REVISTA COLOMBIANA DE COMPUTACIÓN
Volumen 17, número 2
Págs. 23 - 33

Estudio de las técnicas de privacidad basadas en ambientes sensibles al contexto

Study of the techniques of privacy based on ambients sensitive to the context

Mabel Y. Cogollo
Universidad Autónoma de Bucaramanga
Correo: mcogollo@unab.edu.co

José G. Hernández
Universidad Autónoma de Bucaramanga
Correo: jhernand@unab.edu.co

Fecha de recibido: 16/06/2016 y Fecha de aprobación: 19/09/2016

Resumen

El presente artículo 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* en los órdenes 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 PCs y dispositivos móviles. Se obtuvieron resultados favorables en su ejecución, destacándose la autenticación de usuarios, la implementación de VLAN por grupo y la viabilidad del programa BYOD en el Smart Campus de la Universidad Autónoma de Bucaramanga.

Palabras Clave: *Privacidad, técnicas, seguridad, entornos sensibles, Ciudades Inteligentes, BYOD, NAC.*

Abstract

The following paper 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

Keywords: *Privacy, Context-Aware Computing, Privacy Techniques, Security, Smart Citiess, BYOD, Network Access Control*

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 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.

1. Introducción

Esta propuesta de investigación tiene como propósito identificar los principios, los estándares, las técnicas y los 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 esta recibirá por las aplicaciones que la requieran. Lo anterior, debido a que los niveles de seguridad y privacidad brindados por los entornos inteligentes y las aplicaciones móviles utilizadas por los cibernautas, pueden llegar a vulnerar la información suministrada por los usuarios en el contexto.

En el presente documento se hará una descripción de la prueba piloto ejecutada en la UNAB, basada en los principios, las técnicas y los mecanismos de privacidad investigados; en la primera sección del documento se hace un breve recuento de los principios, los estándares, las técnicas y los mecanismos de privacidad. A continuación, se hace una descripción y análisis de la computación sensible en contexto o en entornos sensibles; de igual manera, se describen los elementos fundamentales de las aplicaciones sensibles al contexto, su funcionamiento y operación. Debido a que la prueba piloto ejecutada pretende sentar un precedente en el diseño y la arquitectura del Smart Campus de la UNAB, se hace una descripción del NAC utilizado para garantizar la privacidad de los usuarios que participen de la red en el entorno sensible.

2. Principios, estándares, técnicas y mecanismos de privacidad

2.1 Principios de privacidad

En la computación, la privacidad ha recibido varias definiciones durante distintas etapas históricas. Según Alan Westin en 1968, en su libro de "*Privacy and Freedom*" [1], 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 acerca 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.

Westin definió cuatro tipos de privacidad: Soledad, Intimidad, Anonimato y Reserva, todos los anteriores regidos por siete principios de privacidad, definidos como: Apertura y Transparencia, Participación individual, Limitación en la recopilación, Calidad del Dato, Limitación de uso, Seguridad Razonable y, Responsabilidad.

Por otra parte, Daniel Solove en el 2006, 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 [2]. Sin embargo los cambios que se hagan sobre la percepción de la privacidad estarán ligados a los 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.

2.2 Estándares

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 con la publicación de la serie de estándares ISO/IEC 27000, orientada a lo con-

cerniente a la seguridad de la información, los cuales consisten en la especificación de las operaciones de un Sistema de Gestión de Seguridad de la Información, (ISMS, por sus siglas en inglés), la provisión de los lineamientos para poner en marcha un ISMS, la presentación de las guías para la implementación de un ISMS destacando la pertinencia del método *Plan-Do-Check-Act,* PDCA; el diseño del 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.

2.3 Técnicas y mecanismos

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 y 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.

Para la ITU, la privacidad va más allá de la confidencialidad de la información, ya que cada individuo debe tener el control de su información personal sea pública, privada o profesional; debido a la facilidad con la que los datos pueden manipularse en la nube. La compatibilidad de las 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 se realizó una breve revisión en el apartado anterior.

Para lograr dicho objetivo, 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 cuya descripción de su procesamiento es fundamental para hacer las precisiones necesarias en la evaluación de los riesgos que puede correr la información.

La primera PET que todo ISMS debe tener, propuesta por la ITU, 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. Otra PET avalada son los *Anonymizer:* 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.

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. 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.

Por otra parte, el Consorcio de la *World Wide Web,* es una comunidad internacional encargada de desarrollar estándares para la WEB. 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 ha establecido: la Web para todos y la Web de 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.

