutar de forma eficiente sus obligaciones; debido a la flexibilidad que el programa trae consigo, la fuerza de trabajo tiende a incrementarse ya que la mera posibilidad de tener disponible los datos de relevancia para ejecutar procesos, permite que el recurso humano pueda tener más tiempo para actividades de gran beneficio para la compañía, como la investigación y el desarrollo de nuevas estrategias comerciales y logísticas para el crecimiento de la empresa.

Para que el programa tenga un buen funcionamiento es necesario que la compañía cuente con un buen servicio de almacenamiento en la nube así como un ISMS robusto, con políticas precisas de privacidad sobre la PII, el Raw Data y los procesos de gestión de la información, de tal forma que soporten y cumplan con las medidas y las leyes impuestas para garantizar la privacidad de los Titulares de la información, al igual que la empresa.

[60] Por su traducción en español, *Trae Tu Propio Dispositivo.*

Si bien las plataformas de gestión de datos y la capacidad de almacenamiento han aumentado, la portabilidad de los datos es más factible, los estándares para la producción de dispositivos móviles de calidad son más rigurosos (ISO, 2005), la accesibilidad de los datos está sometida a mayores controles, y las PET han recibido el aval de las grandes organizaciones reguladoras de las telecomunicaciones (ITU-T, 2012); el programa BYOD aún sigue generando más dudas que expectativas, en especial en los asuntos concernientes a la seguridad y la privacidad de la información, esta última, objeto de estudio en el presente documento.

### *3.4.2 BYOD: Desarrollo y Aplicaciones*

La tendencia del programa BYOD comenzó en el año 2009, bajo la tutela de Integrated Electronics Corporation, Intel Corporation (2013), cuando sus empleados empezaron a usar sus teléfonos inteligentes, tabletas y dispositivos de almacenamiento portable en su trabajo. El principal propósito de acoger esta nueva práctica fue debido a la necesidad imperante de recortar costos operativos y mejorar la productividad. Un año más tarde, la cantidad de empleados haciendo uso de sus dispositivos para cumplir con sus obligaciones laborales se había triplicado. Indudablemente, las preocupaciones por la seguridad no se hicieron esperar y desde la oficina de CISO[61] se decidió hacer de esta nueva tendencia, un caso de estudio y un modelo a seguir, repensando la infraestructura de su ISMS interno, resultado que finalmente obtuvieron cuando otros gigantes de las redes y de la producción de dispositivos móviles, como CISCO, Google y Blackberry, se convirtieron en promotores del programa.

A pesar que el movimiento empezó a cobrar más presencia y aceptación por parte de los empleados de otras compañías, algunas de ellas prefirieron bloquear los servicios de correo electrónico y conexión a la red local en los dispositivos

[61] *Chief Information Security Officer*: Oficial Jefe de Seguridad de la Información

personales de sus empleados. Solo hasta la aparición del iOS 4[62], con una nueva interfaz para la programación de aplicaciones[63], y con el desarrollo de software de gestión de dispositivos móviles[64], la aprobación del programa empezó a traer nuevos y mejores resultados en la productividad de los empleados. Ahora el objetivo consistía en hacer proporcional ese crecimiento con el del ROI[65] de las empresas. El 2011 fue el año crucial del programa cuando, solo en Estados Unidos, el 75% de las empresas habían incluido una política para hacer uso del BYOD (Laird, 2014); en países como en Brasil, Rusia, India, Emiratos Árabes Unidos y Malasia, considerados *Mercados de Alto Crecimiento*, eran igual de propensos a trabajar con BYOD, además de contar con la aceptación de los empleados por permitírseles trabajar con sus propios dispositivos, considerando que esto les daba la posibilidad de estar conectados constantemente y hacer un mejor trabajo. Ese era el segundo reto que debía enfrentar la tendencia: convertirse en una verdadera oportunidad de negocio. Para cumplir con este aspecto, la proyección se cimentó en tres fenómenos comerciales y tecnológicos que estaban sucediendo en paralelo:

- El crecimiento en la producción de nuevos dispositivos móviles e incursión de nuevas marcas.

- La evolución de las capacidades en los dispositivos móviles.

- La evolución de la computación en la nube y las tecnologías de virtualización (Cavoukian, 2013).

Sin embargo, el 2012 significó el replanteamiento del programa. Aparecieron las primeras preocupaciones respecto a la seguridad de los datos que se procesaban y la información que se manipulaba por los empleados, y que estuvieran sujetos a

[62] Sistema Operativo Móvil de los dispositivos de Apple Inc.
[63] *Application Programming Interface*, API, por sus siglas en inglés.
[64] *Mobile Device Management*, MDM, por sus siglas en inglés.
[65] *Return on Investment,* ROI, Retorno de la Inversión, por sus siglas en inglés.

la portabilidad de sus dispositivos móviles. Los riesgos subyacentes consistían en que si cada rol de usuario se hacía cargo de cierto tipo de datos en un dispositivo externo a la empresa, sería mucho más difícil de rastrear la gestión que se estuviera haciendo de los mismos, dificultando el control sobre los dispositivos. Por lo tanto, el CISO[66] de cualquier compañía tenía que considerar la proporción entre las cantidades de dispositivos activos, roles de usuario, la capacidad de la red local y, por supuesto, los datos (ico., 2015) y sus interrelaciones, bajo las siguientes premisas:

- Qué tipo de dato es retenido.
- Dónde son almacenados los datos.
- Cómo son transferidos los datos.
- Cuál es el potencial de tener fuga de datos.
- Confusión entre el dato de uso personal y uso empresarial.
- Capacidades de seguridad del dispositivo asociado a la red.
- Qué hacer con el dispositivo cuando el empleado abandona la empresa.
- Cómo tratar la pérdida, robo, falla o soporte técnico del dispositivo asociado a la red.

Basados en lo anterior, las empresas optaron por enfocarse en establecer y comunicar las políticas de seguridad y privacidad de los datos, trabajando bajo la premisa de ser conscientes de las implicaciones que traía hacer vulnerable a la empresa por una mala gestión de los datos. Gracias a la demanda, los MDM se convirtieron en la alternativa para solucionar las preocupaciones en cuanto a la seguridad y la privacidad de los datos, como MobileIron[67], AirWatch[68], InfoSphere de IBM[69], y FiberLink MaaS360[70].

[66] Chief Information Security Officer: Oficial Jefe de Seguridad de la Información
[67] https://www.mobileiron.com/en
[68] http://www.air-watch.com/solutions/mobile-device-management/
[69] http://www-01.ibm.com/software/data/infosphere/
[70] http://www.maas360.com/

El siguiente año fue el periodo del desarrollo de las Aplicaciones para BYOD, siendo este el punto de giro en la percepción del programa. Asegurar un dispositivo no era la solución precisa para acometer los riesgos mencionados anteriormente; las violaciones de las bases de datos iban en aumento mientras que los costos de operación, que se esperaba serían menores al adoptar el programa, se triplicaron (Cio, 2012). Estos últimos fueron previsibles en un principio, pero permanecieron ocultos, esperando a ser redescubiertos; entre estos se encontraban los gastos por gestión del procesamiento de los datos, gestión de los reportes de procesamiento, soporte técnico de los dispositivos y el servicio de asistencia técnica (Cio, 2014).

Para acometer la dificultad de separar los datos de la compañía y los datos del empleado, se utilizó la tecnología denominada *Containerization*[71], creando una clara división entre los dos tipos de datos, con ventajas y desventajas. Si CISO[72] y el departamento de administración de seguridad de datos desean establecer controles en los dispositivos para lograr esta separación entre los tipos de información, es posible reforzar la seguridad utilizando métodos de autenticación, encriptación, restricciones de *cut-and-paste*[73], entre otros; aun así, tener *Containers*[74] para separar la información no implica que el dispositivo esté completamente protegido (NetworkWorld, 2013). A pesar de lo anterior, otra contribución significativa a las problemáticas mencionadas anteriormente fue la expansión de los software tipo MDM a MAM[75]; con la explosión de las aplicaciones en 2013, los software de gestión de datos evolucionaron para ofrecer mayor seguridad a las aplicaciones que los procesaban, encriptando solo los datos correspondientes a las tareas que estas realizaban, separando su funcionamiento

[71] Separación en Contenedores, por su traducción en español.
[72] Chief Information Security Officer: Oficial Jefe de Seguridad de la Información
[73] *Cortar y Pegar,* por su traducción en español.
[74] *Contenedores,* por su traducción en español.
[75] *Mobile Device Management- Mobile Application Management.* Gestión de Aplicaciones Móviles, por su traducción en español.

de las otras actividades que ejecutara el empleado en su dispositivo y que no tuvieran relación con sus obligaciones laborales (Madden, Brian, 2012).

En su quinto aniversario de existencia, el programa BYOD enfrentó la etapa en la que debía ser sometido a nuevas transformaciones o abdicar al trono de las TIC a nivel empresarial, con la llegada del relevo generacional por una nueva tecnología. El primer paso en su nuevo camino fue la transformación de los software tipo MAM a EMM[76]; las empresas encargadas de la gestión de los datos desarrollaron una suite que consiste en una política de gestión y herramientas de configuración para las aplicaciones y el contenido previsto. Sus funciones básicas según Gartner son (2014):

- Inventariar el Hardware
- Inventariar las Aplicaciones
- Gestionar la Configuración del Sistema Operativo
- La Ejecución, Actualización y Desinstalación de las aplicaciones móviles.
- La Gestión de Política de Ejecución y Configuración de las aplicaciones móviles.
- La vista y el control remoto para Resolución de Problemas[77].
- La ejecución de acciones remotas, como vigilancia y cateo.
- La gestión de Contenido Móvil.

Las suites líderes, de acuerdo con el cuadrante propuesto por Gartner, en habilidad de ejecución y completitud de visión son AirWatch, MobileIron, IBM, Good Technology[78], y Citrix[79].

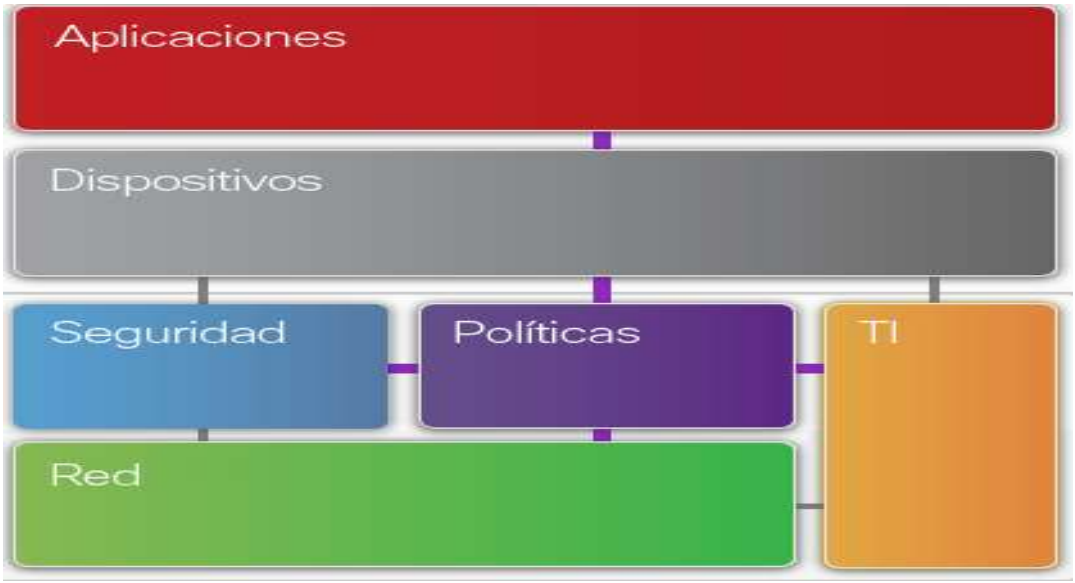
[76] *Enterprise Mobility Management*, Gestión de Movilidad de Empresa, por su traducción en español.
[77] *Troubleshooting (solución de problemas)*, por su definición en inglés.
[78] https://www1.good.com/secure-mobility-solution/enterprise-mobility-management.html
[79] https://www.citrix.com/solutions/enterprise-mobility/overview.html

Con el propósito de mejorar el rendimiento del programa, una vez implementado, y con el advenimiento de nuevas tecnologías, como el IoT[80], han intentado mutar el BYOD en versiones similares como CYOD, *Choose Your Own Device*[81]; BYOT, *Bring Your Own Thing*[82]; BYOA, *Bring Your Own Application*[83]; y la reciente BYOx, *Bring Your Own Everything*[84]. Debido al número de dispositivos disponibles en las compañías y a las solicitudes de Servicio de Asistencia, *Helpdesk*, de los usuarios, los negocios han optado por adaptar el programa a sus necesidades (BCS, 2014).

En todos los casos, la seguridad es el tema de mayor preocupación y a su vez el de mayores avances, a través de servicios unificados que incluyan políticas y estrategias para mantener la privacidad y la confidencialidad de los datos, la protección de la propiedad intelectual de la información cuando se usa un dispositivo que no es de propiedad de la empresa, la adquisición de licencias de funcionamiento, tanto de las aplicaciones como de los dispositivos. Se recomienda que cualquier empresa, al momento de implementar el programa original o alguna de sus versiones mencionadas anteriormente, siga el método I4: *Investigación, Iniciación, Implementación, Integración*; en la primera etapa se deben establecer los parámetros de funcionamiento, la capacidad de operación y los objetivos a alcanzar al trabajar con el programa. En la siguiente etapa se crea el plan de implementación, se definen las políticas esenciales y se desarrolla la estrategia de trabajo colaborativo. Al momento de implementarlo, se debe adquirir la tecnología, el software y la infraestructura de soporte y servicio ideal; e identificar la capacidad de crecimiento y desarrollo del recurso humano al momento de trabajar bajo el programa. Finalmente, en la integración se debe hacer una revisión constante del impacto del programa, en niveles de seguridad, privacidad, eficiencia y productividad.

[80] *Internet of Things*, Internet de las Cosas, por su traducción en español.
[81] Escoge Tu Propio Dispositivo, por su traducción en español.
[82] Trae Tu Propia Cosa, por su traducción en español.
[83] Trae Tu Propia Aplicación, por su traducción en español.
[84] Trae Tu Propio Todo, por su traducción en español.

Imagen 6 : Marco de acceso unificado BYOD Smart Solution,




Fuente: www.cisco.com

El Modelo de la plataforma de red inteligente para la implementación del BYOD en las empresas, es el desarrollado por Cisco Systems Inc. La solución plantea el acceso unificado en la configuración base de la red, la seguridad, las políticas y las Tecnologías de la información, lo anterior permite que las empresas ganen flexibilidad y control de la red.

En la actualidad, BYOD se ha beneficiado de las innovaciones en los EMM y de las dinámicas del mercado laboral. La demanda de espacio para operar en la nube por parte del sector empresa ha crecido a nivel mundial al igual que la contratación temporal, haciendo de la figura de prestación de servicios el recurso para abaratar los costos de operación y funcionamiento (TechRepublic, 2015). Además, la hibridación del programa con sus versiones ha permitido que la flexibilidad en el modelo haga más atractiva su implementación. Si en un principio la preocupación por la seguridad y la privacidad de los datos parecía ser solo de las empresas, en la actualidad son los empleados los que están invirtiendo la balanza a su favor

gracias a un factor que pasó desapercibido en el primer lustro de la existencia del BYOD: la *visibilidad* de los datos. Aunque los empleados estén dispuestos a participar, no desean que sus datos estén expuestos a los CISO[85] por robusto que sea el ISMS; las políticas no deben estar orientadas a reducir los costos operativos sino el mejoramiento de la productividad de los empleados, garantizando que sus datos personales se encuentran igual de protegidos como los datos de la empresa y en retorno, los empleados deben asegurarse de hacer un uso correcto de sus dispositivos cuando no se encuentran en su lugar de trabajo, respondiendo a la necesidad de trabajar bajo los estándares de seguridad y privacidad requeridos en la empresa, al final, su rendimiento individual depende de cuán responsable sea el uso que le dé a su propio dispositivo.

Toda empresa que desee liderar en su sector, sea educativo, de salud o comercial, debe estar a la vanguardia en la percepción de las TIC como un beneficio para su crecimiento. BYOD es un programa que ha trascendido los límites del desarrollo tecnológico llegando a la esencia del trabajo colaborativo, renovando el esquema espacial del sector laboral. Si se desea ser parte de esta nueva forma de hacer empresa, es necesario que se inicie con una política de seguridad y privacidad robusta, compatible con los estándares internacionales y la ley nacional, y diseñar su estrategia de gestión de movilidad de la empresa desde allí, auditando su progreso y evolución, siempre manteniendo un canal de comunicación efectivo con los empleados para asegurarse de los beneficios que se desean obtener.

[85] *Chief Information Security Officer*: Oficial Jefe de Seguridad de la Información

**Lista para evaluar la disposición y la capacidad del programa BYOD**

**Respetuoso de la intimidad**

Tabla 2 **:** Readiness/Capability Checklist

| #. | Control | Descripción |
|---|---|---|
| 1 | Política de uso aceptable | Definición qué es admisible en el dispositivo personal, una vez se permite el acceso a los datos de la organización. |
| 2 | Política de Privacidad | La empresa dispone del uso de los dispositivos móviles y el comportamiento que se espera de los empleados, que actúan en nombre de la organización. |
| 3 | Declaración del lugar de uso | Descripción del lugar dónde se necesiten utilizar los dispositivos |
| 4 | Decisión sobre el modelo operativo para el MDM – interno o subcontratado | Definición de los perfiles y permisos de usuario para acceder al dato corporativo o al dato personal. |
| 5 | Acuerdo sobre uso de la cámara de los dispositivos móviles | Declaración de dónde y cuándo es permitido el uso de la cámara, esto se puede reforzar técnicamente mediante el MDM. |
| 6 | Clasificación de datos y su extensión a dispositivos móviles | Declaración de la sensibilidad de los datos de la organización permitidos en los dispositivos móviles. Todo Dato restringido no debe llegar a ningún dispositivo. |
| 7 | Consideración de las aplicaciones de Android, Linux, Samsung Knox, Cisco AnyConnect, etc. | Los recientes anuncios de seguridad de los OS de los dispositivos móviles, necesitan ser testeados por medio de pruebas piloto. Los test que resultan exitosos proveen una fuerte separación del dato personal y el dato corporativo. |

Fuente: Cavoukian,2013

### *3.4.3 BYOD en Colombia*

Desde la creación del Ministerio de Tecnologías de la Información y las Comunicaciones[86], MINTIC, nuestro país empieza a dar un vuelco necesario para

[86] Página official del Ministerio de Comunicaciones MINTIC: http://www.mintic.gov.co/portal/604/w3-propertyvalue-6077.html

la adopción de nuevas estrategias que permitieran el crecimiento del sector y su impacto en las demás esferas de la economía de la nación. Casualmente, el mismo año sale al mercado el programa BYOD, despertando el furor en las grandes empresas para aprovechar al máximo las grandes oportunidades de negocio al migrar a la nube. La primera de las medidas implementadas fue la valoración y renovación de la infraestructura del sistema de telecomunicaciones de tal forma que en eventos posteriores, los proveedores de servicios en el *cloud* pudieran garantizar la calidad del mismo. Solo hasta después del informe de la IBM, en 2012 (IBM, 2012), las empresas en Colombia empezaron a tener sus primeros acercamientos con la *tendencia* de las grandes compañías de Estados Unidos. El principal asesor y proveedor del programa BYOD en Colombia es Cisco Systems Inc., quienes desde 2001 (Value), se han encargado de posicionar sus productos, no solo por sus capacidades técnicas sino también desde el nivel educativo, con la entrada de su Academia de Redes Cisco[87], la cual se encuentra actualmente activa. En el año 2013, mientras los principales diarios publicaban notas relacionadas con las amenazas que podía representar para las compañías la adopción del modelo de empresa propuesto por BYOD, amenazas y riesgos similares a los mencionados en el apartado anterior, desinformando sobre el verdadero alcance del programa bajo la ley colombiana. Ya para ese año, la consultora Gartner anunciaba que para el 2016 el 38% de las empresas dejaría de proporcionar dispositivos móviles a sus empleados (Universia Colombia, 2013); según la firma, basados en una encuesta aplicada a los CISO[88] de empresas en el mundo, para el 2017 la mitad de los profesionales deberá hacer uso de sus dispositivos móviles para trabajar, afianzando la adopción del modelo, no obstante la prudencia al momento de implementarlo ya que en la misma encuesta, tan solo el 22% de los encuestados afirmaba que estaban dispuestos a destinar recursos para ponerlo en marcha en sus empresas.

[87] Cisco Networking Academy
[88] *Chief Information Security Officer*: Oficial Jefe de Seguridad de la Información

Instituciones internacionales como PMI[89] Capítulo Bogotá, han estado atentos a la incursión de la BYOD en las empresas colombianas, denominándola como una estrategia comercial, afirmando que las multinacionales que venden soluciones para la gestión de la información, alientan a sus clientes a comprar sus productos para convertirlos en *Empresas de Clase Mundial*, teniendo graves repercusiones en su presupuesto y a largo plazo, con la compra de más productos que permitan un funcionamiento eficiente del programa (PMI, 2014). A este tipo de estrategia, al que hacen alusión, la llaman *Cantos de Sirena*.

Al parecer, la anterior no es la percepción definitiva del BYOD en nuestro país. Desde su aparición, varias empresas han conseguido avances considerables en la implementación del programa, gracias al aumento del uso de plataformas móviles, la incursión del Teletrabajo en el sector oficial y privado ( Corporación Colombia Digital , 2015) y la adopción de medidas para migrar transitoriamente a la nube como la disponibilidad del servicio Microsoft Exchange en cualquier dispositivo móvil relacionado al empleado, el registro de las aplicaciones descargas en los software tipo MDM y MAM adquirido por la empresa, como los ofrecidos por Citrix Systems (Citrix , 2015). De igual manera, las compañías están empezando a ver en la *Movilidad Empresarial* una alternativa eficiente para mejorar la productividad de sus empleados y transformar la relevancia del Departamento encargado de la gestión de la Información, pasando de estar enfocado la mayor parte del tiempo en el Servicio de Asistencia y Soporte Técnico, a abrir su intervención en los procesos de eficiencia de la empresa facultando a sus empleados a contar con aplicaciones y soluciones que extiendan su acceso a los servicios de datos, voz y mensajería, contando con un servicio seguro en entornos sensibles, en redes públicas o privadas. A pesar de la prudencia enunciada, el porcentaje ha ido creciendo paulatinamente, siendo las empresas de tecnologías de la información y telecomunicaciones con presencia en nuestro país, las primeras en implementarlo contando con el respaldo del MinTic (Ruiz, 2013).

[89] http://www.pmi.org/

En el sector educativo en nuestro país, la experiencia de mayor relevancia de uso del BYOD, es la Universidad Pedagógica y Tecnológica de Colombia. El informe resuelve que las características del ancho de banda, la cantidad de estudiantes con dispositivos móviles y el acceso que ellos hacen a servicios de la universidad por medio de la red inalámbrica, como la Biblioteca Digital, requerían la reestructuración de la arquitectura de la red, diferenciando los tres segmentos a mayor actividad en el campus universitario: administrativo, académico e invitado. El principal enfoque del uso del programa BYOD está orientado exclusivamente para los servicios académicos que el estudiante puede aprovechar siempre y cuando se encuentre en el campus universitario. Aunque no hay un referente directo a las aplicaciones que haya desarrollado la universidad para implementar el programa, el sistema de gestión de calidad interno SIGMA funciona a la par con el Sistema Integrado de Gestión SIG, que involucra las normas nacionales e internacionales de gestión de calidad (Rodriguez H., et al. 2015). A partir de lo anterior, la UPTC trabaja en la definición de sus protocolos para la gestión de los dispositivos móviles que pueden funcionar en la implementación del BYOD.

Traiga su propio dispositivo (BYOD), es una estrategia alternativa que permite a los empleados y socios comerciales, utilizar su dispositivo móvil personal para ejecutar aplicaciones empresariales y datos de acceso. Típicamente, se extiende por los teléfonos inteligentes y las tabletas, pero la estrategia también se puede usar para PCs; estudios muestran que casi un 62% de los empleados utilizan regularmente su dispositivo móvil en actividades de su trabajo (Gartner, 2015). Estudios realizados por Gartner, Inc. (NYSE: TI), empresa dedicada a la investigación y el asesoramiento principal en compañía de tecnología de la información del mundo, Gartner destaca que para la aplicación del BYOD, normalmente se necesitan Tecnologías de apoyo de la red, que permitan una protección significativa como: la autenticación, control de acceso a la red (NAC), Protección en administración de dispositivos móviles (MDM) y de gestión de aplicaciones móviles, el cifrado de contenidos y los mecanismos de entrega

(tiendas de aplicaciones, sistema de intercambio de archivos y la virtualización de escritorio), entornos multi-plataformas, desarrollo de aplicaciones móviles y creación de políticas de seguridad (Willis, 2012).

# 4 PROCESO INVESTIGATIVO

## 4.1 ASPECTOS METODOLÓGICOS

Para el desarrollo de este proyecto se optó por utilizar los métodos de la investigación exploratoria y la investigación aplicada que permitieran cumplir con los objetivos propuestos y respondiera a la hipótesis planteada, que mediante la aplicación de las técnicas de privacidad, resultado del estudio, y con las políticas de seguridad en la red, se lograra desarrollar una prueba de aplicación de los estándares propuestos.

El proceso de Investigación se desarrolló en tres (3) fases, que se ilustran a continuación:

Imagen 7 : Fases metodológicas del proceso de Investigación;


Fuente: Autora del proyecto

Se hizo una exploración en los repositorios y bases de datos científicas como IEEE, ProQuest, EBSCOhost, E-Libro, ACM - Association for Computing

Machinery, además Google Scholar, una muestra de referencias con tipos de documentos se presenta en la tabla del apéndice denominada: Tabla tipo de documentos referenciados, inicialmente se estaban seleccionando referencias desde 2005 a la fecha, pero por las referencias que se encontraban de historia la brecha tocó admitir abrirla y se va a encontrar referencias desde 1890, dado que son decretos, normas o políticas que han ocurrido en una fecha determinada.

### *4.1.1 FASE 1: Exploratoria*

El proceso investigativo comenzó con una fase exploratoria que abarca la consulta de fuentes bibliográficas en las bases de datos Científicas con el fin de revisar las diferentes técnicas y mecanismos que existen para controlar la privacidad en ambientes inteligentes, y realizar un estudio diagnóstico de las mismas, analizar e identificar las palabras claves; de igual manera, se incluye la construcción del marco teórico de la propuesta con el fin de describir las técnicas, mecanismos y políticas de privacidad y seguridad en ambientes sensibles, además de las técnicas que se pueden aplicar con el BYOD, de manera que se dé cumplimiento al objetivo uno (1) y dos (2).

### *4.1.2 FASE 2: Análisis y Diseño*

La segunda fase se enfoca en el desarrollo del estudio diagnóstico de técnicas y mecanismos de privacidad y seguridad, cuáles serían aplicables en el BYOD, se analizan las técnicas y como seria implementar dichas técnicas en el Smart Campus, si su aplicación ya se encuentra en el mercado y qué tan eficiente ha sido. En el caso de no existir, se procede a proponer un esquema de técnicas de privacidad, de manera que se da cumplimiento al objetivo específico tres (3).

### *4.1.3 FASE 3: Aplicación y Análisis de Resultados*

La tercera y última fase permitió comprobar y evaluar la aplicación de las técnicas de privacidad en ambientes sensibles al contexto con la metodología del BYOD, demostrando su funcionalidad con las políticas y técnicas básicas de privacidad en el Smart Campus de la Universidad Autónoma de Bucaramanga. Las pruebas se documentaron en el informe de resultado de pruebas y evaluación del esquema propuesto, la utilización de PacketFence como NAC permitió el análisis de cómo se implementaba la privacidad con los diferentes actores de usuarios en la UNAB.

De otra parte, esta fase faculta el envío de un artículo de investigación a consideración y publicación, en revista nacional indexada que plasme los resultados del trabajo de grado.

### *4.1.4 Actividades Detalladas*

A continuación se describen en detalle las actividades que conforman cada fase metodológica, así como, sus resultados y entregables (Tabla2), donde se relacionan explícitamente los objetivos con los indicadores y éstos con las actividades, y los resultados esperados.

Tabla 3 : Relación de objetivos con indicadores, actividades y resultados

| | OBJETIVO ESPECÍFICO | INDICADOR | ACTIVIDAD | RESULTADOS ESPERADOS |
|---|---|---|---|---|
| **FASE 1: Exploratoria** | Realizar<br>Una revisión de las diferentes técnicas y mecanismos que existen para controlar la privacidad en ambientes inteligentes. | • El anteproyecto cuenta con una revisión de la literatura desde el año 2000, y de referencias en línea sobre Mecanismos para el control de acceso, seguridad de la información y políticas tipo BYOD.<br>• En la consultas se ha tenido en cuenta investigaciones de Maestrías y Doctorados, además de informes y reportes empresariales. | • Seleccionar artículos de acuerdo al número de citaciones y pertinencia al tema.<br>• Determinar motores de búsqueda, bases de datos y periodo de tiempo.<br>• Seleccionar por palabras clave<br>• Revisar cuales son las políticas de privacidad actuales.<br>• Revisar herramientas y mecanismos para la implementación de políticas relacionadas con la seguridad y privacidad de la información<br>• Revisar las políticas de privacidad en la estrategia BYOD<br>• Primera versión del artículo de investigación a entregar | • Caracterización de los entornos inteligentes<br>• Documento que describe las técnicas y mecanismos más relevantes encontrados que existen para controlar la privacidad en ambientes inteligentes, |
| **FASE 2: Análisis y Diseño** | • Realizar un estudio diagnóstico de los estándares, técnicas y mecanismos de privacidad implementados en aplicaciones móviles para ambientes sensibles al contexto.<br>• Proponer un esquema de estándares de privacidad que permitan manejar grados de seguridad de la información del usuario | • Revisar las políticas de privacidad encontradas<br>• Revisar los tipos de contexto<br>• Diagnóstico sobre las técnicas y mecanismos de privacidad implementados en aplicaciones móviles para ambientes sensibles al contexto.<br>• Documento que describa el esquema de estándares de técnicas y mecanismos de privacidad de la información en ambientes inteligentes y como son aplicados al BYOD. | • Identificar políticas de seguridad y técnicas de privacidad en ambientes sensibles al contexto.<br>• Identificar los tipos de contexto<br>• Identificar los tipos de usuarios<br>• Documentar las políticas a implementar con respecto al BYOD. | • Diagnóstico sobre las técnicas y mecanismos de privacidad implementados en aplicaciones móviles para ambientes sensibles al contexto.<br>• Documento que describa el esquema de estándares de técnicas y mecanismos de privacidad de la información en ambientes inteligentes y como son aplicados al BYOD. |
| **FASE 3:Aplicación** | • Desarrollar una prueba de aplicación de los estándares del modelo propuesto en un entorno urbano real. | • La prueba aplicada incluye hacer las pruebas con el NAC (control de acceso a la red),<br>• Evaluar los dispositivos que intentan acceder a la red asegurandose que cumplen los criterios de seguridad.<br>• Definir politicas según la funcion del usuario, para que puedan acceder a la información correspondiente desde su puesto de trabajo e impedir acceso no autorizado. | • Seleccionr un espacio de la universidad<br>• Documentar la evaluacion a partir de las pruebas<br>• Elaborar un documento de resultados de la prueba y evaluacion del esquema propuesto<br>• Desarrollo de un artículo donde se plasme los resultados de la investigacion. | • Documento resultado de la prueba y evaluación del esquema propuesto.<br>• Artículo científico donde se consignen los resultados del proyecto de investigación. |

Fuente: Autora del Proyecto

# 5 RESULTADOS

## 5.1 ESTUDIO DIAGNÓSTICO DE ESTÁNDARES

Para realizar efectivamente la búsqueda, se clarificaron los conceptos de las palabras clave, en que tipos de Bases de datos se debe consultar, entre qué fechas se debe manejar la consulta y qué tipo de documentos consultar.

Las bases de datos que se usaron para la Fase Exploratoria, fueron las bases de datos Proquest, Ebesco, Scopus, IEEE, ACM, Digital Library y E-libro, las palabras clave fueron consultadas en el tesauro de la Unesco, además de otras fuentes como son Google Scholar y la literatura suministrada por el departamento IT sobre BYOD de Gartner.

La literatura consultada fue de corte científico como páginas oficiales, artículos de revistas, tesis de grado, entre otros. En el Anexo 1, se describe en una tabla la relación de las Referencias consultadas con tipo de documentos referenciados. Se tuvieron en cuenta los documentos posteriores al año 2000, en lo concerniente a los objetivos del proyecto, sin embargo, se consultaron fuentes anteriores debido a la necesidad de referenciar las bases históricas de eventos relacionados con el objeto de estudio del proyecto de grado. De igual manera, se tuvieron en cuenta las publicaciones de las autoridades internacionales en materia de telecomunicaciones, entre ellos, la ISO (International Organization for Standardization), la ITU (International Telecommunication Union) y el W3C (World Wide Web Consortium), contenidos en las normas internacionales. La primera, se ha encargado de las normativas y las especificaciones mundiales para los productos, servicios y los sistemas de los que se hace uso, buscando garantizar su calidad, seguridad y eficiencia. La ITU, activa desde 1865, es una organización

con presencia mundial, con especial interés en el control que los usuarios deben tener de su información, ya sea pública, privada o personal. Por otra parte, el Consorcio W3C (World Wide Web), lidera el diseño de estándares y principios de la Web, con una visión de una red abierta, previendo los alcances y beneficios del internet de las cosas, IoT.

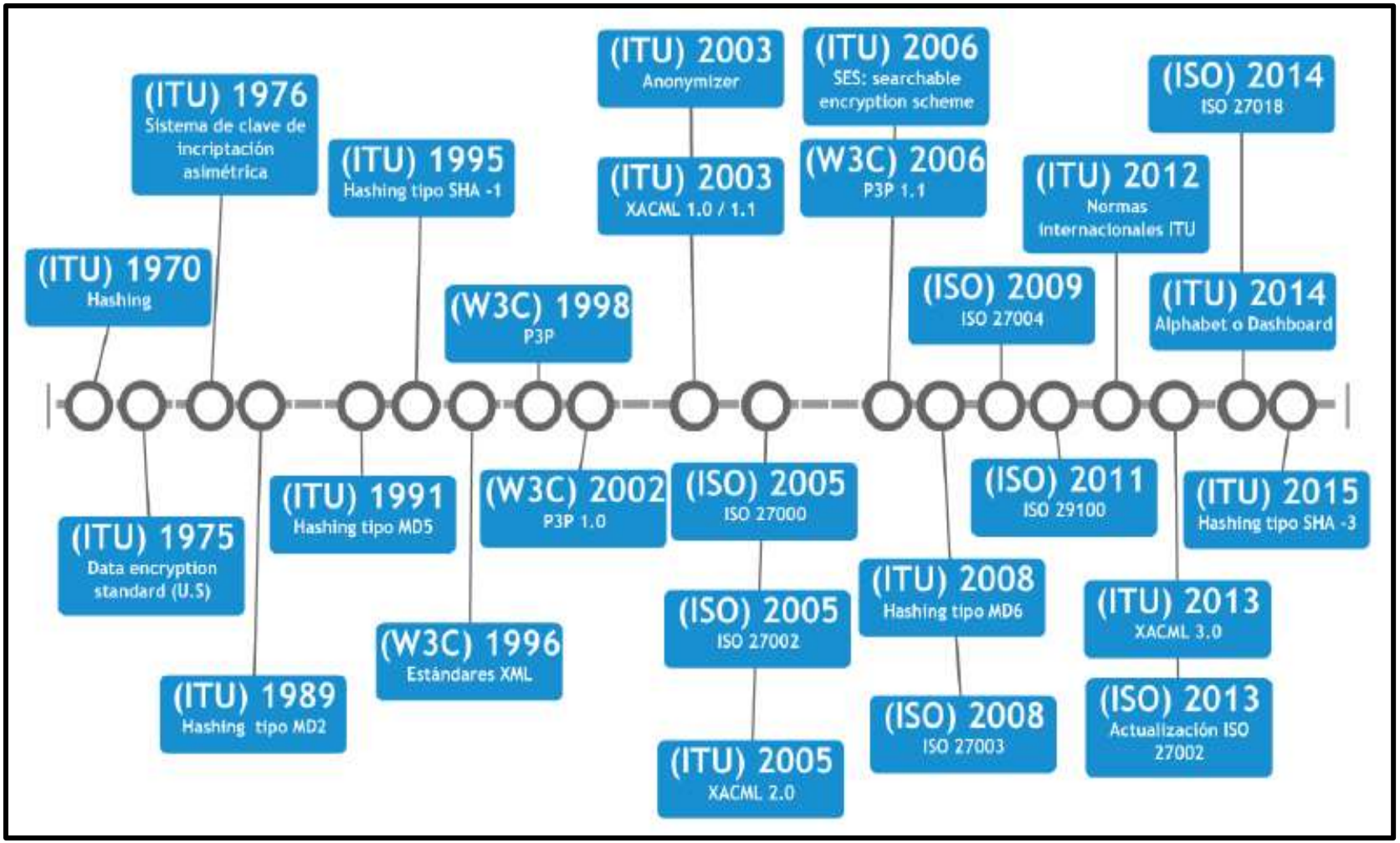
En la siguiente imagen se muestra una línea de tiempo con los estándares más relevantes publicados y sus aportes. La ISO inicia el proceso de proveer requerimientos para establecer, implementar y mantener los sistemas de gestión eficientes, en el 2011 con el estándar ISO 29100, donde se especifica la terminología para privacidad, actores y roles para el procesamiento de PII y principios de privacidad en las TI, continuando, en el 2014, con el estándar ISO 27018, donde se establecen los objetivos, controles y lineamientos que permiten implementar medidas de protección del PII además de los principios de computación en la nube.

En 2012, la ITU publica las normas internacionales sobre la privacidad y el Cloud Computing, enfocándose en la posibilidad compartir recursos en la nube, cuestionando las prácticas de seguridad, confianza y privacidad, que toda compañía debe tener. La ITU propone las PET (Privacy Enhancing Technologies) como un recurso valioso para proteger los datos personales. En 1975 propone la encriptación, que permite aislar los datos, y sus políticas en ambientes de multiples inquilinos para alcanzar el objetivo mencionado; a partir de 1976, se implementa por primera vez la encriptación asimétrica que permite encontrar la información en la nube con el método *Hashing*; otros recursos actuales con los que se cuenta, es el Dashboard de Alphabet y el XACML, un lenguaje extensible para el control de acceso a redes. En la imagen se muestra que en el 2003 se incluyen los Anonymizer, encargados de procesar toda PII bajo anonimato, cambiando la información real por información temporal no rastreable utilizando seudónimos, IP aleatorias, o emails descartables. Para 2006, la ITU adoptó la

estrategia de encriptación rastreable, SES (Searchable Encryption Scheme), que garantiza la confidencialidad de la PII en la nube. La ITU ha ido fortaleciendo las normas de encriptación asimétrica, en el 2008 y 2015, robusteciendo el Hashing en la protección de contraseñas encriptadas (proteger la contraseña encriptada), en el 2014, con el Dashboard de Alphabet y en 2013 el XACML (algoritmos basados en la delegación).

En 1996, el Consorcio W3C desarrolla el estándar XML y plantea la plataforma P3P para las preferencias de privacidad, método que fue diseñado para promover la privacidad y la confianza en la Web, incluyendo la manipulación de la PII y la privacidad de los niños en la Web. Con la primer versión de la plataforma P3P 1.0, los sitios web son habilitados para expresar sus prácticas de privacidad; en 2006, aparece la versión P3P 1.1., en la cual se definen las políticas de privacidad y la sintaxis de la Data Base Schema del W3C, con el diagrama de los datos dinámicos, el diagrama de datos de usuario, diagrama de datos de terceros y el diagrama de datos de negocios.

Imagen 8 : Línea de Tiempo por orden de desarrollo de estándares ISO, ITU y W3C




Fuente Propia Autora del Proyecto

## 5.2 ESQUEMA DE ESTÁNDARES PROPUESTO

### *5.2.1 Técnicas de privacidad comunes encontradas*

En las aplicaciones sensibles al contexto, la privacidad está ligada al control de la información del usuario que contribuyen a los servicios que le puedan presentar, sin embargo un individuo puede interactuar con muchos entornos sensibles abiertos, donde sus datos pueden ser utilizados, es aquí donde se nota la complejidad de la relación usuario – contexto, es por esto que se debe pensar en sistemas conscientes al contexto y que se incluyan políticas de privacidad y seguridad basada en perfiles de usuario, según (Dey A. K., 2001).

Siempre se ha hablado sobre las precauciones que se deben tener al acceder en redes públicas (centros comerciales, restaurantes, parques, entre otros), al correo personal o hacer transacciones bancarias, ya que en éstas cuentas se registran datos personales. Si es necesario el acceso, el usuario debe haber establecido previamente los niveles de privacidad en su dispositivo móvil; contar con una red privada virtual- VPNs (servicio de internet por telefonía móvil) disminuye significativamente el riesgo (Paul, 2013) en las redes públicas, impidiendo que personas ajenas a la red roben su información; parte de ese respaldo están el monitoreo que el proveedor de servicio puede hacer de las actividades del usuario.

Aprovechar los sitios en la nube que proveen espacio de almacenamiento masivo como Dropbox, Google Drive, Sky Drive entre otros, representan un gran riesgo para los datos privados del usuario; en caso de ser así, es preferible utilizar un servicio de almacenamiento en la nube con encriptación como BoxCryptor, TrueCrypt, SpiderOak, Wuala. Al contar con un servicio en línea, es necesario tener presente los siguientes factores: un código numérico corto y la contraseña para tener acceso a su cuenta, incluyendo en algunos casos un *token* como número de verificación.

### *5.2.2 Seguridad en la Red*

Es definida como un conjunto de tecnologías y aplicaciones que utilizan la infraestructura de la red para hacer cumplir las políticas de seguridad en todos los dispositivos que pretenden acceder a sus recursos informáticos.

Adoptar medidas de seguridad que hagan frente a las nuevas amenazas, así como la búsqueda de herramientas que manejan la productividad y la calidad del trabajo que desempeñan sus empleados es uno de los logros del programa BYOD.

Para el presente proyecto se evaluó la seguridad con Cisco, por ser éste el proveedor de la infraestructura de red de la Universidad Autónoma de Bucaramanga UNAB, permitiendo una integración con mayor facilidad en la implementación. Adicional a lo anterior, se evaluaron otras soluciones del tipo OpenSource como FreeNAC y PacketFence cuyas características incluyen el control de acceso e implementación de políticas de seguridad y privacidad de la información, objeto de estudio del presente documento.

### *5.2.3 NAC: Control de Acceso a la Red*

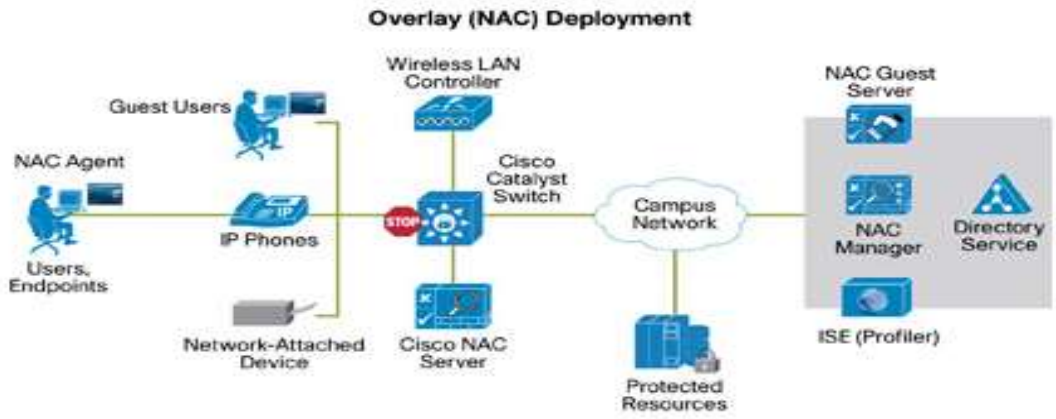
Los administradores de la red de la UNAB utilizan la aplicación CISCO NAC Appliance, para autenticar, autorizar, evaluar y remediar los usuarios alámbricos, inalámbricos y remotos antes de que puedan acceder a la red. (CISCO, 2014).

Con Cisco NAC Appliance es posible:

- Reconocer los usuarios, sus dispositivos y sus funciones en la red.
- Evaluar si las máquinas cumplen con las políticas de seguridad.
- Hacer cumplir las políticas de seguridad mediante el bloqueo, aislamiento y reparación de máquinas que no cumplen.

- Proporcionar fácil y seguro acceso para invitados.
- Simplificar el acceso de dispositivos que no se autentican.
- Informe de Auditoría sobre quien está en la red.

Imagen 9 : Aplicación NAC




Fuente Cisco NAC

El sistema Cisco Network Admission Control, compuesto por el NAC Manager y el servidor de Cisco, es un componente de la política de la solución Cisco TrustSec, representado en la gráfica anterior. Puede implementar este sistema como una solución de recubrimiento para las cuentas que requieren autenticación de red, control de acceso basado en roles y la evaluación de su posición.

### *5.2.4 Jabber Guest Cisco*

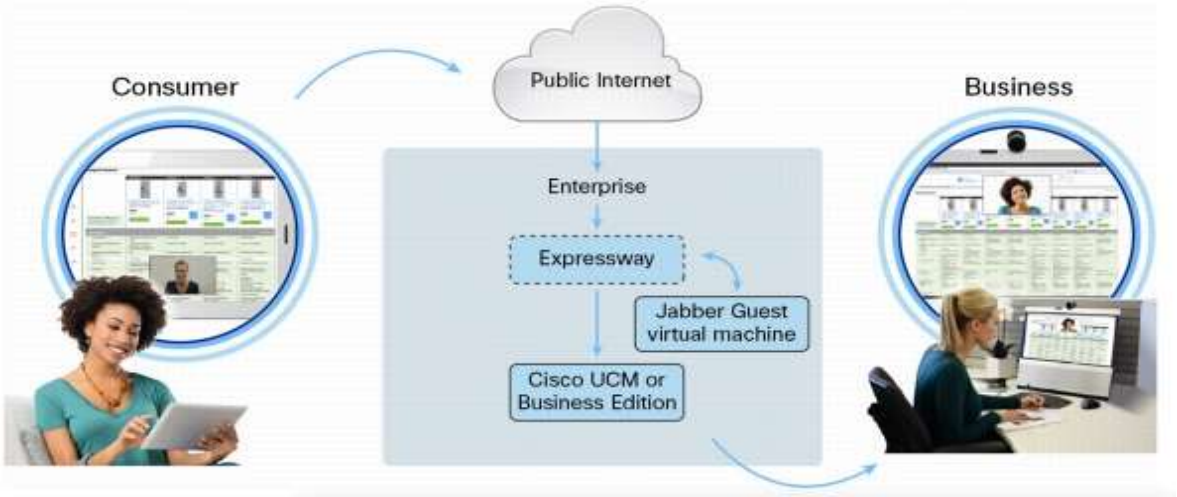
Es una herramienta de comunicación basada en web, que permite establecer conexión de alta calidad entre los usuarios, independientemente de la plataforma a través de su sitio web o aplicaciones móviles para interactuar con agentes del centro de contacto y hace posible que los clientes puedan se puedan contactar

con la empresa para obtener soporte o servicios de video-conferencia de manera inmediata sin necesidad de contar con hardware dedicado. La comunicación se establece por medio de la aplicación CISCO EXPRESS WAY, enmarcada en la arquitectura CISCO EDGE.

Imagen 10 : Aplicación NAC; Fuente Cisco


Fuente Cisco

Imagen 11 : Conexión con Jabber Invitado en la estructura de Comunicaciones Unificada que ya tiene.




Fuente Cisco

### *5.2.5 CISCO TrustSec*

Es una solución que permite controlar de forma inteligente el acceso a los datos corporativos empleando el etiquetado de ingreso y filtrado de salida, para hacer cumplir las políticas de control de acceso de una manera escalable. Las políticas de control de acceso son basadas en roles llamados grupos de seguridad o listas de control de acceso, que deben aplicarse en cualquier parte de la red con switches, routers o dispositivos de seguridad. Cisco TrustSec simplifica en buena parte la gestión de políticas de seguridad y reduce el riesgo al proporcionar una aplicación coherente en cualquier lugar de la red. Con esta aplicación se puede definir el tipo de autenticación de dos formas: Access Control, Tarjeta de testigo o contraseña.

### *5.2.6 Soluciones Open Source: PacketFence*

Para efectos propios de la tesis se trabajó con el programa, Packetfence, que es una solución de acceso a la red tipo OpenSource confiable, de control abierto y libre acceso a la red. Packetfence puede ser empleado en ambientes de redes de cualquier tamaño en diferentes mercados. Así mismo, Packetfence cuenta con un con funciones de tipo portal cautivo para registro, administración y gestión para redes cableadas e inalámbricas; a su vez cuenta con un aislamiento de segunda capa para dispositivos con problemas, soporte 802.1X, integración con Snort IDS y scanner de vulnerabilidades Nessus.

#### *5.2.6.1 Modo de Operación*

PacketFence es una solución a escala geográfica amplia y resistente a fallos, cuando se utiliza la tecnología adecuada (como seguridad de puerto), que consta de una imagen de sistema operativo que corre sobre Linux o Windows y realiza chequeos de políticas de dispositivos según acceden a la red. Su software

autentica a los usuarios mediante cualquiera de los métodos soportados por los servidores Web Apache de fuente abierta y realiza análisis de vulnerabilidades, desviando a los sistemas que no cumplan las políticas a una zona preparada para solucionar su situación. Puede aislar dispositivos mediante cambios por DHCP, manipulando cachés ARP Address Resolution Protocol, contando con un servidor que puede ser usado para controlar cientos de switches y en múltiples nodos.

PacketFence es innovador entre los paquetes NAC basados en software libre, la mayoría de ellos creados en reacción a los problemas de seguridad en las redes, detonante que empuja a las firmas comerciales a desarrollar sus propias soluciones. Los usuarios se han inclinado por el software libre debido a su bajo precio, independencia de fabricantes y compatibilidad con la mayoría de los *switches*, posibilitando el enriquecimiento del software en su arquitectura gracias a las mejoras compartidas que los usuarios hagan de él.

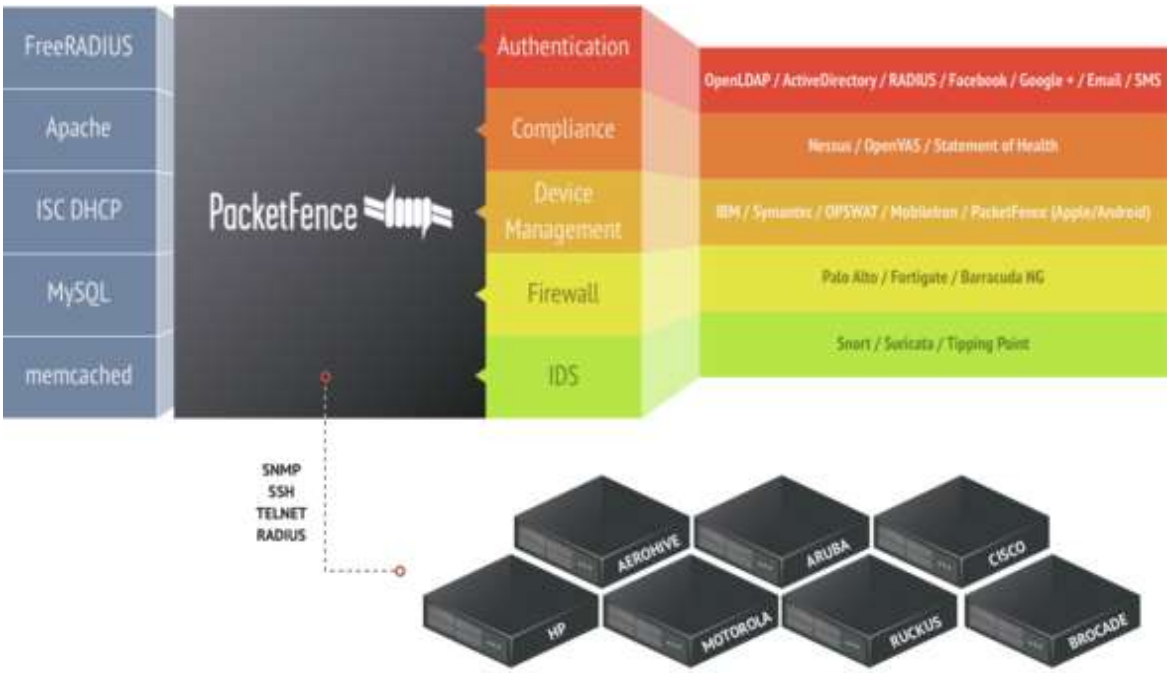
La gestión de la seguridad en las redes que usan la plataforma FreeNac representa grandes ventajas para las compañías; una de sus aplicaciones consiste en la detección de los dispositivos ajenos a la red que intenten obtener acceso a través de un conector de red Ethernet, acto seguido, niega el acceso y registra el evento. Los usuarios Conocidos y registrados se habilitan en la red LAN, en tanto que los usuarios con el perfil de visitantes (dispositivos desconocidos) pueden tener un acceso opcional a una zona llamada VLAN de default / guest VLAN. Para las organizaciones que deseen permitir acceso a los visitantes Web / VPN de acceso por Internet, pero que no tienen acceso a las redes internas, esto puede ser una solución. Lo anterior es visible en las redes de compañías como:

- Bancos, Empresas de ingeniería y Fábricas.
- Colegios y universidades.
- Centras de convenciones y exposiciones.

- Hospitales, centros médicos.
- Hoteles.

### *5.2.6.2 Arquitectura*

Imagen 12 : Arquitectura PacketFence;




Fuente: http://www.packetfence.org/

### *5.2.6.3 Autenticación y Registro*

La autenticación y registro en la red se realiza ejecutando los siguientes pasos:

- **Soporte 802.1X:** inalámbrico y cableado se apoya en un módulo FreeRADIUS incluido en PacketFence.

- **Integración inalámbrica:** Se integra perfectamente las redes inalámbricas a través del módulo FreeRADIUS. Utilizando la misma base de datos del usuario; permite asegurar las redes cableadas e inalámbricas haciendo uso del mismo portal cautivo, proporcionando una experiencia de usuario consistente. La combinación de los puntos de acceso (AP) proveedores y controladores inalámbricos es compatible.
- **Voz sobre IP:** Es también llamada de telefonía IP, VoIP es totalmente compatible para diversos proveedores de conmutación.

- **Registro de dispositivos**: defiende un mecanismo de registro opcional similar a soluciones del "portal cautivo". A diferencia de las otras soluciones de portal cautivo, PacketFence recuerda a los usuarios que no es necesario hacer una autenticación cuando existe una previamente registrada, dándoles automáticamente el acceso. También es configurable. Una política de uso aceptable se puede especificar de forma que los usuarios no pueden permitir el acceso a la red sin antes aceptarla.

*5.2.6.4 Detección de Vulnerabilidades*

- **Detección de actividades anormales de red:** como actividades anormales de la red se encuentran (virus informáticos, gusanos, spyware, tráfico denegado por la política de establecimiento, etc.) y pueden ser detectados utilizando el sistema de detección de intrusos, de forma local o remota. Más allá de la detección simple, PacketFence crea su propia alerta y ejecuta la supresión del mecanismo en cada tipo de alerta. Para los administradores está disponible un conjunto de acciones configurables para cada tipo violación.