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 para su funcionamiento y su combinación con los lenguajes de HTML, RSS y KML. Este primer avance en la seguridad se vió fortalecido, dos años después, con el desarrollo del Proyecto de la Plataforma para las Preferencias de la Privacidad, P3P, 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.

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. 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.

3. El contexto: Computación sensible y aplicaciones

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 [3]. 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, identifica cuatro características primordiales: el contexto es definible, es estable, es una forma de información y puede ser divisible.

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 con los objetivos propios de cada una de ellas sin lograr una precisión definitiva del término [4]. 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., define el contexto como las circunstancias dentro de las cuales algo existe o sucede, identificando 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 [5].

Con las definiciones, 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.

3.1 Aplicaciones sensibles al contexto

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 comporta-

miento basado en el contexto de la aplicación y del usuario, proveyendo información o ejecutando procesos en tiempo real cuando es detectado por los sensores. Según Haya Coll, una aplicación sensible al contexto es aquella que emplea el contexto como medio para ofrecer al usuario información y/o servicios, dependiendo qué necesita el usuario en un momento dado, [6] y pueden ser clasificadas de acuerdo con su función: la presentación de la información, la ejecución automática, el etiquetado del contexto, las aplicaciones activas y las pasivas.

Toda aplicación sensible al contexto debe cumplir con cuatro requisitos: la percepción, adaptación, detección y amplificación contextual, de acuerdo con los postulados de Lucas & Rodríguez. Por tal motivo, las dinámicas del contexto se han convertido en las determinantes en el rendimiento de cualquier aplicación. Sin embargo, parte de la causa para que las aplicaciones presenten dificultades en el desempeño, cuando se encuentran funcionando en contexto [7], según Schmidt, consiste en que la computación en Contextos Sensibles no funciona a un 100%, no es perfecta [8]. 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.

3.2 Smart Cities, Smart Campus

El crecimiento del uso de las tecnologías para la gestión de la información (TIC), la aparición de los entornos sensibles y la expansión de los servicios en la nube, llevaron a que naciera una nueva perspectiva de la ciudad con el concepto de Smart City. 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. Actualmente, el Foro de Comunidades Inteligentes, ICF, 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. El escalafón anual ofrecido por el ICF 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, una en Asia y una en Oceanía. Para 2016, Canadá y Taiwán se posicionan como los países líderes en ciudades inteligentes [9]. 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 (Banco Interamericano de Desarrollo) y funciona en el marco de la ICES (Iniciativa de las Ciudades Emergentes y Sostenibles) 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).

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. 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 la nube.

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 per-

cepción de la sostenibilidad. Las universidades se están haciendo más fuertes con la entrada del IoT (Internet de las cosas), 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, ha ampliado la percepción de la capacidad digital de la educación. Que exista una apertura en los espacios físicos para la interconexión hace 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? Un Smart Campus debe facilitar la integración de los datos y su modelo no dista del utilizado en una Smart City.