- **Scans de vulnerabilidades proactivas:** detecta las vulnerabilidades programadas o sobre una base ad-hoc. PacketFence correlaciona los ID de la

vulnerabilidad con cada ID de exploración, a la configuración de violación Nessus / OpenVAS, revelando el contenido de páginas web específicas en las que se identifique cualquier vulnerabilidad que el huésped pueda tener.

- **Declaración de Salud:** Mientras que se realiza la autenticación de un usuario 802.1X, PacketFence puede evaluar la posición del dispositivo de conexión con el Protocolo de Declaración de Salud, TNC. Por ejemplo, PacketFence puede verificar si se ha instalado un antivirus hasta la fecha, si los parches del sistema operativo son todos aplicados, todo lo anterior sin ningún agente instalado en el dispositivo de punto final.

#### *5.2.6.5 Portal Cautivo*

- **Remediación a través de un portal cautivo:** Una vez atrapado, todo el tráfico de la red se determina por el sistema PacketFence. En base a la situación actual de los nodos (no registrado, violación abierta, etc.), el usuario es redirigido a la URL correspondiente. En el caso de una violación, el usuario será presentado con las instrucciones para la situación particular que él / ella se encuentra, reduciendo la intervención.
- **El aislamiento de los dispositivos problemáticos:** PacketFence soporta varias técnicas de aislamiento, como el aislamiento de VLAN con soporte VoIP (incluso en entornos heterogéneos) para varios fabricantes de switches.

#### *5.2.6.6 Administración*

- **Línea de comandos y gestión basada en Web:** son interfaces basadas en Web y de línea de comandos para todas las tareas de gestión. Administración basada en Web es compatible con diferentes niveles de permisos para

usuarios y la autenticación de usuarios contra LDAP o *Microsoft Active Directory*. (PacketFence)

### *5.2.6.7 Características Avanzadas*

El nodo se utiliza para referirse a un dispositivo de red consciente de que es controlado y supervisado por PacketFence. Puede ser un PC, ordenador portátil, impresora, teléfono IP, etc.

- **Gestión VLAN flexible y control de acceso basado en roles**:
  VLAN y los roles se pueden asignar utilizando los diversos medios:
  - Por interruptor (por defecto para VLAN).
  - Por categoría de cliente (por defecto para papeles).
  - Por cliente.

- **El acceso de invitados - Traiga su propio dispositivo (BYOD):** Hoy en día, la mayoría de las organizaciones se ocupan de una gran cantidad de consultores de diversas empresas en las instalaciones que requieren acceso a Internet para su trabajo. En la mayoría de los casos, un acceso a la red corporativa se da con poca o ninguna auditoría de la persona o dispositivo. Además, rara vez se requiere que tengan acceso a la infraestructura corporativa interna, que se hace de esa manera para evitar (administración de VLAN por puerto) carga administrativa.
  Si utiliza una VLAN de invitados, se debe configurar la red para que la VLAN de invitados solamente salga a la Internet y la VLAN de registro y el portal cautivo son los componentes que se utilizan para explicar a los invitados cómo registrarse para el acceso. Esto normalmente se marca por la organización que ofrece el acceso a la red. Son posibles varios medios de huéspedes para:
  - Registro manual de los huéspedes.

- Contraseña del día.
- Auto-inscripción (con o sin credenciales).
- Acceso para patrocinar invitados (empleado que dé fe de un huésped).
- Acceso para invitados activado por correo electrónico de confirmación.
- Acceso para invitados activado por la confirmación de teléfono móvil (mediante SMS).
- Acceso para invitados activado a través de una autenticación de Facebook / Google / GitHub.

PacketFence también soporta el acceso para invitados, creación de múltiples perfiles e importación de perfiles de usuario. PacketFence también se integra con la solución de facturación en línea, como Authorize.net. El uso de esta integración puede manejar los pagos en línea necesarios para obtener acceso a la red adecuada.

*5.2.6.8 Modos de Funcionamiento*

La ejecución del PacketFence puede ser desplegado en 3 modos de funcionamiento:

- **Out-Of-Band:** en este modo, el servidor de PacketFence se encarga de realizar las comprobaciones de políticas, acceso a la red, consulta a servidores de autenticación, este modo es el más usado siendo el método más escalable, resistente a fallos y es utilizado en las redes que soportan VLANs.

- **In-Band:** utilizado en redes con switchs antiguos. Desde la versión 3.0 de PacketFence se implementa el modo “In-Line” donde el servidor PacketFence se convierte en la puerta de enlace de la red, donde se conectan todos los dispositivos incompatibles.

Este modo presenta limitaciones del siguiente orden:

a. Todos los dispositivos de la red están en la misma LAN de capa 2, donde se ve afectado por temas de broadcast en el caso de muchos dispositivos.

b. Todos los paquetes enviados por los dispositivos deben pasar por el servidor de PacketFence, por lo que aumenta la carga de trabajo en el servidor.

c. Dispositivos de red sin autenticar.

- **Modo Hibrido:** soporta el modo de autenticación 802.1x y autenticación por MAC, es posible autenticar dispositivos por medio de RADIUS a través de 802.1x o autenticación por Mac desde la versión 3.6 de PacketFence.

*5.2.6.9 Perfiles del Portal*

PacketFence apoya el concepto de perfiles del portal. Un perfil de portal define el flujo de trabajo de registro que se utilizará, junto con las páginas de registro y regularización.

- **User – Agent**

PacketFence puede bloquear dispositivos basados en el User-Agent proporcionado cuando esos dispositivos particulares realizan actividad de la red utilizando su navegador web incorporado.

- **Direcciones MAC**

PacketFence puede bloquear el acceso de red a dispositivos que tienen un patrón específico de direcciones MAC. Usando esto, se podía bloquear de forma automática, por ejemplo, todos los dispositivos de un proveedor de red específica.

- **Inscripción automática**

Debido a que la mayoría de las redes de producción ya son muy grandes y complejas, PacketFence ofrece varios medios para registrar automáticamente un cliente o dispositivo.

- Por dispositivo de red:

  Un dispositivo de red (Switch, AP, mando inalámbrico) se puede configurar para registrar automáticamente todas las direcciones MAC que la solicitud de acceso a la red. Muy útil para la transición a la producción.

- Por DHCP toma de huellas dactilares:

  Huellas dactilares DHCP se puede utilizar para registrar automáticamente los tipos específicos de dispositivos (por ejemplo. Los teléfonos VoIP, impresoras).

- Por dirección MAC del vendedor:

  La parte del proveedor de una dirección MAC se puede utilizar para registrar automáticamente los dispositivos de un proveedor. Por ejemplo, todos los productos de Apple podrían ser registrados de forma automática utilizando una norma de este tipo.

- **Caducidad**

La duración de acceso a la red puede ser controlada con los parámetros de configuración. Puede ser una fecha absoluta, una ventana cuando el dispositivo se vuelve inactivo (por ejemplo. "Cuatro semanas desde el primer acceso a la red"), o vencido el registro de los dispositivos, se convierten en *no registrados*. Con poca personalización también es posible hacer esto en una base categoría de dispositivo. Vencimiento también se puede editar manualmente en función de cada nodo.

- **Auditoria de Ancho de banda**

PacketFence puede rastrear automáticamente el ancho de banda consumen dispositivos en la red. Con su apoyo violaciones incorporados, se puede poner en cuarentena o cambiar el nivel de acceso de los dispositivos que consumen demasiado ancho de banda durante una ventana de tiempo en particular. PacketFence también tiene informes sobre el consumo de ancho de banda. (PacketFence, 2015).

A continuación se muestra en una tabla el resumen de las características de PacketFence:

#### *5.2.6.10 Características de PacketFence*

Tabla 4 : Características de PacketFence

| **CARACTERISTICAS DE PACKETFENCE** | | |
|---|---|---|
| **Control de Acceso** | **Seguridad de la información** | **Remediación** |
| Mecanismo de registro similar a “Portal Cautivo”.<br><br>El usuario solo necesita autenticarse a la red y una sola vez, ya que PacketFence recuerda a los usuarios que ya se han autenticados en la red. (política de uso)<br><br>Soporta Vlans y se encarga de realizar las comprobaciones de políticas, acceso a la red o consultas,<br><br>Y utiliza RADIUS para la autenticación de dispositivos. | • **Detección de actividades anormales de la red**<br>Packetfence cuenta con acciones configurables para cada tipo de violación.<br>• **Exploraciones de vulnerabilidades proactivas**<br>Packetfence correlaciona los ID de la vulnerabilidad de cada uno de exploración a la configuración violación Nessus/OpenVAS (herramientas para auditoria de la seguridad), retornando a vulnerabilidad del huésped.<br>• **Aislamiento de dispositivos problemas**<br>Soporta aislamiento de VLAN con VoIP para varios fabricantes de Switches. | La remediación a través de un portal cautivo (o puerta de enlace)<br><br>En el caso de No registrado, violación abierta, etc., el usuario es redirigido a la URL correspondiente.<br><br>En el caso de violación el usuario será presentado con las instrucciones para la situación particular |

Fuente: Autora del Proyecto

#### *5.2.6.11 Proveedores de servicios*

Cisco es una compañía fundamentada en el crecimiento exponencial de las nuevas tecnologías. Su visión del mercado atiende directamente los aspectos estructurales de redes, soporte técnico y capacitación en todos sus productos, aplicaciones y soluciones; lo anterior la convierte en una elección acertada para las empresas que procesan grandes cantidades de datos e información. Contar con un proveedor de servicios como Cisco, implica recibir apoyo en las actividades de la empresa, siendo un respaldo para las operaciones que requiera el sistema; El costo que representa su participación coincide con la regulación internacional, pasando a ser una buena inversión cuando los procesos ejecutados en entornos sensibles necesitan mayor acompañamiento y seguimiento en etapas de inicio y de reestructuración.

Por otra parte, el software de tipo Open Source es una solución de carácter colectivo, cuya finalidad es generar un espacio de intercambio de conocimientos que permitan mejorar y robustecer cualquier aplicación de este tipo. Implementar un proveedor de servicios utilizando PacketFence, conllevaría capacitar el personal que haga el soporte técnico de la plataforma e influya en las modificaciones estructurales que la red requiera. A su vez, En los costos se ven reflejados la creación de un departamento encargado del acompañamiento de los procesos ejecutados en la plataforma, el seguimiento de las fallas y correcciones del sistema, la constante revisión de la compatibilidad entre los protocolos de privacidad y seguridad de la información que funcionan en la red, y el acoplamiento de las funciones ejecutadas por el software a las necesidades de la compañía.

A continuación se presenta una tabla comparativa entre las dos formas de proveedor de servicio y lo que se refiere a costos no es competencia del presente trabajo.

## CUADRO COMPARATIVO ENTRE SISTEMA PROPIETARIO & OPENSOURCE

Tabla 5 : Cuadro comparativo de dos proveedores de servicio Cisco y Open Source (con Packetfence)

| | Autenticación y Registro | Integración Inalámbrica | Tipo de seguridad | Políticas por puerto | Integración otros fabricantes | Soporte máquinas virtuales | Edición de módulos Interfaz | Detección de Dispositivos | Soporte Actualizado | VLANs Dinámicas o Listas de control de acceso | Agente |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **PacketFence OpenSource** | Soporta 802.1X LAN inalámbrica, se envía la dirección MAC en lugar del nombre | Apoyo de Servidor FreeRADIUS.<br><br>Utiliza la misma base de datos del usuario y el portal cautivo, proporcionando una experiencia de usuario. | Mecanismo "Portal Cautivo" de registro y remediación, gestión centralizada por cable e inalámbrico.<br>El usuario debe ser previamente registrado antes de autenticarse | Si<br><br>Recuerda la dirección MAC conectada al puerto | Si | Si | Si | Si | Si | Si<br>Asigna VLAN a un dispositivo | No |
| **Cisco Propietario** | Soporta 802.11i LAN inalámbrica<br>Apoyo de ISE (Identity Service Engine) | Radios-LA 802.11a. (admite las funciones de punto de acceso de cisco IOS versión 1.4 y posteriores) | Configurado el punto de acceso asociando con AES y cifrado TKIP.<br><br>Con el motor de Servicios de identidad - ISE crea el control de acceso basado en roles, además de controlar las amenazas. | No | No | Si | No | No | Si | No | Si |

Fuente: propia autora proyecto

### *5.2.7 Almacenamiento de datos de usuario y seguridad según GSMA[90]*

Una de las inquietudes que se genera en la red cuando hablamos de dispositivos móviles es si la red maneja seguridad de la información corporativa y cada usuario debe tener claro que es él/ella quien maneja la privacidad de su información personal sensible. La GSM (Global System for Mobile Communications)[91] es la organización que representa los intereses de los operadores móviles a nivel mundial: GSM es una tecnología celular abierta, digital utilizada para la transmisión de voz y datos móviles, y ***GSM Association (GSMA)*** es una asociación con sede en Londres, que se dedica a apoyar la estandarización, despliegue y promoción del sistema telefónico móvil de GSM. Con presencia en 219 países, más de 800 operadores móviles de todo el mundo, más de 200 empresas de sistemas móviles (fabricantes de dispositivos móviles, fabricantes de software, proveedores de equipos, compañías de Internet, y de entretenimiento). La GSMA está enfocada en innovar, incubar y crear nuevas oportunidades para sus miembros con el propósito de impulsar la industria móvil en el mundo[92]. Ésta organización se ha interesado en la privacidad y la seguridad en los dispositivos móviles; sostienen que puede haber seguridad sin privacidad pero no puede haber privacidad sin seguridad.

Lo más importante es ¿Cómo el usuario del dispositivo móvil administra su información personal? ¿Cómo almacena su información? ¿Por cuánto tiempo es necesaria esa información personal para el modelo de negocio? ¿Cómo eliminarla de forma segura? (GSMA Association 2012).

Se pretende que los principios, métodos y estándares que se refieren a la privacidad deberán identificar medidas efectivas y seguras para permitir que la privacidad del usuario en sus dispositivos móviles esté protegida en contextos

[90] GSMA: Asociación del Sistema Global para Comunicaciones Móviles
[91] GSM: Sistema Global para Comunicaciones Móviles su traducción al español
[92] GSM Association: Asociacion del Sistema Global para Comunicaciones Móviles, Fuente: http://www.gsma.com/latinamerica/mobile-and-privacy

sensibles, controlados o no, permitiendo adoptar el enfoque de “Privacidad por Diseño” armonizando el contexto con las aplicaciones y el usuario.

Los principios de privacidad móvil expuestos por la GSMA van relacionados con los principios de protección de datos y privacidad reconocidos por Alan Westin, donde ha planteado dos principios adicionales que son muy importantes y aceptados a nivel internacional como son Educación (se debe informar al usuario sobre la privacidad y seguridad de su información además de las formas de administrar y proteger su privacidad), y Niños y Adolescentes (dirigido a la población de niños y adolescentes, que permita asegurar que la información recopilada, el acceso y uso es apropiada en cualquier circunstancia y compatible con la ley). (GSMA Association 2012).

#### *5.2.7.1 Opciones y Mecanismos para Controlar la Privacidad*

De acuerdo con las tablas anteriormente presentadas, un factor crítico de protección efectiva de la privacidad, en cuanto a las aplicaciones y servicios móviles ha sido la oportunidad de crear y promocionar condiciones que aseguren una plataforma para la conectividad personal y protección de los datos, ya que los usuarios buscan técnicas y normas consistentes que le permitan cumplir las expectativas de privacidad.

La confianza que el usuario puede tener a la hora de utilizar sus dispositivos móviles, se da cuando le permite conocer:

- Quién está recopilando y utilizando su información personal.
- Por qué se utiliza su información personal.
- Qué información personal está siendo compartida, con quién y con qué propósitos.

Por lo tanto la situación del usuario se puede definir en TEC (transparente, capacidad de elección y control) como se muestra en la siguiente tabla donde se

describen las directrices que deben ser atendidas, por los diseñadores de las aplicaciones móviles y qué debe tener en cuenta el usuario al momento de ejecución de la aplicación, relacionando algunos casos prácticos a tener en cuenta. (GSMA, Móviles y Privacidad, 2012).

Tabla 6 : Opciones y Mecanismos para controlar la privacidad

| OPCIONES Y MECANISMOS PARA CONTROLAR LA PRIVACIDAD | | |
|---|---|---|
| **Directriz** | **Ejecución** | **Casos prácticos y ejemplos** |
| **TEC1**<br>No acceda a/o recopile información personal de forma clandestina.<br><br>Una aplicación no puede acceder ni recopilar información personal de sus usuarios de forma secreta.<br><br>Los usuarios deben ser informados de la recopilación y uso de su información personal desde el inicio, permitiéndoles tomar decisiones informadas sobre el uso de una aplicación o servicio. | Antes que un usuario descargue o active una aplicación, debe ser informado de:<br>• Qué información personal va a acceder, recopilar y usar.<br>• Qué información personal será almacenada (en su dispositivo y de forma remota)<br>• Qué información personal será compartida, con quién y con qué propósito<br>• Por cuánto tiempo se almacenará esa información personal<br>Considerar que cualquiera términos y condiciones de uso afectan a la privacidad del usuario<br><br>Garantice la usabilidad y evite un exceso de mensajes instantáneos que agobien al usuario. | Una aplicación **no** puede acceder a la localización del usuario si no es una aplicación de servicios basados en localización.<br>Una aplicación **no** puede acceder y usar los datos de los contactos guardados en la agenda de ningún dispositivo móvil, a no ser que sea una parte funcional de la aplicación y haya sido explicada claramente al usuario.<br>Si desea utilizar la información personal para otros propósitos distintos de los que manifestó a sus usuarios en un principio, tendrá que volver a ponerse en contacto con ellos, informarles acerca de los nuevos usos y conseguir su permiso. |
| **TEC2**<br>Identifíquese con los usuarios<br><br>Los usuarios tienen que saber quién está recogiendo o usando su información personal y cómo pueden ponerse en contacto con esa entidad para conseguir más información o para ejercer sus Derechos. | Antes que un usuario descargue o active una aplicación, debe ser informado de la identidad de las entidades que recogerán o usarán su información personal dentro del ámbito de la aplicación, indicando el Nombre de la empresa o persona y el país de origen.<br><br>Los usuarios deben contar con acceso fácil a los datos de contacto de la organización. | La página de inicio de la aplicaciones es un lugar excelente para publicar los puntos clave en materia de privacidad,<br>Información de contacto y para proporcionar un enlace a un informe más detallado sobre privacidad.<br>Sea creativo y anime a los usuarios a que exploren las mejores maneras de controlar su privacidad. |

| Directriz | Ejecución | Casos prácticos y ejemplos |
|---|---|---|
| **TEC3**<br>Deje que los usuarios ejerzan sus derechos.<br>Proporcione a los usuarios información suficiente, de forma que sea razonable pensar que saben cómo acceder y corregir cualquier información personal que pueda almacenar sobre ellos. | Proporcione un informe breve y realmente informativo, explicando en términos claros y sencillos cómo puede conseguir el usuario una copia de su información personal o corregir y<br>Actualizar la información proporcionada por ellos mismos o que usted almacena. | Como se indica previamente, la página de inicio de la aplicación puede ser el lugar idóneo para ubicar un aviso claro y sencillo para los usuarios o para dirigirles a un apartado con información más detallada sobre como ejercer su derecho a la protección de datos. |
| **TEC4**<br>Minimice la información que recopila y limite su uso. La información recopilada por una aplicación debe ser razonable, no excesiva, y usada dentro del ámbito de las expectativas del usuario y otros propósitos legítimos de la empresa, tal y como se notificó a los usuarios. | Piense qué información necesita y luego justifíquelo. ¿Es realmente necesaria?, ¿tiene que recopilarla, compartirla o almacenarla para cumplir con una necesidad de empresa u obligación legal?<br><br>Una aplicación tiene que acceder, recopilar y usar únicamente la mínima información requerida para:<br>• generar, operar o mantener la aplicación<br>• cumplir con los objetivos identificados de la empresa, sobre los que ha informado a los usuarios o para cumplir con las obligaciones legales. | Si necesita acceso a los datos de una lista de contacto, identifique que campos se necesitan obligatoriamente para que se desempeñe una función específica de la aplicación y no recopile más que los campos requeridos.<br><br>No use esa información para otros propósitos que no sean obvios, a no<br>Ser que el usuario haya accedido a esta utilización. |

| Directriz | Ejecución | Casos prácticos y ejemplos |
|---|---|---|
| **TEC5**<br>Cuando fuese necesario, obtenga el consentimiento activo del usuario En algunas ocasiones los usuarios tienen que dar su consentimiento activo para el uso de su información personal.<br><br>Recopilación o uso de información personal que no es necesaria para el propósito principal de la aplicación. | Los usuarios deben tener la oportunidad de decidir si quieren permitir y dar por obvios los usos de su información. Redes sociales y medios digitales, publicidad móvil, servicios de localización, niños y adolescentes. Allí donde sea necesario contar con el consentimiento activo, los usuarios deberían ser informados de:<br>• Por cuánto tiempo es válido ese consentimiento<br>• Cómo pueden administrar ese consentimiento que han dado<br>• Las consecuencias de mantener o retirar su información<br>• Consentimiento: Los usuarios tienen que poder retirar su consentimiento de una forma simple y eficiente, sin esperas o costes indebidos | Las aplicaciones que no usan los servicios de localización para ninguna de sus funciones u operatividad contratadas por el usuario, no deberían recopilar esta información para otros propósitos -por ejemplo, publicidad dirigida o estadísticas- a no ser que el usuario brinde su consentimiento activo. |
| a) Compartir información personal con terceros | Si terceras partes recopilarán o tendrán acceso a la información del usuario para sus propios propósitos, el usuario tiene que ser informado lo antes posible de que sus datos serán compartidos, indicando:<br>• Con quién serán compartidos y con qué fines<br>• Enlaces para ponerse en contacto con esas terceras partes y sus informes de privacidad. Los usuarios deben tener la opción de elegir si quieren permitir esa recopilación, acceso y uso por terceros. | Las aplicaciones no deberán incluir un código de terceros que recopile y analice información personal para dirigir Publicidad a los usuarios, sin el consentimiento activo del usuario. |

| Directriz | Ejecución | Casos prácticos y ejemplos |
|---|---|---|
| b) Almacenar información personal inmediatamente después del uso de la aplicación. | Si los datos de un usuario se retienen inmediatamente después del uso de una aplicación, los usuarios tiene que ser informados sobre:<br>• Los periodos durante los que se almacenará la información y por qué<br>• Cómo puede ejercitar el usuario sus derechos específicos sobre su información | |
| **TEC6**<br>Dé control a los usuarios sobre la frecuencia de los mensajes instantáneos.<br>Siempre que sea posible, los usuarios deberían tener la opción de decidir cómo -y con qué frecuencia- se les recuerda qué funciones y procesos usan su información personal | Siempre que sea posible, dé a los usuarios la posibilidad de decidir cómo y con qué frecuencia recibirán mensajes instantáneos para la toma de decisiones referentes al acceso y uso de su información personal.<br><br>*Privacidad por Diseño significa poner al usuario en primer término y ayudar a que sea consciente de las implicaciones de privacidad que tienen las aplicaciones y servicios y que las administre*, de forma que se mejore la experiencia de privacidad del usuario. | Los usuarios deben tener la opción de “recordar” sus datos de acceso, dirección de facturación, direcciones de correo electrónico o su localización.<br><br>Los usuarios pueden permitir que una aplicación acceda de forma permanente a los servicios de localización del dispositivo o durante un periodo específico o seleccionar que se les avise periódicamente de esta circunstancia por medio de un email, un mensaje de texto, una notificación de la aplicación o un icono. |

| Directriz | Ejecución | Casos prácticos y ejemplos |
|---|---|---|
| **TEC7**<br>No a las actualizaciones silenciosas (“secretas”)<br>Los usuarios deben aceptar cualquier cambio en una aplicación que afecte a su privacidad | Los usuarios tienen que ser informados sobre cualquier cambio substancial en la forma que una aplicación recopila o usa su información personal, antes de que el cambio sea llevado a cabo, de forma que puedan tomar una decisión informada sobre si desean continuar utilizando la aplicación.<br>El consentimiento puede ser obtenido de dos formas:<br>1. Notifique que se llevará a cabo un cambio y desactivar la aplicación.<br>2. Que el usuario pueda elegir si los adopta: un mensaje instantáneo con las opciones de si desea permitir los cambios o continuar con la configuración previa. | Esto no impide las actualizaciones remotas de tipo inalámbrico que son necesarias para mantener la operatividad principal e integridad de una aplicación o servicio.<br><br>La directriz se aplicaría, por ejemplo, siempre que la aplicación deseara de repente acceder y subir los datos de contacto almacenados en el dispositivo móvil o los datos de localización del dispositivo |

En el desarrollo de aplicaciones, los TEC (transparente, capacidad de elección y control). Fuente: (GSMA, Móviles y Privacidad, 2012)

#### *5.2.7.2 Almacenamiento de Datos y Seguridad*

Los grandes proponentes de los términos Seguridad y Privacidad, han llegado a la conclusión que “puede haber seguridad sin privacidad, pero no puede haber privacidad sin seguridad”. La empresa asegura su información y permite ofrecer al usuario niveles de privacidad de los datos de la empresa mas aún no es tan efectivo que pueda ofrecer privacidad a los datos del usuario PII.

Como empresa, asegúrese de que está protegiendo adecuadamente la información personal que un usuario le ha confiado; por medio de su dispositivo móvil o por medio de las aplicaciones que recopila información. Es necesario

preguntarse ¿Por qué necesita retener la información personal de un usuario? y por ¿cuánto tiempo necesitaría tenerla almacenada?, ¿puede justificarlo?, ya que la información personal almacenada indefinidamente pierde valor con el paso del tiempo porque deja de ser actualizada, pero incrementa su costo y su riesgo. Si el modelo de negocio necesita una información personal determinada es importante eliminarla de forma segura cuando ya no sea requerida.

Establecer periodos de almacenamiento pequeños para sus datos es una buena práctica de negocio, ya que puede evitar acciones regulatorias negativas, teniendo en cuenta la ley de protección de datos que actualmente rige en nuestro país, el Habeas Data, Ley 1581 del 2012 con el Decreto reglamentario 1377 del 2013.

#### *5.2.7.3 Estudio de GSMA sobre las actitudes relacionadas con la privacidad de los usuarios móviles en Colombia.*

GSMA lanzó la iniciativa de privacidad en el sector móvil en Enero de 2011 que incluye la investigación sobre formas de brindar a los usuarios maneras contextuales amigables para manejar su privacidad e información en dispositivos móviles. El estudio fue realizado por Futuresight y entregado en Marzo (2013).

- **Los Objetivos del estudio:**

Los resultados del reporte ayudan a entender las preocupaciones de privacidad que tienen los usuarios de dispositivos móviles y cómo éstas influencian el uso y sus actitudes hacia los servicios y aplicaciones de internet móvil. El estudio también cooperó con el desarrollo de políticas públicas y a apoyar el desarrollo de experiencias de privacidad efectiva y consistente, que permitirá que los usuarios se familiaricen con las formas de gestionar su privacidad en dispositivos móviles.

Esta investigación se ha realizado en España, Reino Unido, Singapour, México, Brasil y Colombia, y se ha basado en las respuestas de más de 8500 usuarios de dispositivos móviles." (Futuresight, 2013). La ficha técnica corresponde a la Visión general de la muestra en la siguiente tabla, donde se observa la muestra de 1.511 usuarios de dispositivos móviles, donde el 67% son usuarios de Smartphone; también se hace una comparación por fabricante donde han seleccionado las 4 empresas más representativas.

Tabla 7: Visión general de la muestra (Colombia)

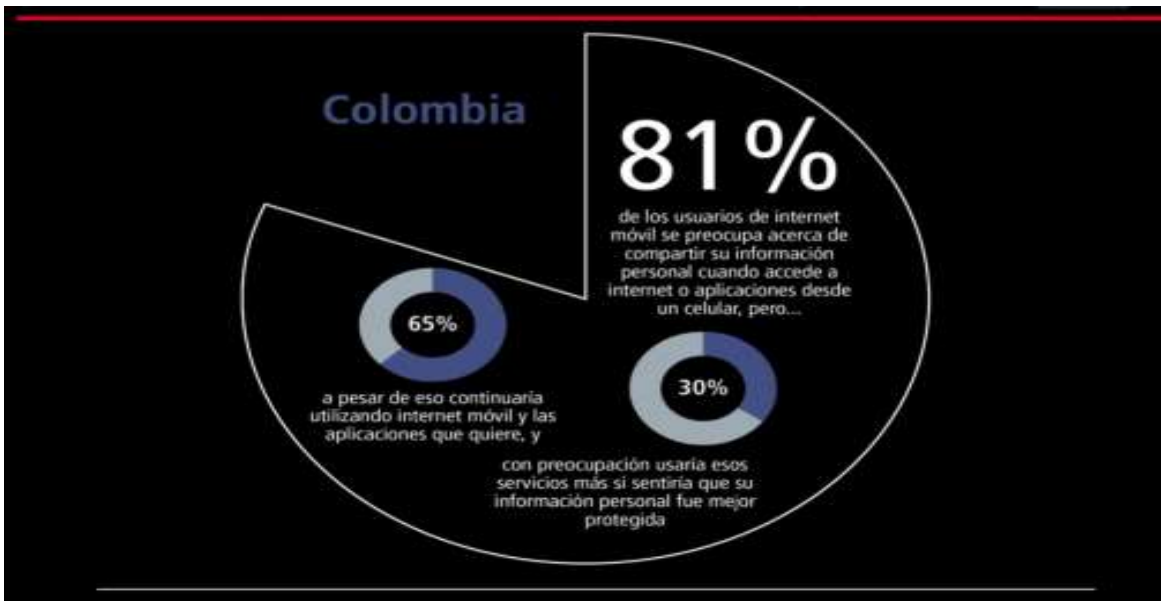
| TABLA COMPARATIVA DEL COMPORTAMIENTO DISPOSITIVOS MÓVILES EN COLOMBIA | | | | |
|---|---|---|---|---|
| Muestra total | 1.511 usuarios móviles | Operadores | | Claro →54%<br>Movistar →27%<br>Tigo → 17% |
| Usuarios Smarphone | 67% | Método de pago | | Contrato 67%;<br>Prepago 33% |
| Género | 52% Masculino<br>y<br>48% Femenino | Fabricantes | Blackberry (23%)<br>Samsung (23%)<br>Nokia (22%)<br>Apple (8%) | LG (5%)<br>Motorola (5%)<br>Sony Ericsson (4%) |

Fuente: MGA estudio sobre las actitudes relacionadas con la privacidad de los usuarios móviles.

Algunas muestran a continuación[93]:

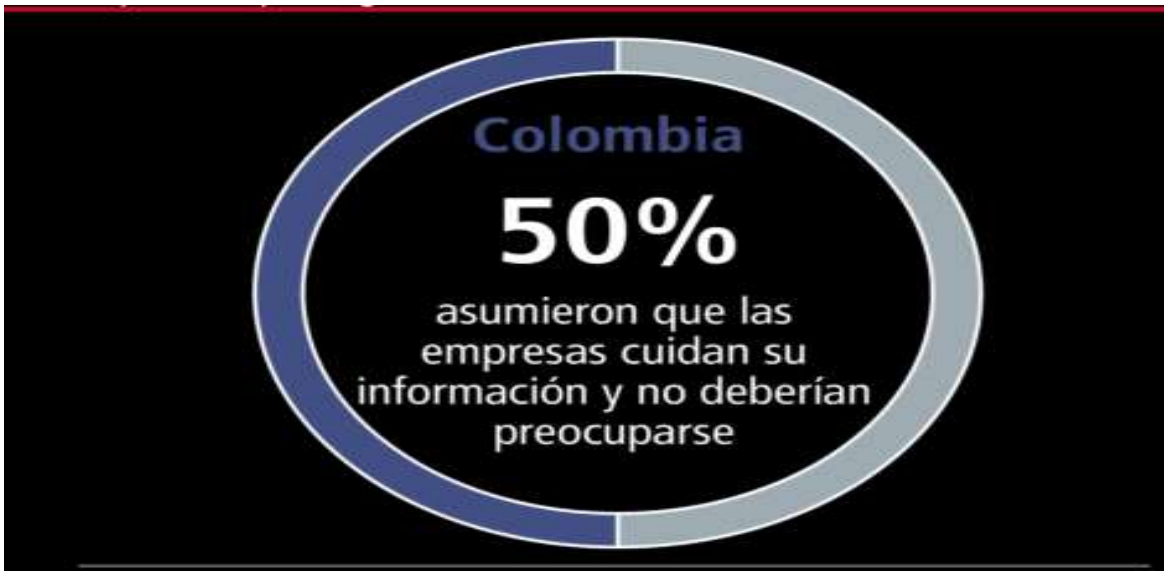
[93] Estudio de GSMA sobre las actitudes relacionadas con la privacidad de los usuarios móviles en Colombia.

Imagen 13 : Los usuarios de internet móvil



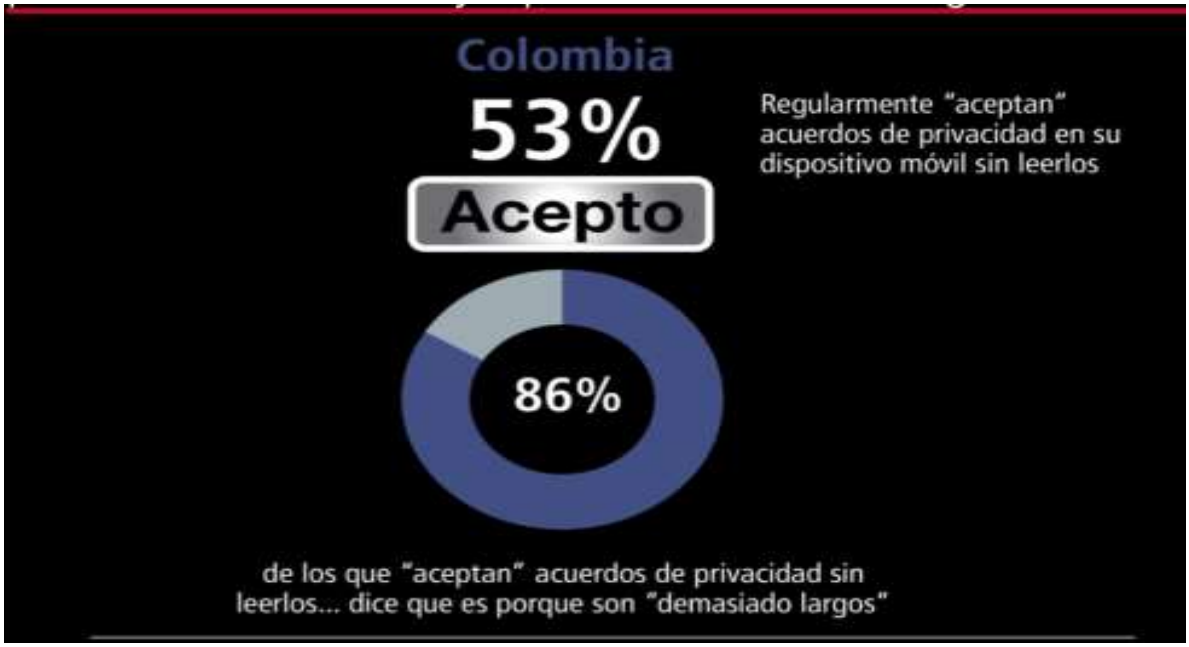

Los usuarios tienen preocupaciones de privacidad y quieren saber que su información está segura. FUENTE: (GSMA, 2013)

Imagen 14 : Los usuarios móviles asumen protección de su información




Menos de la mitad de los usuarios móviles asumen que las empresas protegen su información; Fuente: (GSMA, 2013)

Imagen 15 : Los usuarios y los acuerdos de privacidad sin leerlos.




Los usuarios no leen los acuerdos ya que son "demasiado largos" información Fuente: (GSMA, 2013)

La GSMA ha estado trabajando con todo el ecosistema móvil, incluyendo fabricantes de dispositivos, proveedores de sistemas operativos, desarrolladores de aplicaciones y las redes sociales, además que con las empresas proveedoras de Internet.

A través de la iniciativa de Privacidad GSMA Mobile, el objetivo central es ayudar a establecer pautas universales y enfoques que permitan a los usuarios consumidores de la tecnología móvil un grado de confianza con respecto a la privacidad.

Con este estudio se puede observar que la privacidad aunque es una preocupación, el usuario no se encuentra consiente de los riesgos que corre al compartir su información personal sensible; además, la GSMA en enero del 2011 publicó una serie de principios de privacidad móvil, que son los principios de privacidad universales que indican de qué manera podría respetarse y protegerse

la privacidad de los usuarios de dispositivos móviles, también han publicado un conjunto de directrices para el Diseño de Privacidad en el desarrollo de Aplicaciones Móviles, donde lo que se quiere es articular los principios de privacidad con los dispositivos (fabricantes de dispositivos móviles), las aplicaciones (desarrolladores de Apps) y las plataformas (empresas de sistemas operativos) con los responsables de recopilar y procesar la información personal (Operadores móviles, anunciantes, empresas), adoptando el enfoque de "Privacidad por Diseño"[94], reconociendo que la privacidad debe ser desde un inicio del diseño de las aplicaciones y buscando que el usuario tenga una mayor conciencia y familiaridad con las formas de administrar la privacidad en la red (GSMA, Móviles y Privacidad, 2012).

### *5.2.8 Consideraciones para el programa BYOD según Gartner.*

Gartner ha desarrollado la metodología del BYOD sobre políticas de dispositivos móviles. Con la disponibilidad de los mismos y facilidad para su manejo, en la vida empresarial la tendencia es que los empleados utilicen sus dispositivos móviles para acceder a los recursos de información de la empresa, debido a que cada día los equipos institucionales se encuentran con más políticas restrictivas y más lentos que los dispositivos móviles con los que pueden contar los empleados, en un alto porcentaje son de última tecnología.

La Metodología del BYOD en la empresa, es precisamente aprovechar ésta tendencia y al poderse implementar es necesario tener presentes algunas consideraciones:

- **Opciones de implementación**: dispositivos de propiedad del empleado o un dispositivo híbrido entre la propiedad del empleado y de la compañía.

[94] En el apartado de Privacidad se referenciaron los autores que han propuesto la directriz de "Privacidad por Diseño"

- **Administración de dispositivos móviles**: Solución de seguridad móvil y administración del dispositivo que mantiene la privacidad del empleado.
- **Plan de administración**: Responsabilidad del empleado de administrar el proveedor, plan de datos y gastos incurridos.
- **Estrategia de rembolso**: Una mensualidad para empleados que usan sus dispositivos para uso corporativo, con respecto a la adquisición del equipo.

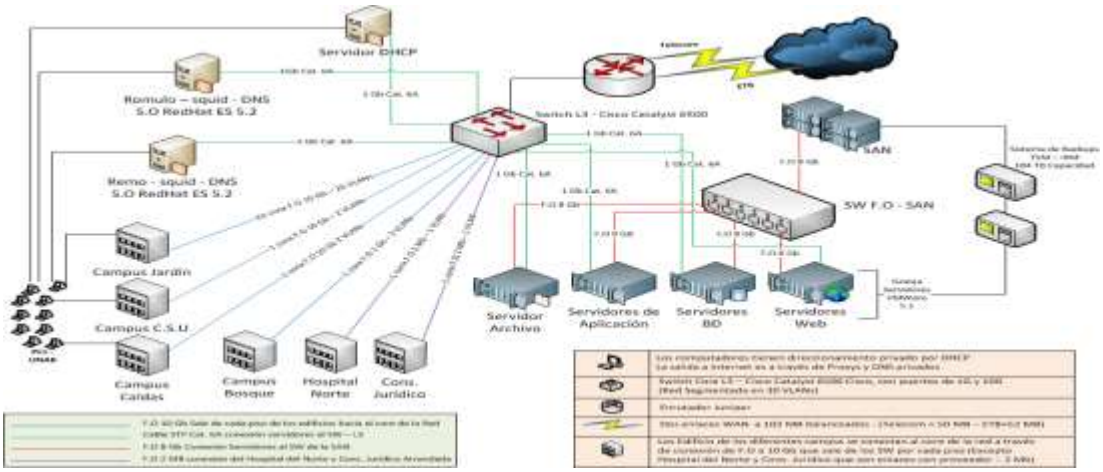
## 5.3 RESULTADO DE PRUEBAS

### *5.3.1 Diseño del Ambiente Sensible para la Prueba*

Como parte de la Fase 3 correspondiente a la aplicación, a continuación describe el diseño del contexto propuesto para realizar las pruebas de control de seguridad y privacidad con la herramienta seleccionada.

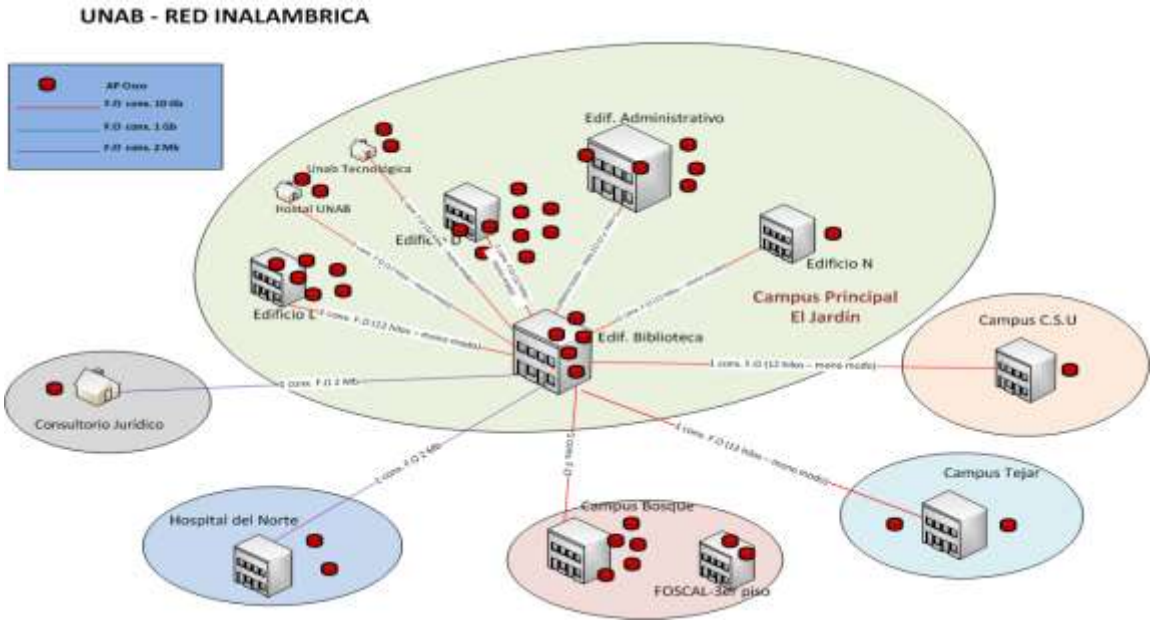
El contexto propuesto para realizar las pruebas fue el campus la Universidad Autónoma de Bucaramanga – UNAB, por ser un ambiente hibrido en donde los usuarios tienen diferentes tipos de perfiles y por consiguiente diferentes niveles de seguridad y privacidad.

Imagen 16 : Topología Red Física UNAB




Fuente: UNAB

Imagen 17 : Red inalámbrica – UNAB




Fuente: UNAB

Los perfiles que se pudieron identificar para realizar los respectivos casos de uso para la aplicación de políticas de seguridad y privacidad son:

**Perfil estudiante**: Corresponde a los estudiantes de pregrado y posgrado de la universidad, para quienes se les define un control de acceso mediante autenticación por control de dirección MAC de sus dispositivos móviles y control de acceso solo a las plataformas académicas que ofrece la institución. Este control de acceso pudo definirse también por medio de un autenticado, un servicio LDAP o Directorio Activo, por ejemplo.

**Perfil docente**: Corresponde a los docentes de la universidad, para quienes se les define un control de acceso mediante autenticación por control de dirección MAC de sus dispositivos móviles y control de acceso solo a las plataformas académicas y administrativas que ofrece la institución. Este control de acceso pudo definirse

también por medio de un autenticado, un servicio LDAP o Directorio Activo, por ejemplo.

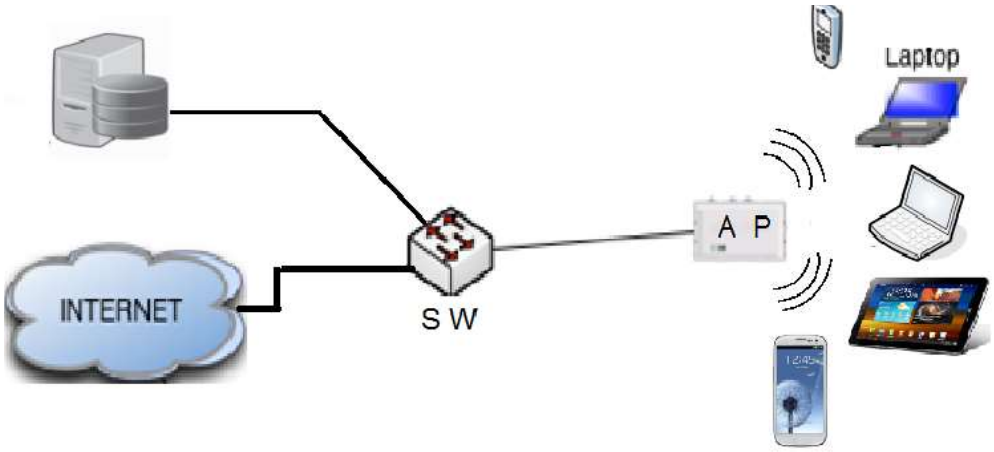
**Perfil administrativo**: Corresponde a los empleados administrativos de la universidad, para quienes se les define un control de acceso mediante autenticación por control de dirección MAC de sus dispositivos móviles y control de acceso solo a las plataformas administrativas que ofrece la institución. Este control de acceso pudo definirse también por medio de un autenticado, un servicio LDAP o Directorio Activo, por ejemplo.

**Perfil invitado**: Corresponde a las personas externas a la universidad que no tienen ningún tipo de vinculación y que asisten a las instalaciones de la institución en calidad de visitantes, a este tipo de perfil se autenticará mediante control de dirección MAC de sus dispositivos móviles y se ofrecerá control de acceso solo a navegación a sitios web institucionales públicos y navegación a Internet. Este control de acceso pudo definirse también por medio de un portal cautivo como un servidor RADIUS.

**Diseño de la topología de red para la prueba**

El siguiente es el diseño que corresponde al ambiente controlado en donde se implementó el modelo de sistema de control de seguridad y privacidad, dado que no fue posible realizar las pruebas en el ambiente de producción de la Universidad por el impacto que estas políticas pueden causar en la operación diaria de los diferentes usuarios.

Imagen 18 : Prototipo Topología red para PacketFence para la prueba




Fuente Autora del proyecto

**Descripción de la topología de red diseñada**

La topología de red diseñada para modelar el sistema de control de seguridad y privacidad de la Universidad Autónoma de Bucaramanga, se basa en el diseño a escala de la topología estrella que tiene la universidad en donde se cuenta con un Switch como dispositivo Core de la estrella y desde el cual se irradia la conectividad.

En el modelo diseñado de la topología los elementos se resumen a un solo:

- **Switch Core:** que permitirá la concentración de la conectividad de todos los elementos activos de la red.
- **Servidor**: Tendrá instalada y configurada la aplicación PacketFence que permite la creación de políticas de control de acceso y seguridad, igualmente ofrecerá los servicios de DHCP y portal cautivo para los dispositivos inalámbricos.
- **Access Points**: son los dispositivos activos de red que permiten propagar la señal de conectividad a la red inalámbrica a los dispositivos móviles de los usuarios.

- **Equipos finales**: Son todos los dispositivos finales de los usuarios que se conectarán a la red inalámbrica de la red diseñada (smartphones, tablets, Laptops, entre otros).

Se instalará PacketFence que es totalmente compatible, confiable de libre acceso a red fuente NAC. PacketFence cuenta con un conjunto de características potente con opciones de gestión de BYOD, y se puede utilizar para asegurar de manera eficaz a redes de cualquier tamaño y heterogéneas, constituyéndose en una solución confiable para redes inalámbricas en contextos sensibles.

Imagen 19 : Foto evidencia del servidor y un usuario final


Foto tomada como evidencia del equipo servidor y un usuario final del ambiente de estudio con PacketFence.

### *5.3.2 LABORATORIO*

Una vez instalado el todo el prototipo de red y el PacketFence se encuentra listo se procede a realizar unas pruebas.

El portátil que actúa como servidor es un HP T6400

Cliente1 - Se conecta un pc Lenovo x230

Switch TP-LINK SF100BD

AP Apple airport

Todo se conecta contra el switch (ap-portatil cliente-portatil server)

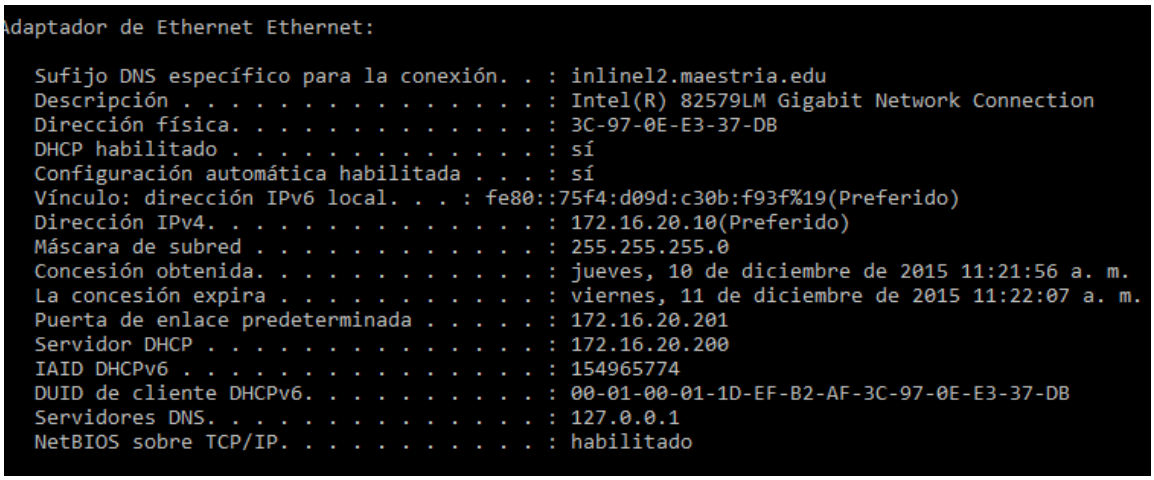
usuario= root

password= Maestri4

usuario= maestria

passwd= 1234567

Imagen 20 : Evidencia de Conexión del Servidor




Como se observa en la imagen se le está entregando datos del servidor que pertenece al rango creado por DHCP y se muestra que el servidor DHCP y el GATEWAY es el servidor PacketFence con sus IP 200 y 201

Para que PacketFence permita la navegación en el cliente este debe haber sido creado previamente, de lo contrario genera el siguiente mensaje al intentar navegar en el cliente

Imagen 21: Mensaje de Error de conexión


Para crear el usuario para permitir la navegación se siguen los siguientes pasos. En el menú superior, opción users / créate

Imagen 22 : Evidencia de creación de usuarios

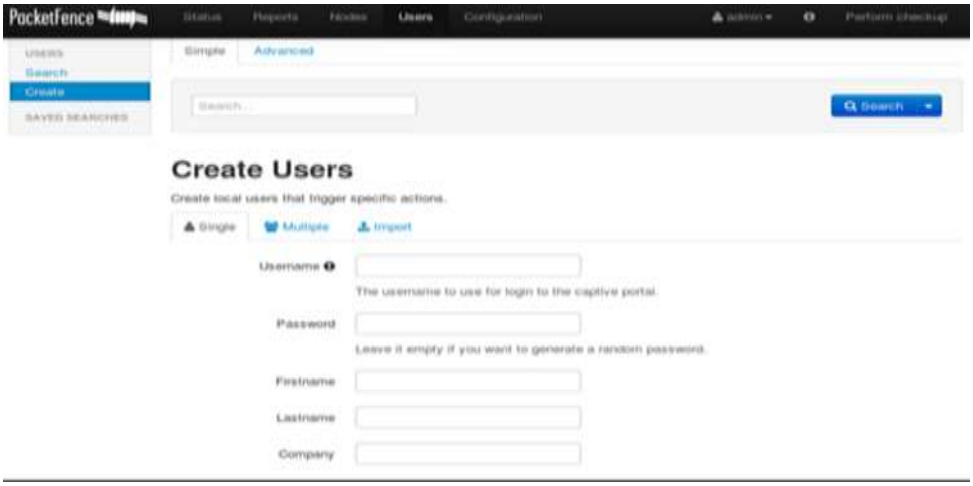


Imagen 23 : Evidencia de crear usuarios

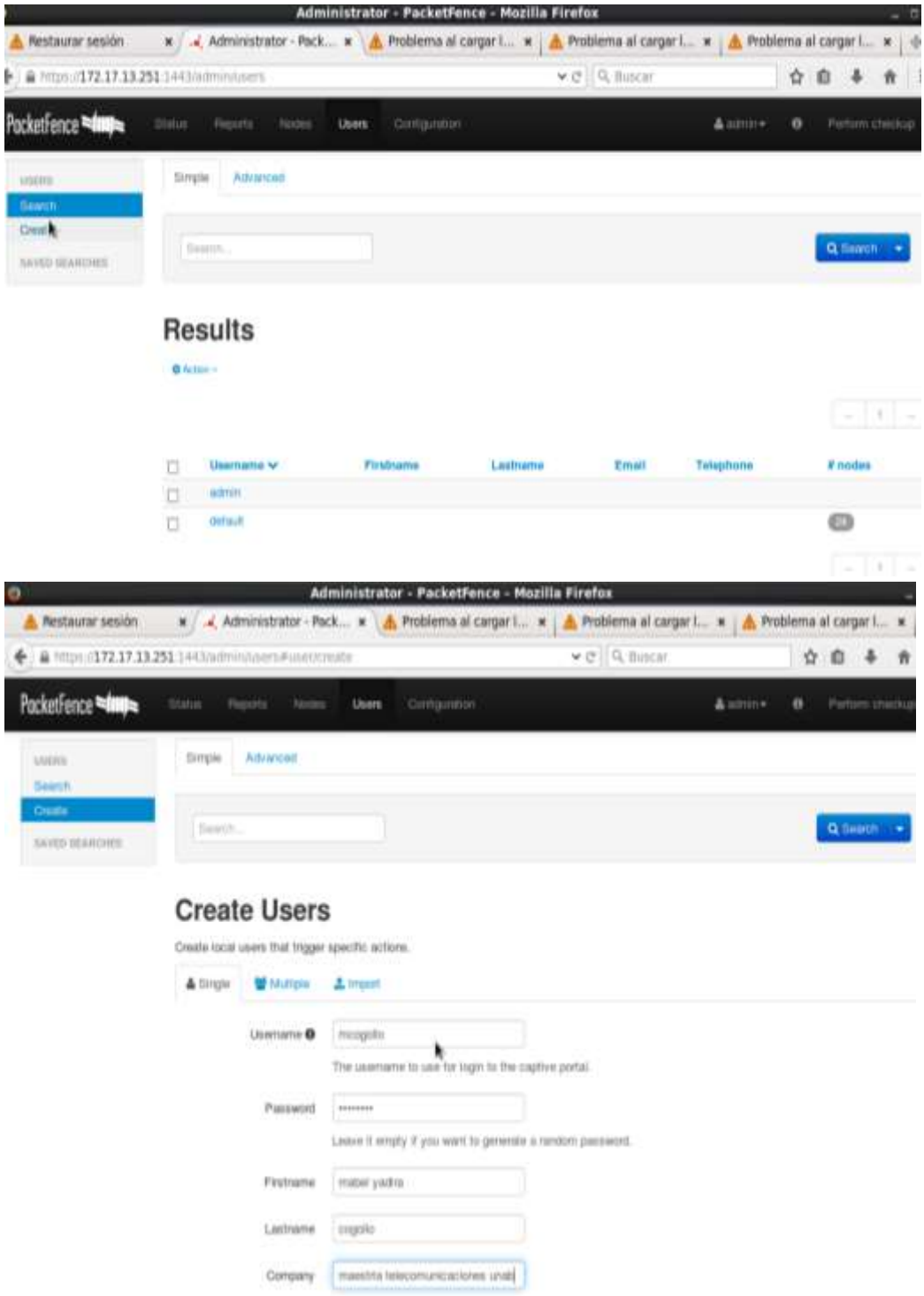
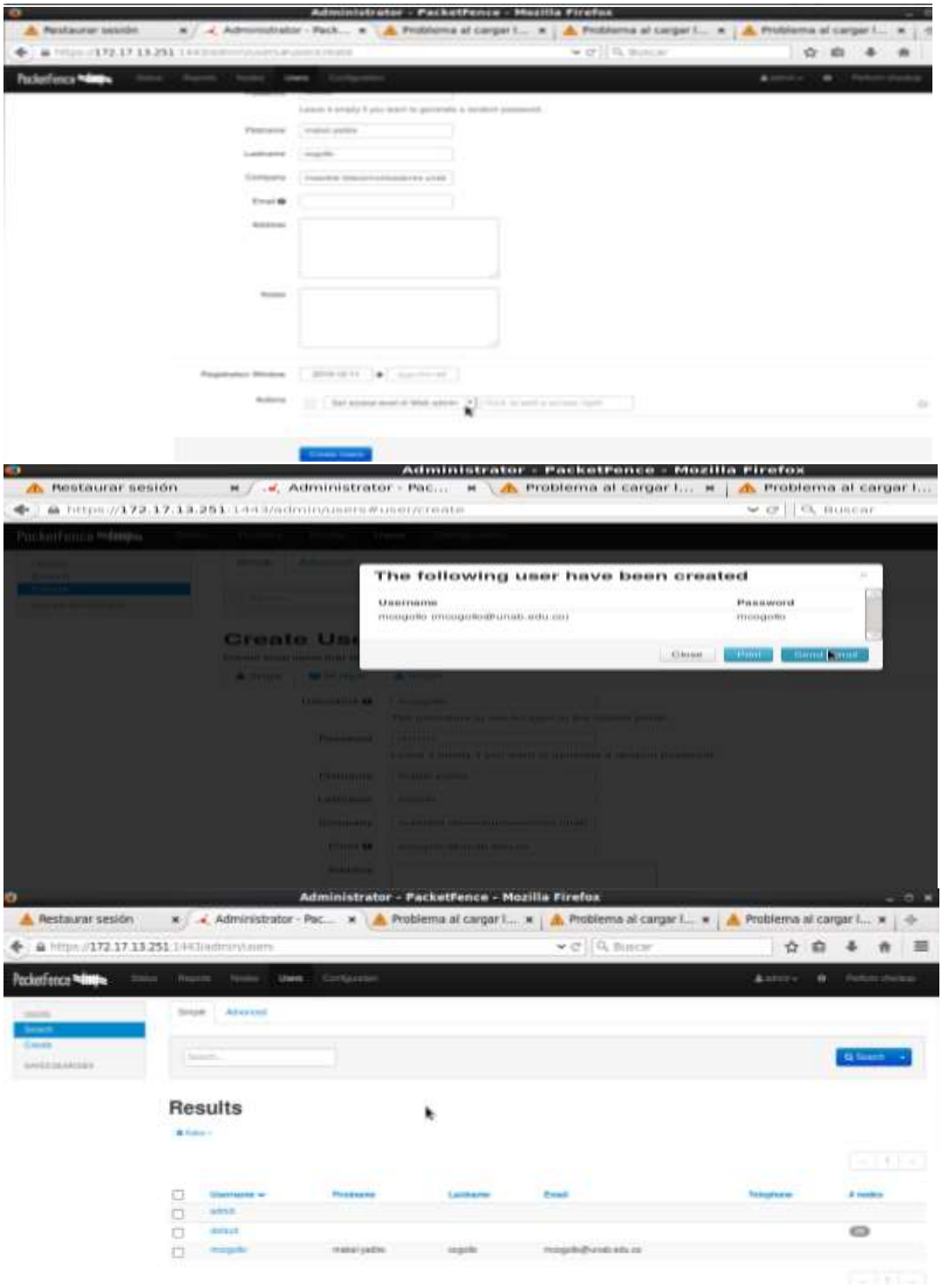


Imagen  24 : Evidencia crear usuarios todo el proceso



Cuando el PC trata de Iniciar Sesión sin haber sido registrado se muestra dentro de los nodos inactivo como se observa en la siguiente imagen

Imagen 25 : Evidencia Autenticando el usuario

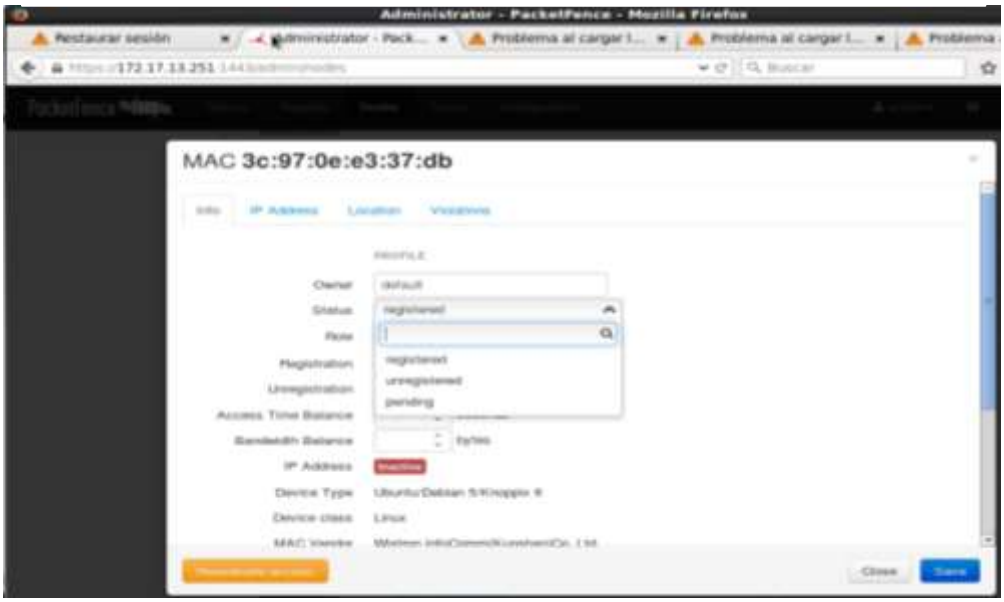



Imagen 26 : Evidencia de usuario sin autenticarse a la red

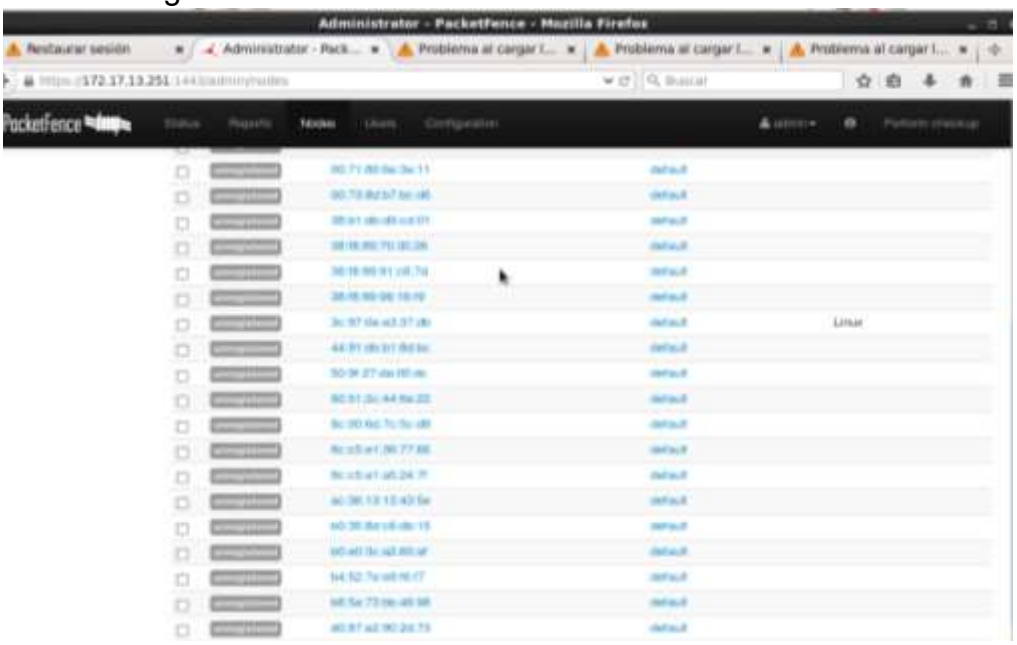
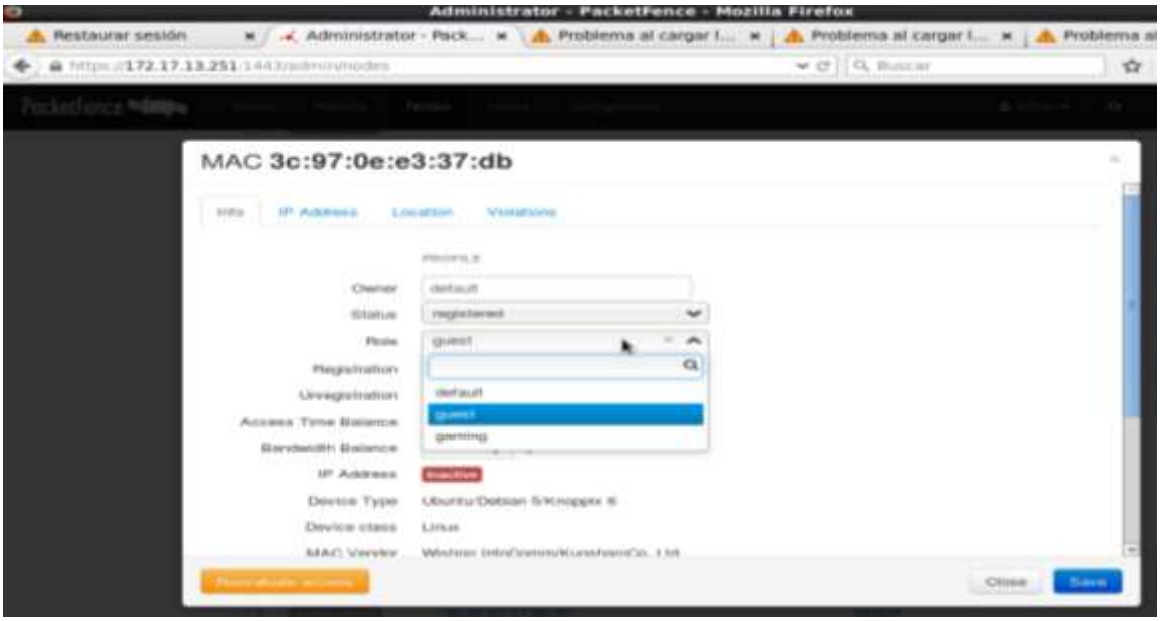


Imagen 27: Se verifica la autenticación del usuario y muestra la dirección MAC




Una vez se agrega el PC a las máquinas permitidas se muestra como PC activo para navegar

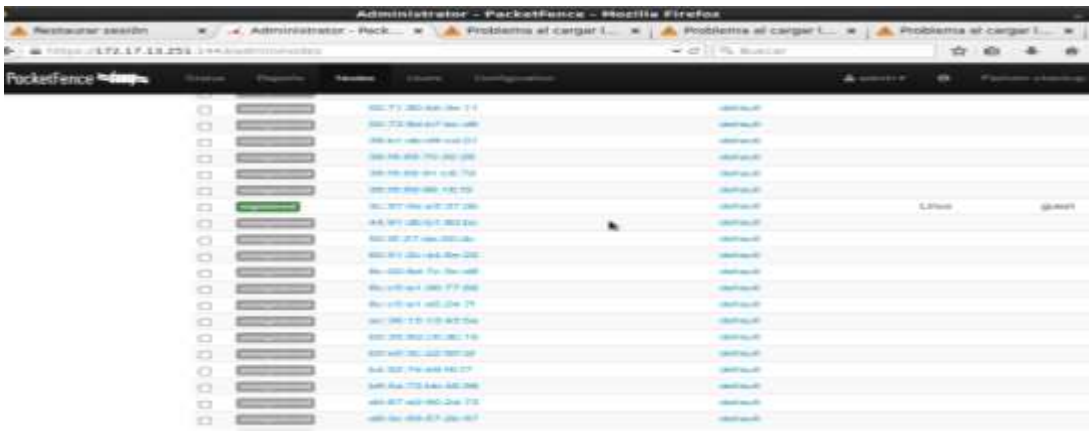
Como se observa en la imagen anteriormente mostrada la MAC del PC es

```
Dirección física. . . . . : 3C-97-0E-E3-37-DB
```

Cuando se abre el navegador del PC solicita la validación del usuario que debe haber sido creado antes por el PacketFence.

### *5.3.3 Pruebas en PC*

Imagen 28: Evidencia de prueba en PC



En la siguiente prueba se evidencia que PacketFence interrumpe la navegación del portal cautivo a través de un interfaz web; para que el usuario se registre

Una vez que el usuario ha iniciado sesión correctamente puede navegar sin problema.

Imagen 29: Evidencia de Autenticación del usuario

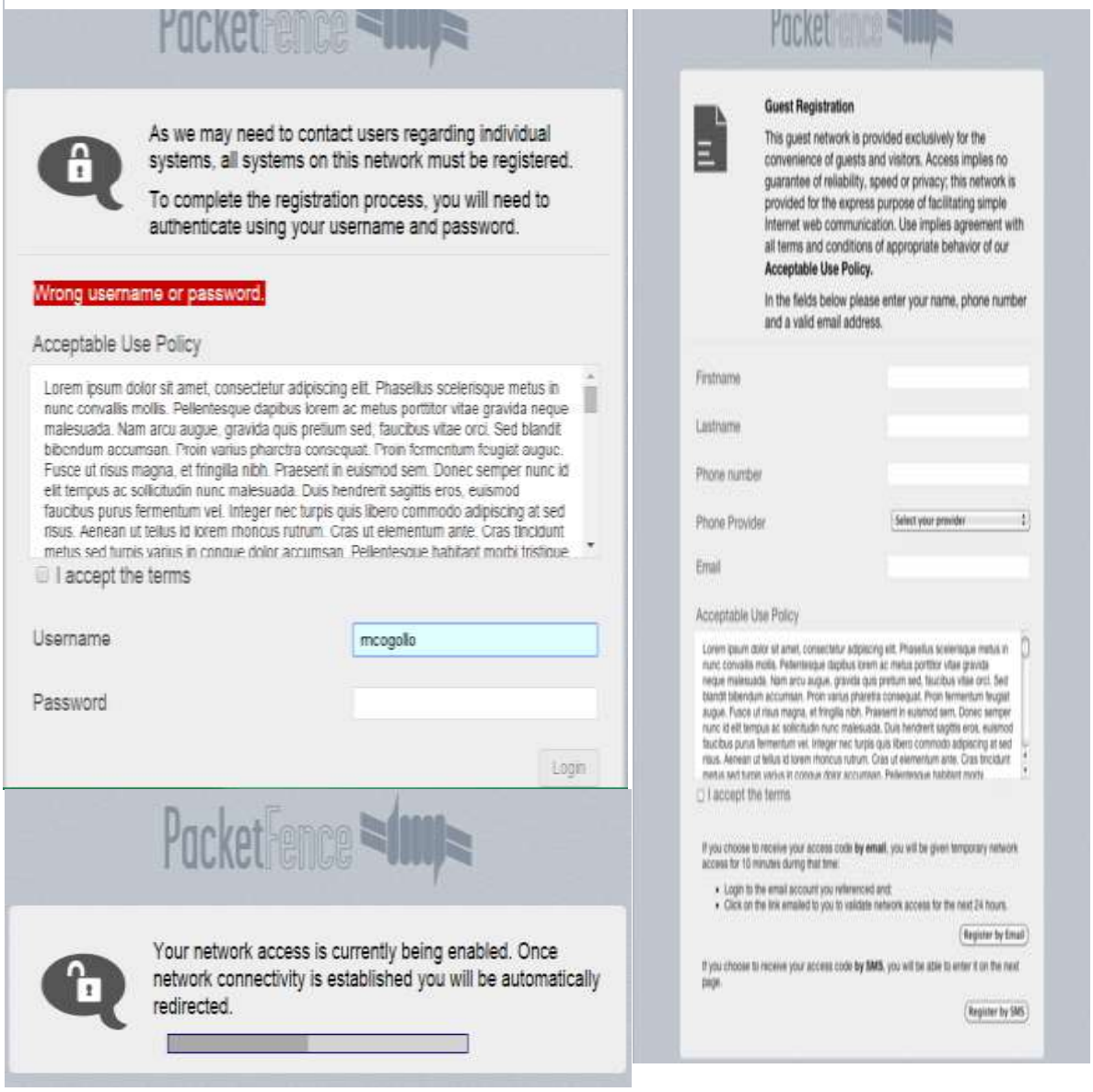
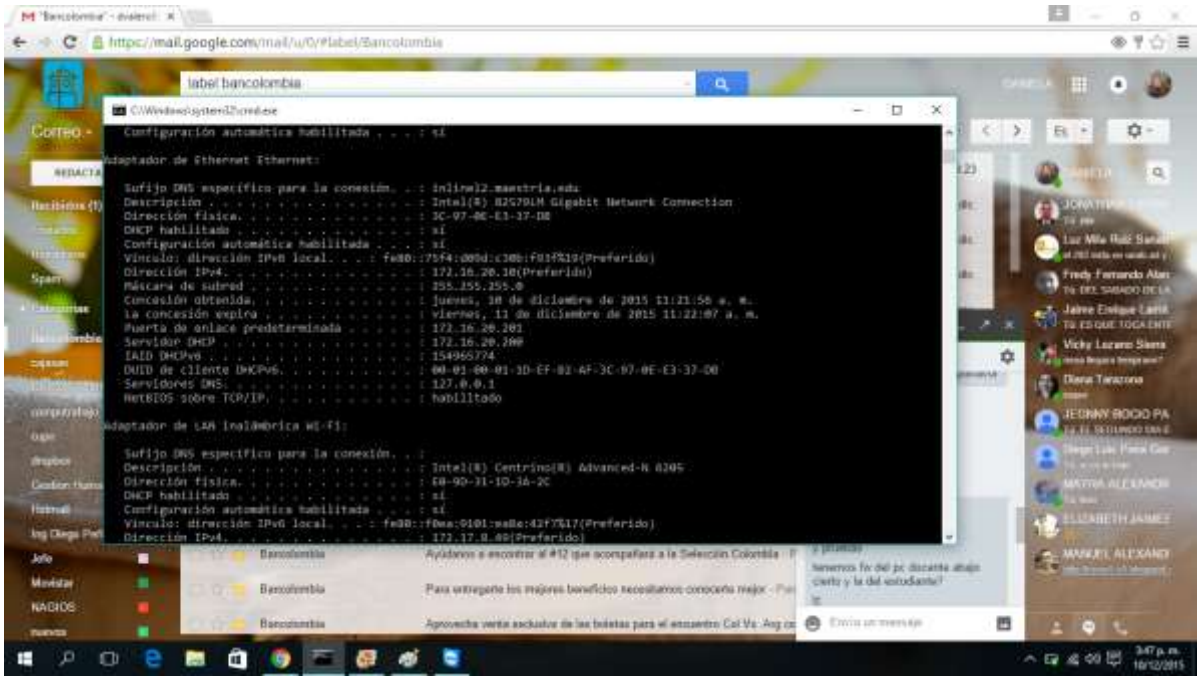


Imagen 30: Evidencia Pc navegando ya en la red con filtro



### *5.3.4 Pruebas en Celulares y Dispositivos Móviles*

Imagen 31: Evidencia en conexión a Celular

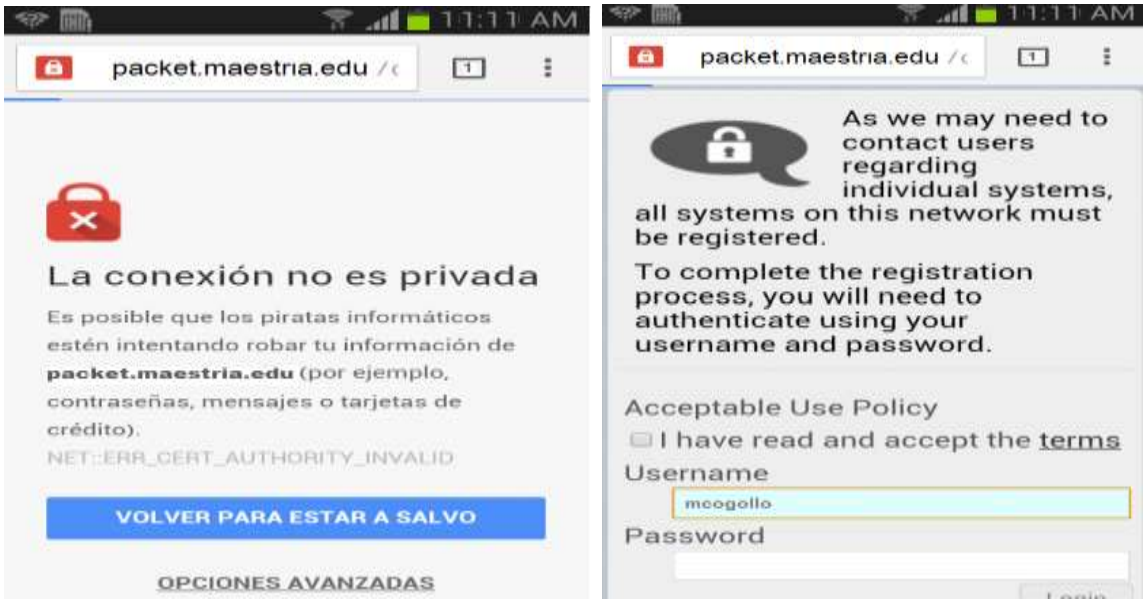
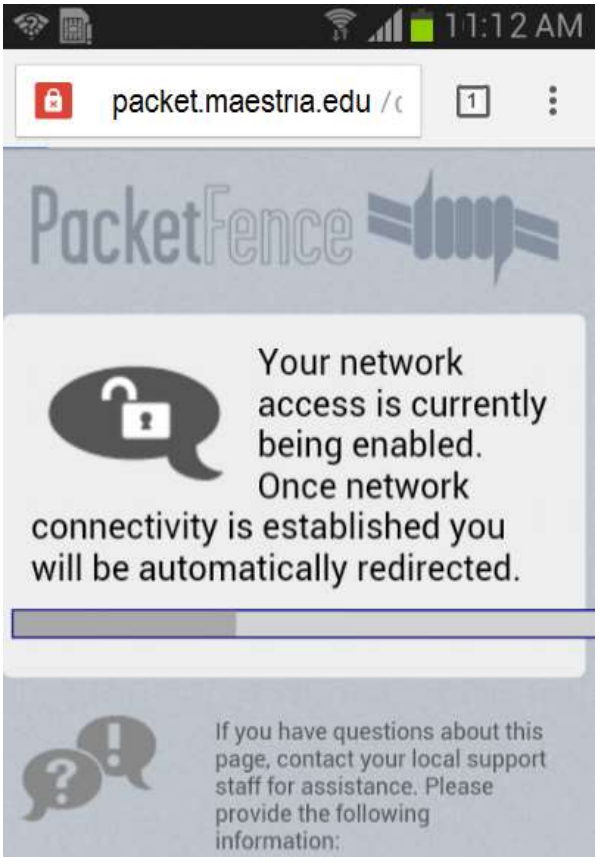


Imagen 32 : Evidencia Conexión en Celular




### *5.3.5 Resultados de las Pruebas*

Se llega a concluir que para la empresa el autenticar a los usuarios permite una mayor seguridad de sus datos y una mayor privacidad a sus usuarios, debido a que se pueden gestionar los usuarios por perfil, por intereses, por departamentos entre otros. Dentro de los resultados se estableció la posibilidad de tener VLANs por grupo.

Como se mencionaba en un apartado anterior, puede existir seguridad sin privacidad, pero no puede existir privacidad sin seguridad, en el caso de BYOD se puedo observar que esta metodología está orientada no solo a ofrecer seguridad a las redes cableadas e inalámbricas de una organización, sino que también tiene en cuenta el manejo de la privacidad de los usuarios por medio de mecanismos que permiten controlar el flujo de información entrante y saliente, así como

mecanismos que permiten borrar información crítica de forma remota para una organización en el evento que un dispositivo móvil sea sustraído sin autorización.

Igualmente se puede observar que BYOD está orientado a ofrecer mecanismos que permitan implementar políticas de seguridad y privacidad orientadas a salva guardar la información de las organizaciones, pero no está orientada a salva guardar específicamente la información y privacidad principalmente del usuario final.

BYOD es una técnica que demanda un alto grado de capacitación de personal técnico y concientización en buenas prácticas para el manejo de los recursos tecnológicos móviles en la empresa.

### *5.3.6 Esquema resumen del ambiente Smart Campus con BYOD*

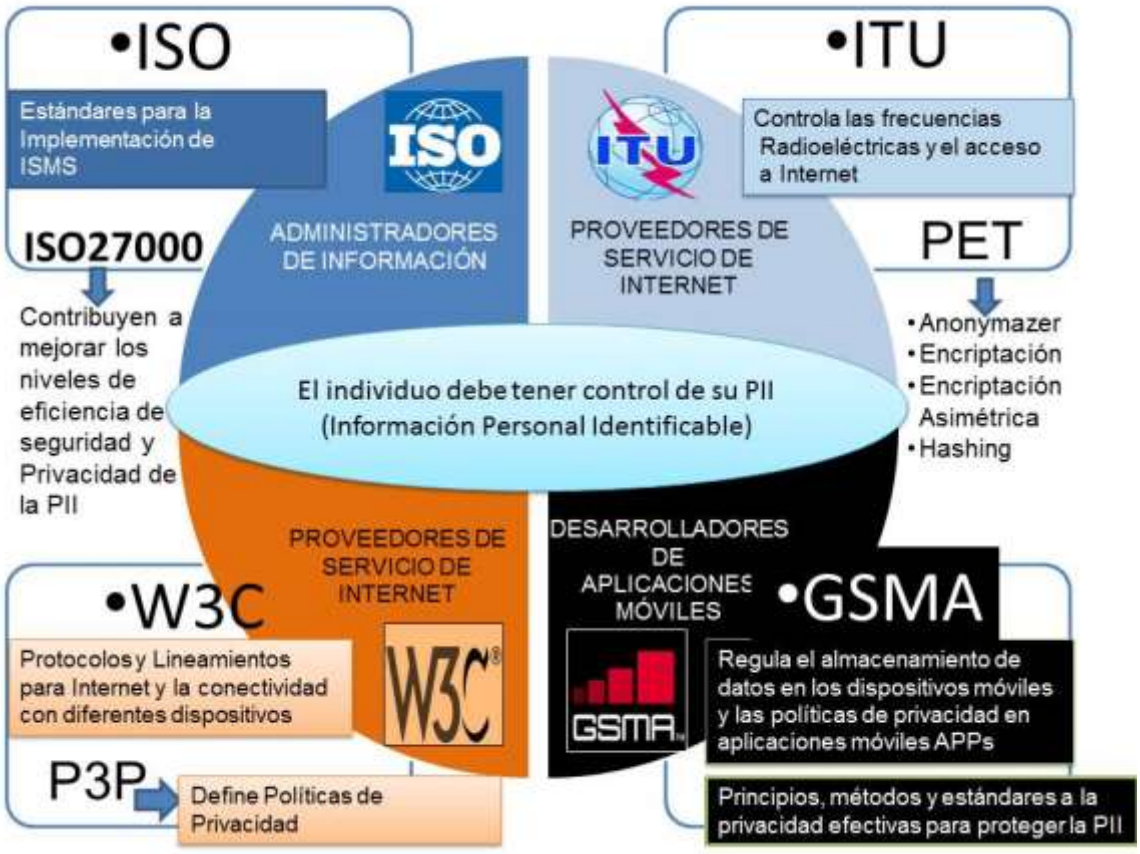
Teniendo en cuenta la literatura consultada, la aplicación de la prueba y los resultados obtenidos, se elaboró el siguiente esquema destacando los aspectos más relevantes a tener en cuenta en la implementación de la solución de la privacidad en entornos sensibles para un Smart Campus, como el que se proyecta en el presente documento para la Universidad Autónoma de Bucaramanga. Se describen los principios y la taxonomía de la privacidad, planteados por Westin y Solove, respectivamente; se referencian las organizaciones internacionales encargadas de la regulación y estandarización de las prácticas de privacidad y los entornos sensibles.

Así mismo, se hace un paralelo entre el Smart Campus y la Smart City y su relación implícita. Finalmente se evalúa el impacto y la necesidad de la implementación del programa BYOD en la optimización de los procesos al interior

de una compañía, compatible con las exigencias de una institución de educación superior como la Universidad Autónoma de Bucaramanga.

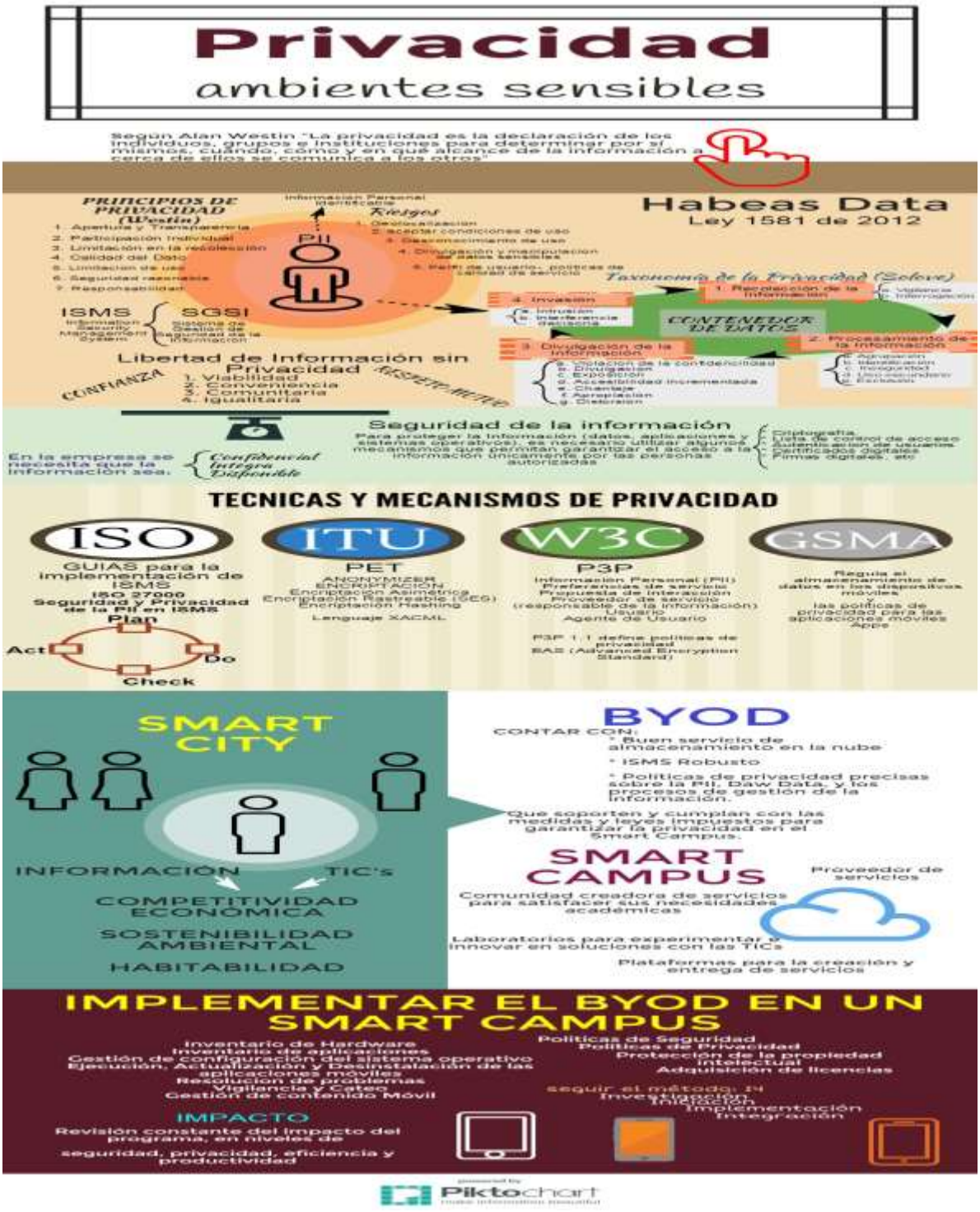
Imagen 33: Esquema de Privacidad

**Esquema Propuesto que enmarca técnicas, estándares, protocolos y políticas de privacidad en ambientes inteligentes - Smart Campus - con BYOD y los actores involucrados**




Fuente Autora del Proyecto

Imagen 34: Infografía que permite la descripción del estudio del proyecto




Fuente: propia autora proyecto

# 6 CONCLUSIONES

La privacidad es un concepto que corresponde a distintas apreciaciones, dependiendo de la disciplina que lo adopta como objeto de estudio. En el campo de las tecnologías de la información y las comunicaciones, la privacidad comprende diversos procesos que influyen sobre la capacidad decisoria del usuario, la arquitectura de las plataformas, redes y entornos sensibles, destacando su importancia en la constante generación de contenidos, que circulan por la World Wide Web. De acuerdo con los planteamientos de Westin y Solove, literatura revisada en el presente documento, la privacidad ha pasado de ser una noción y una percepción a ser una solución fundamental para la implementación de entornos sensibles, ya sea en redes públicas o privadas, ya que para robustecer la seguridad en una red es vital proteger las libertades individuales empezando por su PII, siguiendo con su interacción entre usuarios y el control de los datos que ejerza el administrador de la red.

Para implementar correctamente las técnicas y mecanismos presentados en nuestra propuesta de trabajo, la institución debe regirse por los estándares y parámetros de los entes internacionales de control de tecnologías de información y comunicaciones siendo ISO, ITU, W3C y GSMA, los líderes mundiales.

La arquitectura de todo contexto sensible debe atender a los principios de privacidad, a la regulación jurídica del país de origen, y a las técnicas de privacidad que cuentan con un respaldo internacional. De igual manera, toda entidad que posea un contexto sensible debe contar con un soporte técnico calificado y visible en un proveedor de servicio certificado, que cumpla con los requerimientos de confidencialidad, integridad y disponibilidad de la información generada y contenido en dicho entorno.

BYOD es una solucion empresarial para la optimizacion de los procesos que tienen lugar en una institucion o compañía. Sin embargo, el desconocimiento de las actividades colaterales como la implementación de las políticas y mecanismos de privacidad, impide llevar a buen termino el propósito del programa en que sólo se enfoca en la información empresarial y su seguridad, dejando de lado la privacidad de los usuarios que entran a ser uso de los aplicativos de la empresa. Por lo tanto, su implementación debe ser compatible con las políticas de seguridad, las políticas de privacidad, y el software utilizado para la gestion y control de acceso en la red.

El NAC no es un producto, es un proceso basado en el Hardware, el Software y las dinámicas entre los participantes en la red. Dicho proceso, al incorporarse a un entorno sensible y al integrarse con otras plataformas de seguridad debe contar con un motor de servicios de identidad que permite la completa visibilidad de las terminales y la deteccion de comportamientos que vulneren la seguridad de los usuarios.

Las aplicaciones de tipo Open Source representan una gran ventaja para la constitucion de redes de trabajo asociado al interior de la universidad, entre los miembros de la comunidad educativa que continúen con el propósito del presente trabajo, ya que el codigo abierto posibilita robustecer el software, ademas de las funciones que desempeña en la red. Esto es un factor relevante que facilita el acoplamiento entre la aplicación y las necesidades de la institucion. No obstante, el soporte tecnico del mismo, podria haberse limitado a la falta de un respaldo visible en un proveedor de servicios.

La implementación de un entorno sensible en cualquier tipo de empresa debe atender a las exigencias planteadas por los estándares y reportes publicados por las organizaciones internacionales, ISO, ITU, W3C y GSMA, encargadas de la

regulación y control de la privacidad en los ambitos de plataformas, dispositivos, y aplicaciones. Si bien, una red, una plataforma o una aplicación, atienden directamente a los requerimientos técnicos, la empresa debe encargarse de hacerlos compatibles y adaptables a sus necesidades directas. El funcionar bajo una normatividad representa, además de beneficios al ser referenciados o auditados, pertenecer a una red de intercambio de conocimientos que permitirá a la compañía liderar procesos de investigación y renovación en su entorno inmediato.

# 7 RECOMENDACIONES

- BYOD como una estrategía para la implementación de políticas de seguridad para las organizaciones, ha tenido un desarrollo vertiginoso en los diferentes mecanismos que se pueden implementar para ofrecer control y seguridad de la información, desarrollada por múltiples fabricantes encontrando desde los comerciales hasta los de Open Source. Lo anterior permite continuar con la evaluación de las diferentes soluciones que existen y poder establecer una metodología que permita ser referente a las organizaciones para su adopción, teniendo en cuenta la inclusión de los mecanismos y técnicas de privacidad propuestos en el presente documento.

- La optimización de los procesos debe estar orientada a la valoración positiva de las nuevas tecnologías; la UNAB, al implementar el programa BYOD, debe hacer una transición efectiva teniendo en cuenta el acompañamiento y capacitación de su personal, la adopción de las políticas, técnicas y mecanismos de privacidad vigentes, y el robustecimiento de su infraestructura tecnológica. Para la puesta en marcha de su Smart Campus es necesario realizar una prueba piloto que permita definir los aspectos técnicos requeridos para su funcionamiento efectivo, teniendo en cuenta las apreciaciones presentadas en el documento.

- De acuerdo con las afirmaciones de Miller, un espacio privado permite un espacio público civilizado, por lo tanto, la interacción entre los usuarios en un entorno sensible debe estar orientada a la protección de las libertades individuales. La UNAB como institución de educación superior, debe liderar estos procesos de renovación tecnológica favoreciendo el bien común, con miras a proyectar la vinculación entre su Smart Campus y la arquitectura

Smart City de su ciudad. Para éste caso de estudio, Bucaramanga, una de las 7 ciudades del futuro en Colombia según Findeter y el BID, es un territorio propicio para fortalecer el trabajo conjunto entre la universidad y la ciudad.

- La UNAB debe destinar recursos para el apoyo de la investigacion en Smart Cities, liderando el proyecto de transformación urbana en Bucaramanga, con el advenimiento de las ciudades inteligentes y las vías de cuarta generación en nuestro pais. La integración de la industria con la academia, definiendo las condiciones de seguridad de redes y las políticas de privacidad en la gestión de la PII permitirá ampliar la valoración positiva de las TIC por los habitantes y el recurso humano.

- La elección del proveedor de servicios de Control de Acceso a la Red, debe garantizar la sostenibilidad de la red de conocimiento del Smart Campus en lo que respecta en cuanto a la generacion de contenidos, por lo tanto, el soporte técnico del proveedor elegido debe ser el respaldo para las actividades de la unidad academica. Para este proyecto, trabajar con OpenSource, a manera de proyecto piloto, implicó contemplar los mismos alcances que se pueden obtener con un proveedor visible, que apoye a la institucion, destaca la relevancia de contar con un departamento organizado con personal idóneo que le permita obtener dicho respaldo en la ejecución de sus actividades académicas.

## REFERENCIAS BIBLIOGRÁFICAS


Corporación Colombia Digital . (07 de 04 de 2015). Teletrabajo en Catastro Distrital, un nuevo avance. Obtenido de Aumentar la productividad, mejorar la movilidad empresarial y virtualizar las compañías son algunos beneficios de adoptar esta modalidad.: http://colombiadigital.net/actualidad/noticias/item/8237-teletrabajo-en-catastro-distrital-un-nuevo-avance.html

Intelligent Community Forum (ICF). (11 de 2015). *The Smart21 Communities - Smart 21 of 2016*. Obtenido de Intelligent Communities of the year : https://www.intelligentcommunity.org/index.php?submenu=Awards&src=gendocs&ref=Smart21&category=Events

International Telecommunication Union - ITU. (s.d. de s.m. de 2013). *Protección de datos y privacidad en la nube ¿Quién es el propietario de la nube?* Obtenido de https://itunews.itu.int/Es/3702-Proteccion-de-datos-y-privacidad-en-la-nube-BR-Quien-es-el-propietario-de-la-nube.note.aspx

World Wide Web Consortium (W3C). (3 de 12 de 2015). *W3C Standards*. Obtenido de http://www.w3.org/standards/webofdevices/

Abown, G. (2012). Towards a Better Understanding of Context and Context-Awareness. *Proc. 1st international symposium on Handheld an Ubiquitous Computing. Springer-Verlag, Londres*, 304-307. Obtenido de ftp://ftp.cc.gatech.edu/pub/gvu/tr/1999/99-22.pdf

Access to European Union Law. (23 de 11 de 1995). *Official website of the European Union*. Obtenido de Diario Oficial n° L 281 de 23/11/1995 p. 0031 - 0050: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:31995L0046

Ackerman, M., Darrell, T., & Weizner, D. (2001 ). *Privacy in Context.* Human-Computer Interaction.

Aguilera López, P. (2010). *Seguridad Informática.* Barcelona: Editex. Obtenido de https://books.google.com.co/books?isbn=8497717619

Aguillón Martínez, E. (2012). *Fundamentos de Criptografía.* México: UNAM, Laboratorio de Redes y Seguridad. Obtenido de http://redyseguridad.fi-

p.unam.mx/proyectos/criptografia/criptografia/index.php/1-panorama-general/13-servicios-y-mecanismos-de-seguridad/131-servicios-de-seguridad

Asamblea Nacional Constituyente (1991). (1991). *Constitución Política de Colombia 1991.* Bogotá: República de Colombia. Obtenido de http://www.procuraduria.gov.co/guiamp/media/file/Macroproceso%20Disciplinario/Constitucion_Politica_de_Colombia.htm

Asamblea Nacional Constituyente 1991. (2006). *Nueva Constitución Política de Colombia 1991.* Bogotá: Unión Ltda. Obtenido de http://www.procuraduria.gov.co/guiamp/media/file/Macroproceso%20Disciplinario/Constitucion_Politica_de_Colombia.htm

Augusto, J. C., Nakashima, H., & Agh, H. (2010). Ambient Intelligence and Smart Environments:A State of the Art. 1-29.

Bartoli, A., Hernandez-Serrano, J., Soriano, M., Dohler, M., Kountouris, A., & Barthe, D. (2011). Security and Privacy in your Smart City. *Centre Tecnologic de Telecomunicacions de Catalunya (CTTC),Spain - IEEE*, 1-6. Obtenido de http://www.cttc.es/publication/security-and-privacy-in-your-smart-city/

Batty , M., Axhausen, K., Pozdnoukhov, A., Fosca, G., Bazzani, A., Wachowicz, M., . . . Portugali, Y. (2012). Smart Cities of the Future. En C. f. London, *Working Papers Series Paper 188 -Oct 12 Smart Cities of the Future* (págs. 1-40). London: UCL CENTRE FOR ADVANCED SPATIAL ANALYSIS. Obtenido de https://www.bartlett.ucl.ac.uk/casa/pdf/paper188

BBC News. (17 de 01 de 2014). Edward Snowden: Leaks that exposed US spy programme. *BBC NEWS on Internet*. Obtenido de http://www.bbc.com/news/world-us-canada-23123964

BCS. (06 de 2014). *http://www.bcs.org/.* Obtenido de BYOD, CYOD, BYOT, BYOA and more: http://www.bcs.org/content/conWebDoc/52926

Behrooz, A. (01 de 2010). *Privacy of Mobile Users in Contextaware Computing Environments Master of Science Thesis.* Stockholm, Sweden : Royal Institute of Technology Department of Computer and Systems Sciences (KTH Information Communication Tecnology) TRITA-ICT-EX-2011:233. Obtenido de http://www.diva-portal.org/smash/get/diva2:512292/FULLTEXT01.pdf

BeVier, L. R. (1995). Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection. *William & Mary Law Review*, 455. Obtenido de http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1489&context=wmborj

BHERT. (18 de 01 de 2015). *Internet of Everything - Powering the Smart Campus & the Smart City:Geelong's Transformation to a Smart City.* (B. B. Table, Ed.) Obtenido de In parthershio with University Deakin Worldly Australia, Cisco e IBM: http://www.bhert.com/events/2015-06-08/BHERT-Smart-City-Agenda-June-18.pdf

BID. (2015). *Iniciativa CIUDADES EMERGENTES y SOSTENIBLES*. Obtenido de Banco Interamericano de Desarrollo: http://www.iadb.org/es/temas/ciudades-emergentes-y-sostenibles/ciudades-usando-el-enfoque-de-desarrollo-urbano-sostenible,6693.html

Boulton, A. B. (2011). Cyberinfrastructures and "smart" world cities: Physical, human, and soft infrastructures. *In P. Taylor, B. Derudder, M. Hoyler & F. Witlox (Eds.), International Handbook of Globalization and World Cities. Cheltenham, U.K.: Edward Elgar.*

Braverman, B., Braverman , J., Taylor, J., Todosow, H., & Wimmersperg , U. (2014-2015). The Vision of A Smart City. En C. Communication and Policy Engagement (CPE) Team, *Reconceptualising Smart Cities: A Reference Framework for India Compendium of Resources - Parte 1 Smart City Definitions* (pág. 62). India: STEP Center for Study of Science, Technology & Policy. doi:http://www.osti.gov/scitech/servlets/purl/773961 del documento - 2009

Casa editorial El Tiempo. (6 de 09 de 2015). Las fallas de los bancos al reportar a clientes ante DataCrédito. *El Tiempo* , págs. http://www.eltiempo.com/economia/finanzas-personales/reportes-a-datacredito-y-otras-centrales-de-riesgo/14495887.

Cavoukian, A. (sd de 12 de 2013). *Privacybydesing.ca.* Obtenido de Ph.D. Information and Privacy commissioner Ontario, Canada: https://www.ipc.on.ca/site_documents/pbd-byod.pdf

Cio. (4 de 04 de 2012). *http://www.cio.com/*. Obtenido de BYOD: If You Think You're Saving Money, Think Again por Tom Kaneshige:

http://www.cio.com/article/2397529/consumer-technology/byod--if-you-think-you-re-saving-money--think-again.html

Cio. (13 de 06 de 2014). *www.cio.com.* Obtenido de What Is Going Wrong With BYOD? por Tom Kaneshige: http://www.cio.com/article/2375498/byod/what-is-going-wrong-with-byod-.html

CISCO. (2014). *Cisco*. Obtenido de http://www.cisco.com/en/US/products/ps6128/index.html

Cisco. (18 de 10 de 2015). *¿Cómo el RADIUS trabaja?* Obtenido de Cisco Systems Inc.: http://www.cisco.com/cisco/web/support/LA/102/1024/1024966_32.pdf

Cities for Cities, W. C. (Dirección). (2014). *WCCD ISO 37120* [Película]. Obtenido de http://www.dataforcities.org/

Citrix . (7 de 07 de 2015). *Un enfoque realista de la experiencia BYOD.* Obtenido de Alem, Ricardo: http://colombiadigital.net/opinion/columnistas/movilidad-y-tendencias/item/8399-un-enfoque-realista-de-la-experiencia-byod.html

Cole, S. A. (2001). *Suspect Identities: A HISTORY OF FINGERPRINTING AND CRIMINAL IDENTIFICATION.* Cambridge, MA: Harvard University.

Complejo Ruta N. (2012). *Ruta N Medellín Centro de Innovación y Negocios*. Obtenido de EL LUGAR DONDE POTENCIA LA INNOVACIÓN: http://rutanmedellin.org/es/sobre-nosotros

Congdon, P. (2000). *IEEE 802.1X Overview - Port Based Network Access Control,.* Albuquerque, NM,: IEEE Plenary. Obtenido de http://www.ieee802.org/1/files/public/docs2000/P8021XOverview.PDF

Congreso de Colombia. (27 de Junio de 2013). Decreto 1377 de 2013 por la cual se reglamenta parcialmente Ley No. 1581. *Diario Oficial No. 48834*, pág. 28. doi:http://www.sic.gov.co/drupal/sites/default/files/normatividad/Ley_1581_2012.pdf

Congreso de la República de Colombia. (31 de Diciembre de 2008). Ley Estatutaria 1266. *Diario Oficial 47.219 de diciembre 31 de 2008*, pág. s.p. Obtenido de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

Cornella, A. (1999). La infoestructura: Un concepto esencial en la sociedad de la información. (i. p. Scopus, Ed.) *El profesional de la Información - Revista Internaciona Cientifica y Profesional*, 26. Recuperado el 2015, de http://www.elprofesionaldelainformacion.com/contenidos/1999/enero/el_concepto_de_infoestructura.html

Costas Santos, J. (2014). *Seguridad Informática.* España: RA-MA Editorial Retrieve from www.ebrary.com. Obtenido de http://site.ebrary.com.aure.unab.edu.co/lib/unabsp/detail.action?docID=11038505

Cuppens, F., & Cuppens, N. (2007). Modeling Contextual security policies, (2008), pages(285-305). *International Journal of Information Security*, 285-305.

De Angeli, A. (12 de 03 de 2013). Smart students building their campus: A LARGE-SCALE PARTICIPATORY DESIGN. *Smart Campus Lab*, 55. Obtenido de http://disi.unitn.it/~deangeli/homepage/lib/exe/fetch.php?media=teaching:cscw_smart_campus.pdf

Dey, A. e. (1999). CyberDesk: A Framework for Providing Self-Integrating Context-Aware Services. *Knowledge-Based Systems*, 3-13. Obtenido de http://www.cc.gatech.edu/fce/ctk/pubs/KBS11-1.pdf

Dey, A. K. (2001). Understanding and using context. . *Personal and Ubiquitous Computing*, 4-7.

Dhont, J., Pérez Asinari, M. V., & Poullet, Y. (19 de 04 de 2004). Safe Harbour Decision Implementation Study. *European Commission, Internal Market DG*, 23.

Dourish, P. (2004). What We Talk About When Talk About Context. *Personal and Ubiquitous Computing*, 19-30.

Dziedzic, T., & Levien, R. (s.d. de 11 de 2015). *PacketFence Administration Guide.* Obtenido de http:/www.packetfence.org/downloads/PacketFence/doc/PacketFence_Administration_Guide-5.5.2.pdf

Escrivá, G. G., Romero, S. R. M., & Ramada, D. J. (2013). *Seguridad informática.* España: Macmillan Iberia, S.A.. Retrieved from http://www.ebrary.com. Obtenido de

http://site.ebrary.com.aure.unab.edu.co/lib/unabsp/reader.action?docID=10820963&ppg=45

Esquivel, A., Haya, P., Montoro, G., & Alamán, X. (s.f.). UNA PROPUESTA PARA UN MODELO DE PRIVACIDAD EN ENTORNOS ACTIVOS. Obtenido de http://arantxa.ii.uam.es/~montoro/publications/esquivel05propuesta.pdf

ETSI. (2000). *Broadband Radio Access Network (Bran); HIPERLAN Type 2; SYstem Overview.* Sophia Antipolis Cedex - Francia: Etsi TR 101 683 V1.1.1. Obtenido de https://www.etsi.org/deliver/etsi_tr/101600_101699/101683/01.01.01_60/tr_101683v010101p.pdf

Futuresight. (2013). *Resultados Clave de Colombia.* LONDON: GSMA Latinoamérica.

Futuresight, & Theodorou, Y. (2013). *Estudio de GSMA sobre las actitudes relacionadas con la privacidad de los usuarios móviles - Resultado clave en Colombia.* New Fetter Lane London: GSMA.

Gartner. (3 de 01 de 2014). *Magic Quadrant for Enterprise Mobility Management Suites.* Obtenido de Analyst(s): Terrence Cosgrove, Rob Smith, Chris Silva, Bryan Taylor, John Girard, Monica Basso: http://www.creekpointe.com/pdfs/Magic-Quadrant-for-Enterprise-Mobility-Management-Suites.pdf

Gartner. (17 de 12 de 2015). *http://www.gartner.com/.* Obtenido de Bring Your Own Device (BYOD): http://www.gartner.com/it-glossary/bring-your-own-device-byod

Gartner Inc. (s.d. de s.m. de 2015). *Gartner Enterprise*. Obtenido de http://www.gartner.com/technology/about.jsp

González, J., & Rossi, A. (2001). New Trends for Smart Cities." Competitiveness and Innovation Framework Programme.

Gorenflo , G., & Moran, J. W. (10 de 04 de 2010). *The Elements of the PDCA Cycle.* Obtenido de http://www.naccho.org/topics/infrastructure/accreditation/upload/abcs-of-pdca.pdf

GSMA. (28 de 01 de 2012). *Móviles y Privacidad.* Obtenido de http://www.gsma.com/latinamerica/mobile-and-privacy

GSMA. (s.d. de 03 de 2013). *Estudio de GSMA sobre las actitudes relacionadas con la privacidad de los usuarios Móviles - Resultados clave de Colombia.* Obtenido de http://www.gsma.com/publicpolicy/wp-content/uploads/2013/04/privacy-attitudes-columbia-spanish.pdf

GSMA Association 2012. (s.d. de 06 de 2012). *Móviles y Privacidad Directrices para el diseño de privacidad en el desarrollo de aplicaciones.* doi:www.gsma.com/mobileprivacy

Halpert, Jim; et al. (2015). *DATA PROTECTION LAWS OF THE WORLD.* Londres y Chicago: DLA PIPER. Obtenido de http://www.dlapiperdataprotection.com/#handbook/world-map-section

Halpert, Jim; et al. (2015). *DATA PROTECTION LAWS OF THE WORLD.* Londres y Chicago: DLA PIPER.

Halpert, Jim; et al. (2015). *DATA PROTECTION LAWS OF THE WORLD.* Londres y Chicago: DLA PIPER. Obtenido de http://www.dlapiperdataprotection.com/#handbook/world-map-section

Haya Coll, P. A. (2006). *Tratamiento de información contextual en entornos inteligentes.* UNIVERSIDAD AUT´ ONOMA DE MADRID. Madrid: Tesis Doctora; Universidad Aautónoma de Madrid.

Hervás Lucas, R., & Bravo Rodriguez, J. (2009). MODELADO DE CONTEXTO PARA LA VISUALIZACION DE INFORMACION EN AMBIENTES INTELIGENTES. *Memoria para Doctorados de Informática*. Toledo, La mancha, España: Universidad de Castilla - La Mancha.

Holvast, J. (1993). *“Vulnerability and Privacy: Are We on the Way to a Risk-Free Society?* North-Holland: in the Proceedings of the IFIP-WG9.2 Conference.

Hull, R., Neaves, P., & Bedford-Roberts, J. (1997). Towards Situated Computing. *1st International Symposium on Wearable Computers; . IEEE Network*, 146-153.

IBM. (18 de 10 de 2012). *La adopción de BYOD ¿es una amenaza para las empresas?* Obtenido de Colombia.com / Tecnología / Noticias / Detalle de noticia: http://www.colombia.com/tecnologia/informatica/sdi/48477/la-adopcion-de-byod-es-una-amenaza-para-las-empresas

ico. (2015). *ico. Information Commisioner's Office*. Obtenido de Auditoria Independiente del Reino Unido -defiende los derechos de información de Interés Públido: https://ico.org.uk/

Intelligent Community Forum (IFC). (21 de 10 de 2015). *The Intelligent Community Forum names the Smart21 Communities of 2016.* Obtenido de http://www.intelligentcommunity.org/index.php?src=news&srctype=detail&category=Awards&refno=1830&prid=1830

International Organization for Standardization ISO. (23 de 04 de 2005-2013). *International Organization for Standardization ISO*. Obtenido de http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

International Telecommunication Union - ITU. (2012). *Privacy in Cloud Computing.* Geneva,: ITU.

International Telecommunication Union - ITU. (2013). *Privacy and Data Protection:Model Policy Guidelines & Legislative Texts.* Geneva: Telecommunication Development Bureau (BDT).

Inverse Inc. (11 de 2015). *Administration Guide for PacketFence version 5.5.0.* Obtenido de GNUFreeDocumentationLicense,Ver: http://www.packetfence.org/downloads/PacketFence/doc/PacketFence_Administration_Guide-5.5.1.pdf

ISO. (15 de 06 de 2005). *ISO/IEC 17799 - International Organization for Standardization*. Obtenido de Information technology -- Security techniques -- Code of practice for information security management: http://www.iso.org/iso/catalogue_detail?csnumber=39612

ISO. (15 de 05 de 2014). ISO 37120 briefing note: the first ISO International Standard on city indicators. *Normative references*. doi:http://www.iso.org/iso/37120_briefing_note.pdf

ISO -IEC. (2015). *ISO/IEC JTC 1 Information technology.* Switzerland: www.iso.org. doi:http://www.iso.org/sites/mysmartcity/index.html

IT@Intel White Paper. (11 de 2013). *Enabling BYOD with Application Streaming and Client Virtualization.* Obtenido de enabling-byod-with-application-streaming-and-client-virtualization.pdf

ITU-T – Telecommunication Standardization Bureau (TSB). (s.d. de 09 de 2015). *Security in Telecommunications and Information Technology.* (P. d.–C.-1. Switzerland, Ed.) Recuperado el 08 de 12 de 2015, de http://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-SEC-2015-PDF-E.pdf

ITU-T. (03 de 2012). *Privacy in Cloud Computing.* Obtenido de ITU-T Technology Watch Report: http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf

Jackson, N., & Walshe, P. (2011). *Móviles y Privacidad Directrices para el diseño de privacidad en el desarrollo de aplicaciones.* New Fetter Lane - London: GSMA.

Know, L. (2015). A vision for the development of i-campus. *Smart Learning Environments a SpringerOpen Journal*, 12. Obtenido de http://www.slejournal.com/content/pdf/s40561-015-0009-8.pdf

Laird, J. (07 de 11 de 2014). A Brief History of BYOD and Why it Doesn't Actually Exist Anymore. págs. http://www.lifehacker.co.uk/2014/11/07/brief-history-byod-doesnt-actually-exist-anymore.

Langheinrich, M. (2001). Privacy by design - Principles of Privacy-Aware Ubiquitous Systems. *Ubiquitous Computing - International Conference* (págs. 273-291). Atlanta, Georgia, USA, September 30 - October 2, 2001.: Editorial Springer-Verlag Berlin Heidelberg.

Langheinrich, M. (2005). *Personal Privacy in Ubiquitous Computing – Tools and System Support.* Switzerland: PhD thesis, ETH Zurich, Zurich. Obtenido de PhD thesis, ETH Zurich,Zurich.

Lassila, O. (2005). Using the Semantic Web in Mobile and Ubiquitous Computing. *Proceedings of the 1st IFIP WG12.5 Working Conference on Industrial Applications of Semantic Web), Springer,* , 19--25.

Lazarte, M. (19 de 11 de 2015). *From Australia to Nigeria - The road to building smart cities.* Obtenido de http://www.iso.org/: http://www.iso.org/iso/news.htm?refid=Ref2027

Lee, O., Yonnim, & Kwon. (2010). An index-based privacy preserving service trigger in context-aware computing environments, (2010),pages5192 - 5200,. *Expert Systems with Applications*, 5192-5200.

Lepouras, G. V. (2007). Domain expert user development: The SmartGov approach. *Communications of the ACM, 50 (9)*, 79-83.

Lucent, A. (2011.). "Understanding the Market Opportunity in the Cities of Tomorrow.". *Alcatel Lucent,*.

MACDONALD, N. e. (2010). *The Future of Information Security Is Context Aware and Adaptative.* Stamford: Gartner RAS Core Research Note G00200385.

Madden, Brian. (05 de 2012). *http://www.brianmadden.com/.* Obtenido de What is MDM, MAM, and MIM? (And what's the difference?): http://www.brianmadden.com/blogs/brianmadden/archive/2012/05/29/what-is-mdm-mam-and-mim-and-what-s-the-difference.aspx

Maidan, P. (20-22 de 05 de 2015). Smarter Solutions for a Better Tomorrow. (E. I. Group, Ed.) Obtenido de Exhibitions India Group: https://eu-smartcities.eu/sites/all/files/events/uploads/Smart%20Cities%20India%202015%20Brochure_0.pdf

Malek, J. A. (2009). Informative global community development index of informative smart city. *In Proceedings of the 8th WSEAS International Conference on Education and Educational Technology (Genova, Italy, Oct 17-19)*.

Manzano, V. (2005). *Introducción al análisis del discurso .*

Miller, W. I. (1997). *The Anatomy of Disgust.* Cambridge: Harvard University Press.

Nam , T., & Pardo , T. (2011). *Conceptualizing Smart City with Dimensions of Technology, People, and Institutions.* Obtenido de The Proceedings of the 12th Annual International Conference on Digital Government Research: http://inta-aivn.org/images/cc/Urbanism/background%20documents/dgo_2011_smartcity.pdf

NAM, T. P. ( 2011.). Conceptualizing Smart City with Dimensions of Technology , People and Institutions. (University of Maryland, Ed.) *12th Annual International Conference on Digital Government Research,*, 282-291.

NetworkWorld. (24 de 06 de 2013). *http://www.networkworld.com/.* Obtenido de 'La contenerización' no es la panacea BYOD: Gartner - Gartner señala que es una importante cuestión de desarrollo de aplicaciones de TI:

http://www.networkworld.com/article/2167570/byod/-containerization--is-no-byod-panacea--gartner.html

Normas-ISO.com. (25 de 02 de 2015). *NORMAS ISO*. Recuperado el 2015, de http://www.normas-iso.com/2015/iso-iec-27018-2014-requisitos-para-la-proteccion-de-la-informacion-de-identificacion-personal

ONU (United Nations Organization). (10 de 12 de 1948). *Universal declaration of human rights.* Obtenido de Adopted and proclaimed by General Assembly resolution 217 A (III) of December 10, 1948: http://www.un.org/en/sections/what-we-do/protect-human-rights/index.html

*PacketFence.* (11 de 2015). Obtenido de http://www.packetfence.org/about/advanced_features.html

Pandey, Y. (2015). Journey to Smart Campus How the Internet of Everything is Changing Everything. *CSI Symposium held on BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.,* (pág. 34). Bundesverband, Alemania: CISCO.COM. Obtenido de http://www.csi-2015.org/Downloads/CISCO%20Presentation%20at%20CSI%20Symposium%20held%20on%2006.08.2015.pdf

Parekh, S. (03 de 09 de 2014). *IEEE 802.11 Wireless LANs Unit 11.* Obtenido de EECS Instructional and Electronics Support - University of California, Berkeley: http://inst.eecs.berkeley.edu/~ee122/sp07/80211.pdf

Pascoe, J. (1998.). Adding Generic Contextual Capabilities to Wearable Computers. 2nd International Symposium on Wearable Computers,. *2nd International Symposium on Wearable Computers*, 92-99,.

Patiño Sedan, M. (2013). *CITY OF THE YEAR*. Obtenido de Investments and Corporate Banking, Citigroup: https://online.wsj.com/ad/cityoftheyear

Paul, I. (2013). 3 essential techniques to protect your online privacy. *PCWorld Digital*.

Periódico El Tiempo. (15 de 10 de 2015). Ley de Hábeas Data. *Archivo el Tiempo*, pág. s.p. Obtenido de http://www.eltiempo.com/noticias/ley-de-habeas-data

Pistore, M. (2015). Creating services WITH and FOR people. *Smart Community Lab*, 31. Obtenido de Project Manager – Smart Campus: http://www.science20-conference.eu/wp-

content/uploads/2013/08/14_Marco_Pistore_-_Smart_Campus__Services_with_and_for_People.pdf

PMI. (21 de 07 de 2014). *PMI Colombia Capitulo Bogotá.* Obtenido de Empresas de Clase Mundial: http://www.pmicolombia.org/2014/07/empresas-de-clase-mundial/

Preuveneers, D., & Joosen, W. (2015). Change Impact Analysis for Context-Aware Applications in Intelligent Environments. . *Workshop Proceedings of the 11th International Conference on Intelligent Environments. Open Access, IOS Press,* , 70-81.

Radic, L. (1 de 4 de 2015). *Estándares de privacidad para el entorno cloud.* Obtenido de http://www.ccsur.com/estandares-de-privacidad-para-el-entorno-cloud/

RAE. (2014). *DICCIONARIO DE LA LENGUA ESPAÑOLA - Vigésima segunda edición.*

Real Academia Española. (2014). *DICCIONARIO DE LA LENGUA ESPAÑOLA*. Obtenido de http://lema.rae.es/drae/

Robinson, B. (26 de 07 de 2007). *What you Need to Know About NAC.* Obtenido de IT SECURITY: http://www.itsecurity.com/features/what-you-need-to-know-about-nac-072607/

Rodriguez H., A. A., Espindola, D., J. E., & Rodriguez H., F. (09 de 2015). Implementación de dispositivos móviles personales (BYOD) en la universidad pública. *Memorias II Congreso Internacional de Educación a Distancia; ResearchGate*, 412-420. Obtenido de https://www.researchgate.net/publication/282850481_Implementacin_de_dispositivos_mviles_personales_BYOD_en_la_universidad_pblica

Rosenberg, R. (2004). *The Social Impact of Computers.* San Diego, United States of America: Academic Press.

Round Table Business/Higher Education. (2015). *Internet of Everything -Powering the Smart Campus & the Smart City:Geelong's Transformation to a Smart City.* Deakin Worldly; Cisco; IBM. DC. Victoria Parade: Round Table Business/Higher Education. Obtenido de http://www.bhert.com/events/2015-06-08/BHERT-Smart-City-Agenda-June-18.pdf

Ruiz, C. (31 de 05 de 2013). *Movilidad empresarial y convergencia de dispositivos.* Obtenido de oficina de prensa de Lenovo Colombia: http://www.mintic.gov.co/portal/vivedigital/612/w3-article-4442.html

Sairamesh, J. L. (2004). Information cities. . *Communications of the ACM, 47 (2)*, 28-31.

Salber D, e. a. (1998). Georgia Tech GVU Technical Report GIT-GVU-98-0. 1,. *Georgia Tech GVU Technical Report GIT-GVU-98-0*, 1-15.

Schaffers, H., Komninos, N., Tsarchopoulos, P., Pallot, M., Trousse, B., Posio, E., . . . Almirall,, E. (18 de 04 de 2012). Landscape and Roadmap of Future Internet and Smart Cities. *HAL archives - ouvertes - Fireball Proyect*, 209. Obtenido de https://hal.inria.fr/hal-00769715/document

Schilit, B., & Theimer , M. (1994). Disseminating Active Map Information to Mobile Hosts. . *IEEE Network, 8(5),* , 22-32.

Schmidt, A. (26 de 07 de 2015). *INTERACTION DESIGN FOUNDATION*. (I. D. Foundation, Editor) Obtenido de https://www.interaction-design.org/literature/book/the-encyclopedia-of-human-computer-interaction-2nd-ed/context-aware-computing-context-awareness-context-aware-user-interfaces-and-implicit-interaction#chapter_start

*Siliconweek*. (s.f.). Recuperado el Junio de 25 de 2015, de http://www.siliconweek.es/e-enterprise/como-elegir-la-mejor-solucion-de-control-de-acceso-a-la-red-nac-751

Solove, D. J. (2006). A TAXONOMY OF PRIVACY Vol. 154 No.3. *University of Pennsylvania Law Review*, 477-560. Obtenido de https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477%282006%29.pdf

Stojanovic, D. (2009). *Contex - Aware Mobile and Ubiquitous Computing fir Enhanced Usability: Adaotatuve Technologies and Applications.* New York: Information Science Reference Hershey -IGI GLOBAL - Brithis Library. Obtenido de https://books.google.com.co/books?hl=es&lr=&id=sY6IXsn5xjMC&oi=fnd&pg=PP1&dq=Context+-+Aware+Mobile+and+Ubiquitous+Computing+for+Enhanced+Usability:+Adaptation+Technologies+and+Applications&ots=qB2rAYMeQq&sig=gRdV74xI-EybY0tcX9VnT5-UdG0&redir_esc=y#v=onep

Strauss, J., & Rogerson, K. S. (2002). Policies for online privacy in the United States and the European Union. *Telematics and Informatics 19*, 173-192.

Tacacs. (04 de 2011). *The Advantages of TACACS+ for Administrator Authentication .* Obtenido de www.tacacs.net. : http://www.tacacs.net/docs/TACACS_Advantages.pdf

TechRepublic. (9 de 02 de 2015). *http://www.techrepublic.com/.* Obtenido de 5 Reasons why BYOD survived 2014 and will prosper in 2015, BYOD faced some criticisms in 2014 but appears set to evolve further this year. por Will Kelly: http://www.techrepublic.com/article/5-reasons-why-byod-survived-2014-and-will-prosper-in-2015/

THE COMMISSION EUROPEAN. (27 de 11 de 2013). COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN. *on the Functioning of the Safe Harbour from the Perspective of EU Citizens and*. Brussels,, s.p., Bélgica: EUROPEAN EUROPEAN.

The Federal Council - Portal of the Swiss government. (s.d. de s.m. de 2014). *Schweizerische Eidgenossenschaft - Confederation suisse*. Obtenido de The federal Council: http://www.edoeb.admin.ch/org/00129/00132/index.html?lang=en

The Huffington Post. (27 de 12 de 2013). NSA Phone Surveillance Is Legal, New York Judge Rules . *por: Neumeister, Larry (Internet)*. Obtenido de http://www.huffingtonpost.com/2013/12/27/nsa-phone-surveillance_n_4508483.html

United Nations. (07 de 2014). *Population world*. Obtenido de www.worldometers.info: http://www.worldometers.info/world-population/india-population/

Universia Colombia. (21 de 05 de 2013). *Para el año 2016 se afianzará el BYOD en las empresas.* Obtenido de Universia.net.co : http://noticias.universia.net.co/en-portada/noticia/2013/05/21/1024756/ano-2016-afianzara-byod-empresas.html

Value, N. (2 de 04 de 2001). ACADEMIA DE REDES LLEGA A COLOMBIA. *El tiempo*. Obtenido de http://www.eltiempo.com/archivo/documento/MAM-567980

Volokh, E. (1999). Freedom of Speech and Information Privacy: The Troubling Impli-cations of a Right To Stop People from Speaking About You. *University of California, Los Angeles (UCLA)*, 1049-1051.

W3C NOTE. (21 de 07 de 1998). *P3P Guiding Principles*. Obtenido de NOTE-P3P10-principles-19980721: http://www.w3.org/TR/NOTE-P3P10-principles

W3C Recomentation. (16 de 04 de 2002). *The Platform for Privacy Preferences 1.0* . Obtenido de (P3P1.0) Specification: http://www.w3.org/TR/P3P/

W3C Working Group Note. (13 de 11 de 2006). *The Platform for Privacy Preferences 1.1* . Obtenido de (P3P1.1) Specification: http://www.w3.org/TR/P3P11/

Wan, K. (2009). A Brief History of Context. *International Journal of Computer Science Issues Vol 6, No.2*, 33-42.

Want, R., Schilit, B., & Et al. (Diciembre, 1995.). An Overview of the PARCTab Ubiquitous Computing Experiment. *IEEE Personal Communications,*, 28-43. Obtenido de https://www.cs.colorado.edu/~rhan/CSCI_7143_002_Fall_2001/Papers/Want95_PARCTab.pdf

Ward, R., Hopper, A., Falcao, V., & Gibbons, J. (1992). The active Badge Location System. *ACM Transactions on Information Systems*, 91-102,.

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *4 HARV. L. R EV*, 193.

WatchGuard Technologies Inc. (s.d. de s.m. de 2008). *Las 10 principales amenazas a la seguridad de los datos de las PyMEs*. Obtenido de Parte. No. WGCE66599_112408: http://www.watchguard.com/docs/whitepaper/wg_top10-summary_wp_es.pdf

Weiser, M. (1993). Some computer science problems in ubiquitous computing. *Communications of the ACM*, 137–143.

Westin, A. F. (3 de 1 de 1968). *Privacy And Freedom.* Obtenido de http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr

Willis, D. A. (2012). Bring Your Own Device: New Opportunities,. *Gartner, Inc. G00238131*, 1-9.

World Law Group. (2013). *Global Guide to Data Breach Notifications.* Washington, D.C.: The World Law Group, Ltd.,.

Yovanof, G. S. (2009). An architectural framework and nabling wireless technologies for digital cities & intelligent urban environments. *Wireless Personal Communications, 49(3)*, 445-463.

# 8 ANEXOS

## 8.1 ANEXO 1: TABLA TIPO DE DOCUMENTOS REFERENCIADOS.

Tabla 8: Tabla de una muestra de Referencias

| No. | AUTOR | AÑO | Tipo documento | TITULO | PRIVACIDAD | SEGURIDAD | CONTEXTO | BYOD | APLICACIONES |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Behrooz, A. | 2010 | tesis de grado Master | Privacy of Mobile Users in Context aware Computing Environments Master of Science Thesis | X | | | | |
| 3 | Gartner Inc. | 2015 | Documento sitio Web | Gartner Enterprise Obtenido de http://www.gartner.com/technology/about.jsp | | | | X | |
| 4 | Haya Coll, P. A. | 2006 | Tesis Doctoral | Tratamiento de información contextual en entornos inteligentes UNIVERSIDAD AUT´ ONOMA DE MADRID. Madrid: Tesis Doctora; Universidad Autónoma de Madrid. | | | X | | |
| 5 | Hervás Lucas, R., & Bravo Rodriguez, J. | 2009 | Tesis Doctoral | MODELADO DE CONTEXTO PARA LA VISUALIZACION DE INFORMACION EN AMBIENTES INTELIGENTES Memoria para Doctorados de Informática España: Universidad de Castilla - La Mancha. | | | X | | |
| 6 | ITU-T. | 2012 | Documento sitio Web | Privacy in Cloud Computing Obtenido de ITU-T Technology Watch Report http://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000160001PDFE.pdf | X | | | | |
| 8 | Langheinrich, M. | 2005 | Articulo revista - IEEE | Personal Privacy in Ubiquitous Computing – Tools and System Support. Switzerland: PhD thesis | X | | | | |
| 9 | Periódico El Tiempo. | 2015 | Noticia | Ley de Hábeas Data Archivo el Tiempo | X | | X | | |
| 10 | Schilit, B., & Theimer, M. | 1994 | Articulo revista - IEEE | Disseminating Active Map Information to Mobile Hosts; IEEE Network 8 | X | X | | | |
| 11 | Solove, D. J. | 2006 | Articulo revista | A TAXONOMY OF PRIVACY Vol. 154 No.3 University of Pennsylvania Law Review | X | | | | |
| 12 | Stojanovic, D. | 2009 | libro e-book | Contex - Aware Mobile and Ubiquitous Computing fir Enhanced Usability | | | X | | |

| No. | AUTOR | AÑO | Tipo documento | TITULO | PRIVA CIDAD | SEGURIDAD | CONTEXTO | BYOD | APLICACIONES |
|---|---|---|---|---|---|---|---|---|---|
| 13 | Want, R., Schilit, B., & Et al. | 1995 | Articulo revista - IEEE | An Overview of the PARCTab Ubiquitous Computing Experiment; IEEE Personal Communications | | | X | | |
| 14 | Asamblea Nacional Constituyente 1991. | 2006 | Documento en sitio Web | Nueva Constitución Política de Colombia 1991Obtenido de la página www.procuraduria.gov.co | X | X | | | |
| 15 | CISCO. | 2014 | Sitio Web | Cisco. Cisco NAC Appliance (Clean Access); Obtenido de http://www.cisco.com/en/US/products/ps6128/index.html | | X | | | |
| 16 | Dey, A. K. | 2001 | Articulo revista | Understanding and using context. Personal and Ubiquitous Computing | | | X | | |
| 17 | Dziedzic, T., & Levien, R. | 2015 | Sitio Web | PacketFence Administration Guide Obtenido de http:/www.packetfence.org/downloads/PacketFence/doc/PacketFence_Administration_Guide-5.5.2.pdf | | X | | | |
| 18 | MACDONALD, N. e. | 2010 | Articulo revista | The Future of Information Security Is Context Aware and Adaptative Stamford: Gartner RAS Core Research Note G00200385. | | X | X | | |
| 19 | Nommas-ISO.com. | 2015 | Sitio Web | NORMAS ISO . Recuperado el 2015 | X | | | | |
| 20 | W3C NOTE. | 1998 | Sitio Web | P3P Guiding Principales. Obtenido de NOTE-P3P10-principles-19980721: http://www.w3.org/TR/NOTE-P3P10-principles | X | | | | |
| 21 | Warren, S. D., & Brandeis, L. D. | 1890 | Articulo revista | The Right to Privacy. 4 HARV. L. R EV | X | | | | |
| 22 | Gartner. | 2014 | Sitio Web | Magic Quadrant for Enterprise Mobility Management Suites. Obtenido de Analyst | | | | X | |
| 23 | IT@Intel White Paper. | 2013 | Documento sitio Web | Enabling BYOD with Application Streaming and Client Virtualization. Obtenido de enabling-byod-with-application-streaming-and-client-virtualization.pdf | | | | X | |
| 24 | Willis David A. | 2012 | Artículo de revista | Bring Your Own Device: New Opportunities | | | | x | x |

Referencias con tipo de documento. Fuente propia

## 8.2 ANEXO 2: MANUAL DE INSTALACIÓN Y CONFIGURACIÓN DE PACKETFENCE

Se inician las pruebas basándose en los manuales de packetFence que se encuentran en la página oficial de PacketFence[95], según el sitio oficial del PacketFence la última versión es la 5.5.2, que fue publicada el 07/12/2015. Es una versión considerada estable, pero se ha utilizado la versión 5.5.1 que fue publicada en Nov de 2015. (Inverse Inc., 2015), se utiliza el documento Administration-Guide.pdf como manual de referencia. El primer paso es la instalación del sistema operativo.

### *1. Prueba instalación en Ubuntu 12.04 (FALLA)*

Se realiza la instalación del sistema operacional ubuntu 12 se actualiza se realizan las instrucciones del manual suministrado por el sitio oficial de PacketFence y por otros sitios encontrados pero el resultado es fallido ya que las dependencias de las librerías no cumplen y el error generado es que las librerías requeridas por PacketFence son superiores a las del sistema operacional, aun cuando se descarga el paquete y no se instala con apt-get genera errores de dependencias, que aunque se tratan de corregir no se logra hacer funcionar.

### *2. Prueba instalación en centos 6.6 (FALLA)*

Se instala CentOS release 6.6 y se actualiza se envía instalación de PacketFence y resulta fallida la prueba de instalación, al revisar ya hay una versión más reciente del PacketFence que trabaja con centos 6.7

[95] http://www.packetfence.org/documentation/guides.html

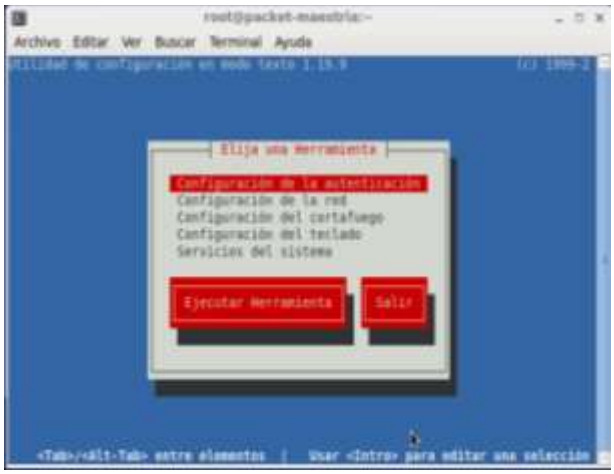
### 3. *Prueba instalación en centos 6.7 (EXITOSA)*

Se instala CentOS release 6.6 y se actualiza se envía instalación de PacketFence y resulta exitosa la prueba, a continuación se describen los pasos seguidos para su instalación y configuración del Yum update.

### 4. *Se deshabilita el FireWall*

Activando el SetUp del SO se puede desinstalar el firewall

Imagen 35 : Evidencia de activar los cortafuegos




### *5. Se deshabilita selinux*

Se corre el siguiente script →

Imagen 36: Script para deshabilitar selinux

```
[root@packet-maestria ~]# sestatus | grep -i mode
Current mode:                enforcing
Mode from config file:       enforcing

[root@ packet-maestria ~]# setenforce 0
[root@ packet-maestria ~]# sestatus | grep -i mode
Current mode:                permissive
Mode from config file:       enforcing
```

Imagen 37 : Evidencia de deshabilitar selinux


### *6. Instalación de PacketFence*

Se manipula el siguiente archivo /etc/yum.repos.d/PacketFence.repo

con el siguiente contenido

```
[PacketFence]
name=PacketFence Repository
baseurl=http://inverse.ca/downloads/PacketFence/RHEL$releasever/$basea
rch
gpgcheck=0
```

7. ***Se instala rom***

En el sitio de http://www.packetfence.org/ se encuentran los documentos necesarios para la instalación[96].

**wget**

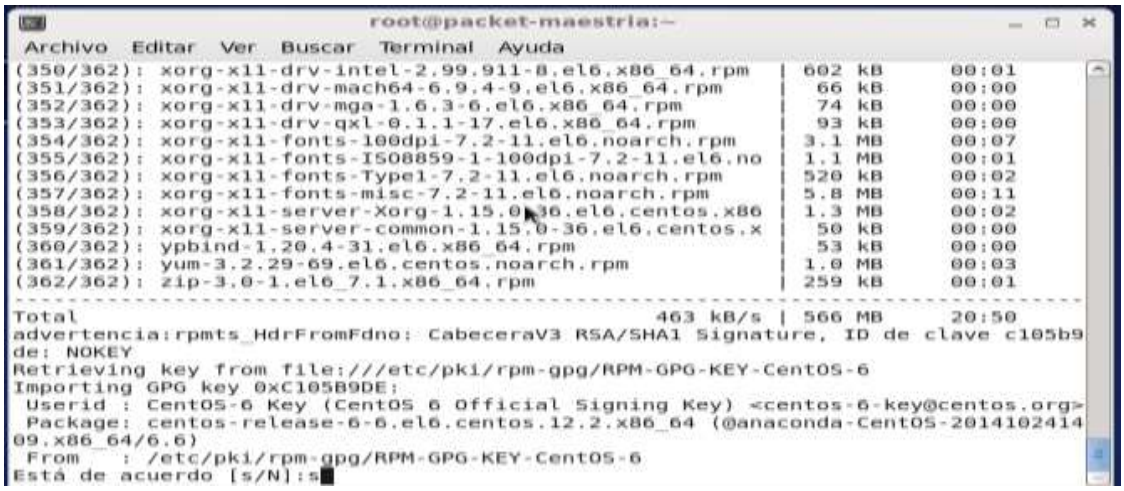
**rpm -Uvh http://packetfence.org/downloads/PacketFence/RHEL6/`uname -i`/RPMS/** packetfence-release-1-1.el6.noarch.rpm

**no funcionó**

8. ***Se instala desde repositorios de PacketFence***

yum -y install packetfence

Imagen 38: Evidencia de instalación del PacketFence




[96] http://packages.sw.be/rpmforge-release/rpmforge-release-0.5.2-2.el6.rf.x86_64.rpm

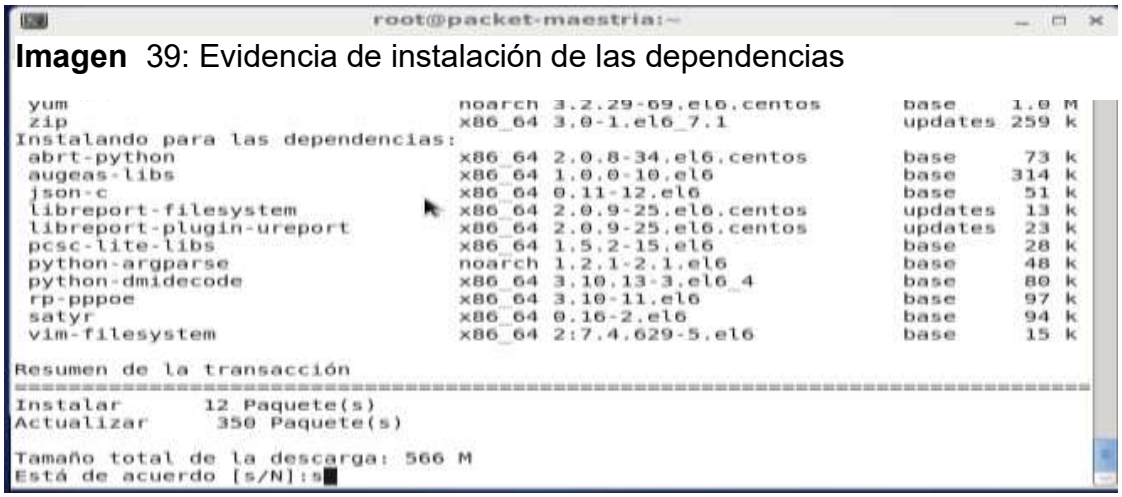
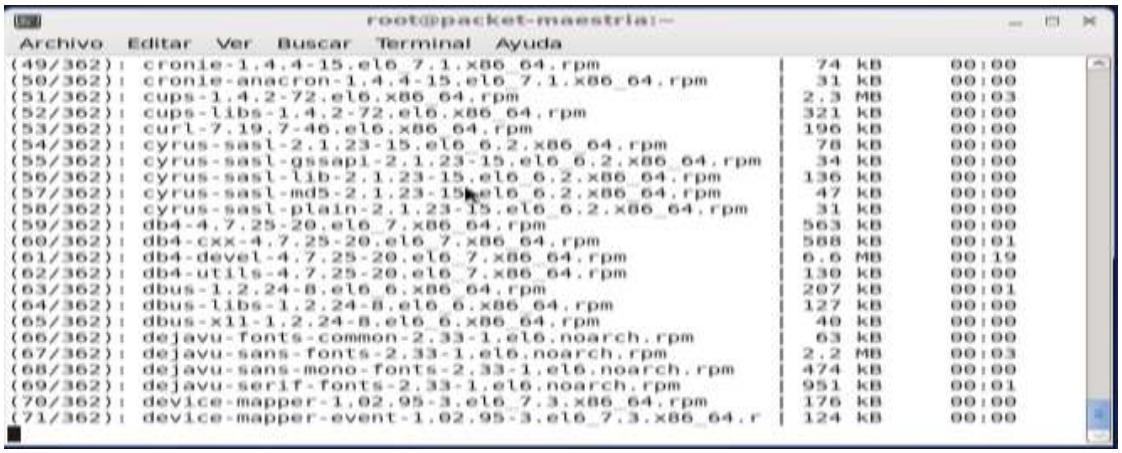



**Imagen** 39: Evidencia de instalación de las dependencias




### 9. *Ingreso a configuración inicial de packetfence*

Se debe ingresar a la dirección del servidor de la red prototipo

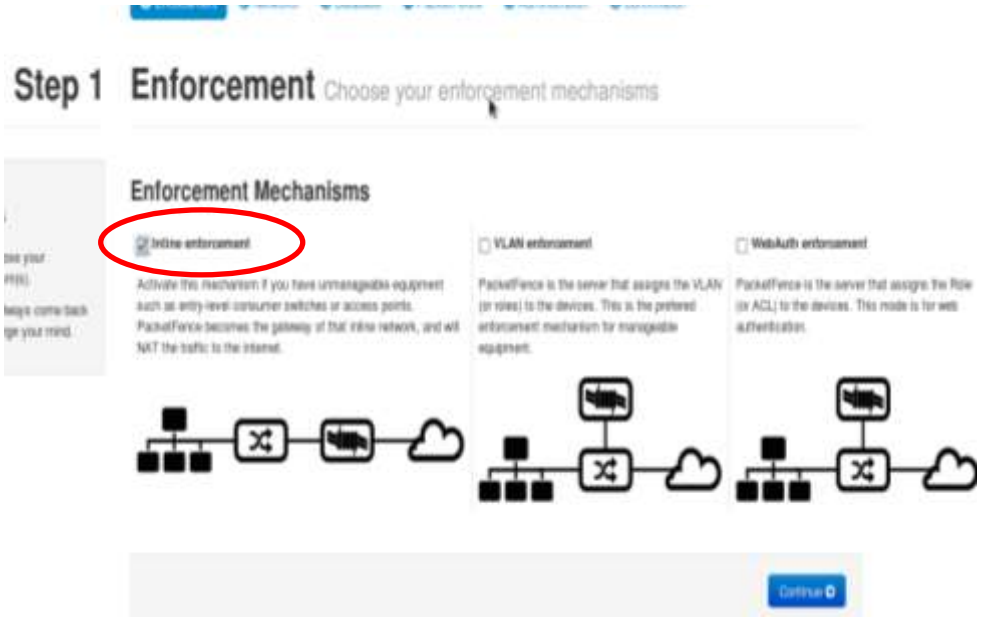
**https**://127.0.0.1:1443/

Imagen 40: Evidencia de la conexión

Imagen 41: se configura el navegador y se añaden excepciones

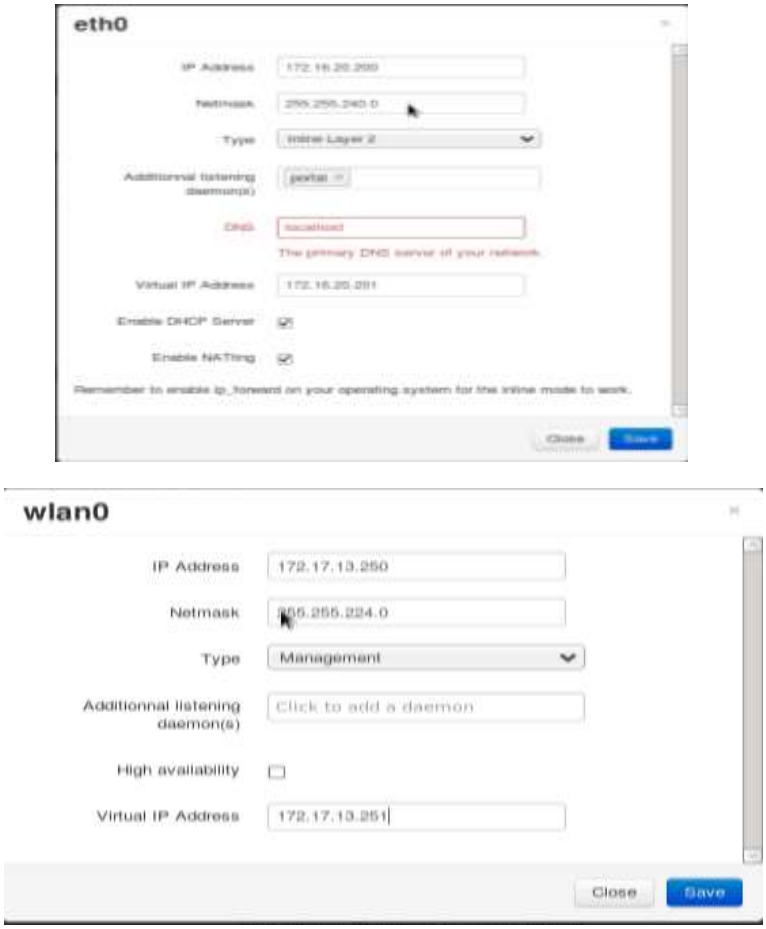

10. ***Se selecciona el modo en que se va a trabajar el PacketFence que es en modo inline***

Imagen 42: Selección del modo In Line del PacketFence



11. ***Creación de interfaces y subinterfaces para eth0 que va a ser la tarjeta que va contra layer2***

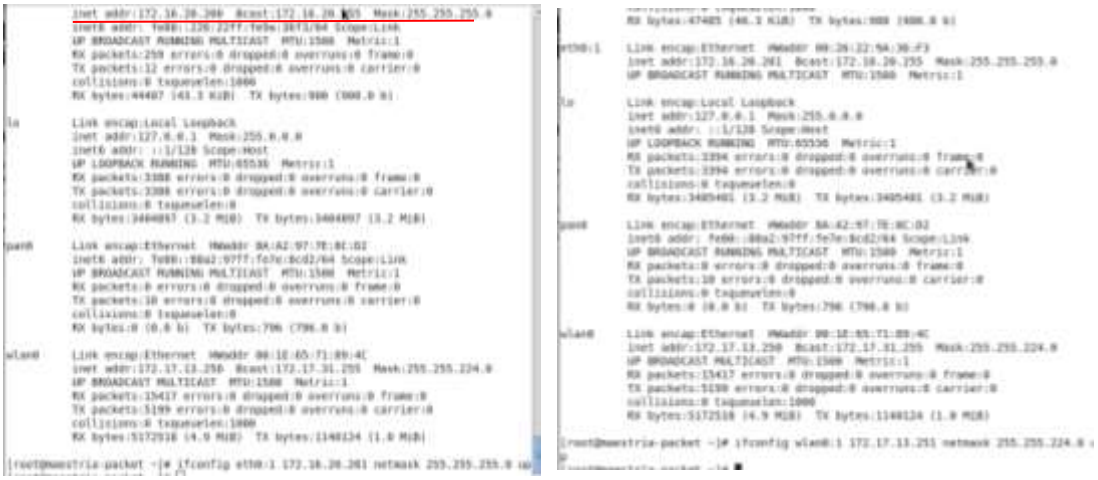
Imagen 43: Evidencia de creación Interfaz y subinterfaz




12. ***Creación de interfaces y subinterfaces para wlan que va a ser la manager, se* configura con la dirección IP**

Una vez se configuran las interfaces por PacketFence se deben configurar por consola o sistema operacional ya que no son agregadas por el aplicativo al sistema operacional.

Imagen 44: Evidencia configuración interfaces



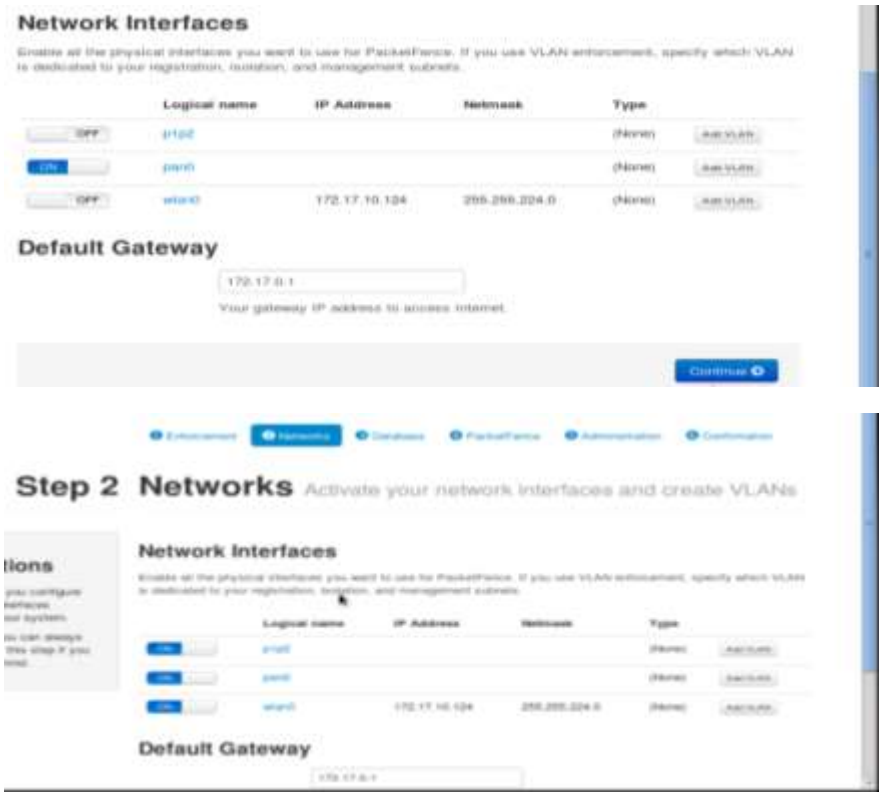
## 8.3 ANEXO 3: CONFIGURACIÓN PACKETFENCE

Se inicia la configuración de PacketFence después de la instalación

***Se inicia configurando las IPs de las interfaces y sus funciones***

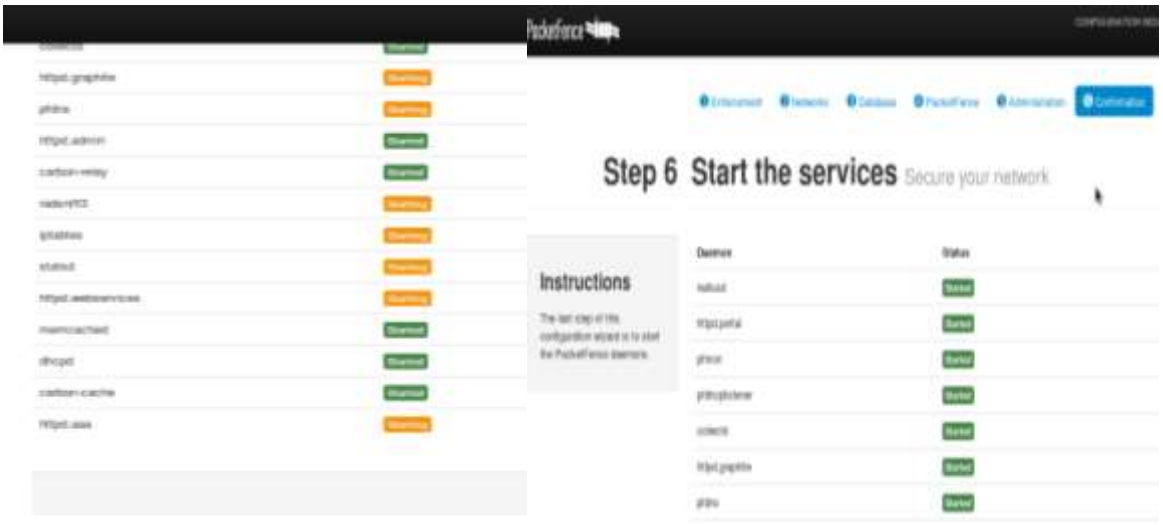
Imagen 45: Primera evidencia de configuración de las IPs

Imagen 46: Evidencia de la configuración de la IPs de la interfaz




**Arranque de servicios de PacketFence**

Imagen 47: Evidencia arranque de servicios de PacketFence



**Configuración de servidor Radius**

Para que funcione radius se debe crear la estructura contra BD MySQL de la siguiente manera:

1. **Se crea la bd radius**

   CREATE DATABASE radius;

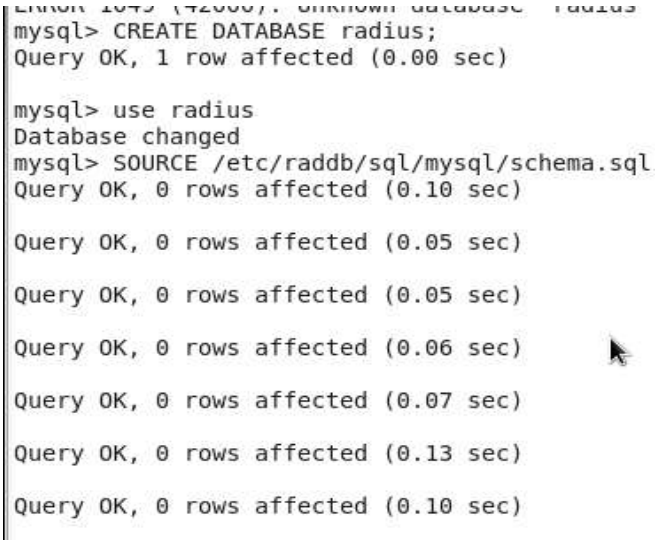
2. **Se asignan permisos full al usuario radius** a la base de datos radius a todas las tablas identificado con la clave radpass

GRANT ALL PRIVILEGES ON radius.* TO radius@localhost IDENTIFIED BY "radpass";

3. **Se hace uso de la base de datos radius** para despues proceder a deshacer el script que trae el esquema predefinido de la bd radius

   use radius;
   source /etc/raddb/sql/mysql/schema.sql

**Imagen** 48: Evidencia Creación de la base Radius




4. Se revisa configuración del archivo de configuración SQL de radius para comprobar que estén activas las siguientes líneas

vi /etc/raddb/sql.conf

# Connection info:
server = "localhost"
login = "radius"
password = "radpass"

# Database table configuration for everything except Oracle
radius_db = "radius"

1. Se revisa la clave de radius para autenticación de usuarios en el archivo

   /etc/raddb/clients.conf

   secret = testing123

2. Se reinicia radius

   /usr/local/pf/bin/pfcmd service radiusd restart

Al reiniciar el servicio se genera el siguiente error

Error: Refusing to start with libssl version OpenSSL 1.0

El error se elimina cambiando el siguiente parámetro en el archivo /etc/radb/radiusd.conf

allow_vulnerable_openssl = no a yes

3. Se realiza prueba de autenticación por radius, para ello se Agrega un usuario por base de datos MySQL para proceder probar

mysql -u root -p

use radius;

INSERT INTO `radcheck` (`id`, `username`, `attribute`, `op`, `value`) VALUES

(1,'test','User-Password',':=','test');

Imagen 49: Evidencia autenticación de radius


**Configuración de Servidor DHCP**

Configuración dhcp en la siguiente ruta /usr/local/pf/var/dhcp/dhcpd.conf

ámbito configurado.

NETWORK 172.16.20.0
MASCARA 255.255.255.0

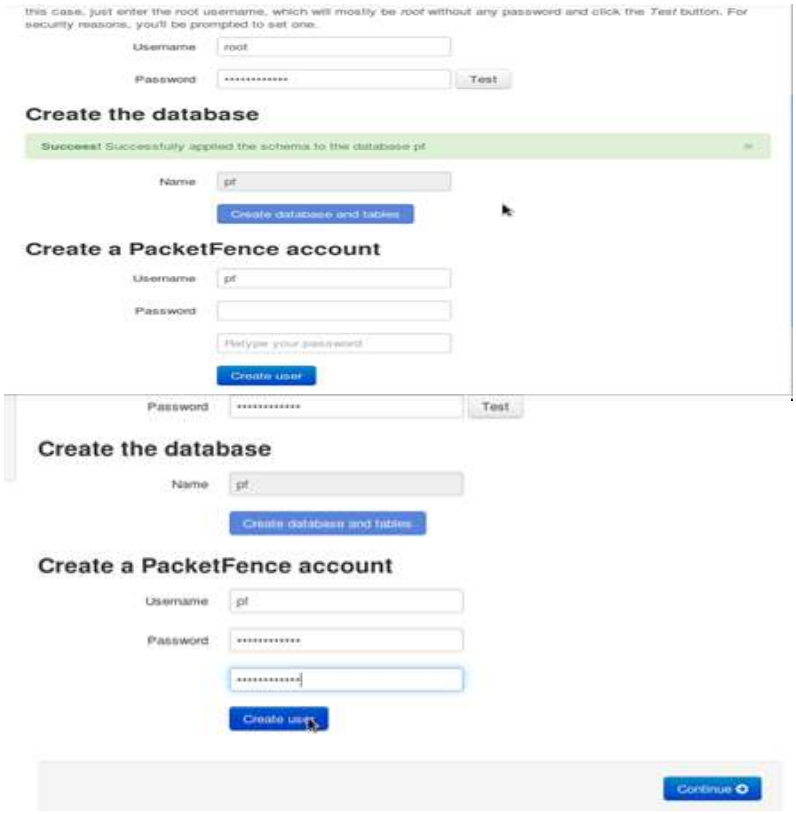
RANGO 172.16.20.0 172.16.20.240

**Configuración Dominio (DNS)**

El dominio creado en la consola es **maestria.edu**

El servidor queda registrado como packet.maestria.edu

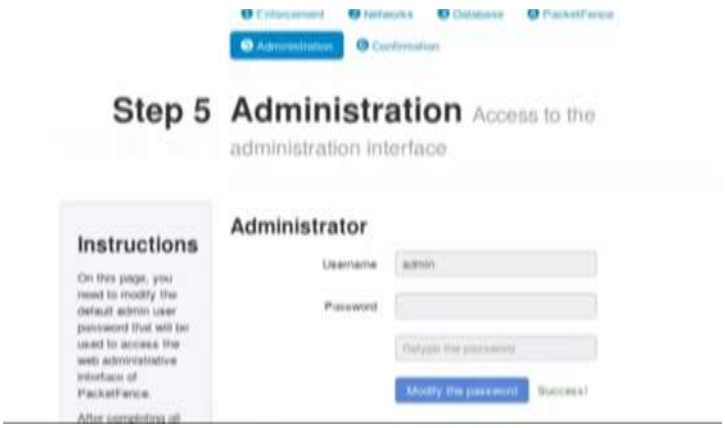
Imagen  50: Evidencia creación de la base de datos




Creación base de datos exitosa

Una vez se llega al final de la instalación exitosa solicita cambiar la clave de admin de la consola de **packetfence**, quedando de la siguiente manera

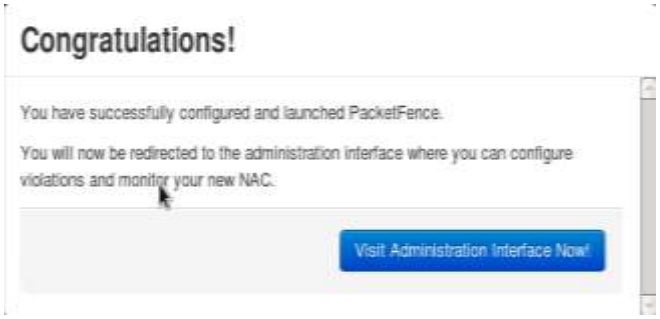
Imagen  51: Evidencia Instalación exitosa



**Administrador consola packetfence**
user= admin
pass= Maestri4

**Cuando finaliza instalación genera el siguiente mensaje**

Imagen 52: Evidencia de finalización del PacketFence




---

**Datos de mySQL server usado por packetfence y por radius**

usuario= root

passwd= Maestri4

usuario para bd packetfence

bd= pf

usuario= pf

clave= Maestri4

**Sistema Operativo Centos**

usuario= root

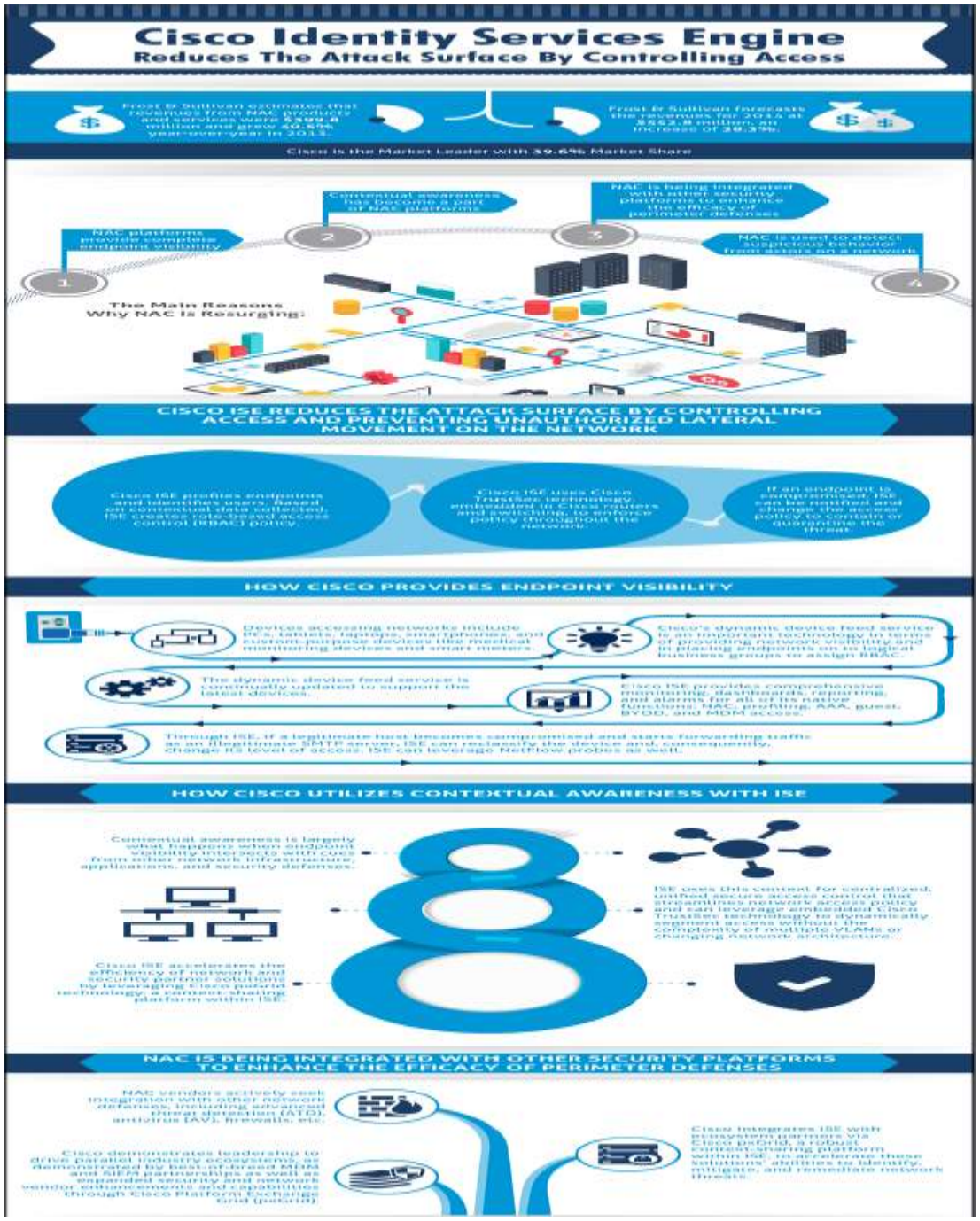
passwd= Maestri4

usuario= maestria

passwd= 1234567

## 8.4 ANEXO 4: INFOGRAFÍA DE ISE DE CISCO[97]

Imagen 53: Infografía de Cisco; controlando el acceso del usuario




[97] http://www.cisco.com/c/dam/en/us/products/security/identity-services-engine/ise-infographic.pdf