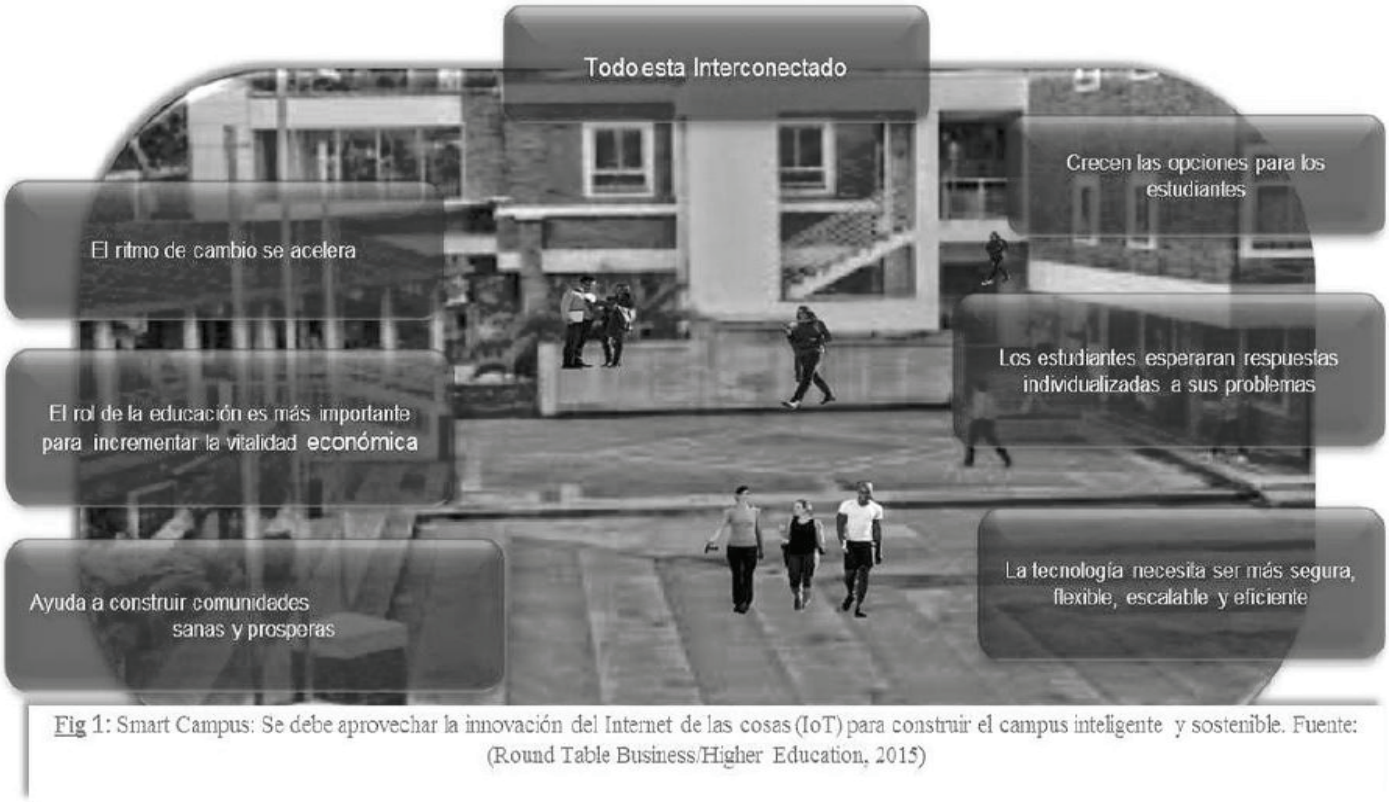

Figura 1. Smart Campus.
Fuente: Round Table Business Higher Education, 2015

Para llegar a ser un sistema eficiente debe cumplir con cuatro fases propuestas: 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 el aprovechamiento de 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, 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.

4. Bring Your Own Device - BYOD

El programa BYOD, *Bring Your Own Device,* 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. La implementación del BYOD en las 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 disponibles 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 sea eficiente es importante implementar políticas de privacidad precisas 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 y de los dispositivos móviles. Las políticas no deben estar orientadas a reducir los costos operativos sino al mejoramiento de la productividad de los empleados y su rendimiento individual depende de cuán responsable sea el uso de su dispositivo en la empresa.

Las leyes de privacidad que cada país ha ido implementando han ido considerando la protección de los datos personales como es el caso de Europa con la Directiva 95/46/CE que ha sido la base para que en el mundo se mire la privacidad como un derecho y la relevancia de la protección de la privacidad en la era del procesamiento del dato digital y la importancia de la cooperación internacional, como es el caso de Colombia con la Ley *Habeas Data*, 1581 de 2012.

En el sector educativo en nuestro país, la experiencia de mayor relevancia de uso del BYOD, es de 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. 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.

5. Control de Acceso a la Red – NAC

Con el desarrollo del estudio diagnóstico de técnicas y mecanismos de privacidad y seguridad, se analiza cómo sería la aplicación con el BYOD, implementadas además en un Smart Campus que para el estudio se tomó como referencia la Universidad Autónoma de Bucaramanga y se propone un esquema que permite tener claros todos los actores que entran a tenerse en cuenta en el contexto con respecto a la privacidad.

Para llevar a cabo el proceso de evaluación se implementó un sistema *Open Source* - NAC, como es el PacketFence, cuyas características incluyen el control de acceso e implementación de políticas de seguridad y privacidad de la información. Estableciendo una pequeña red como se muestra en la Figura 2, se configura el servidor Radius y el modo de autenticación a la red, realizando pruebas de autenticación por Radius, agregando un usuario por base de datos MySQL que permita probar el testeo del usuario, implementando las políticas de privacidad para su autenticación; se procede luego a la configuración del Servidor DHCP, para el ámbito IP y la configuración del dominio DNS.

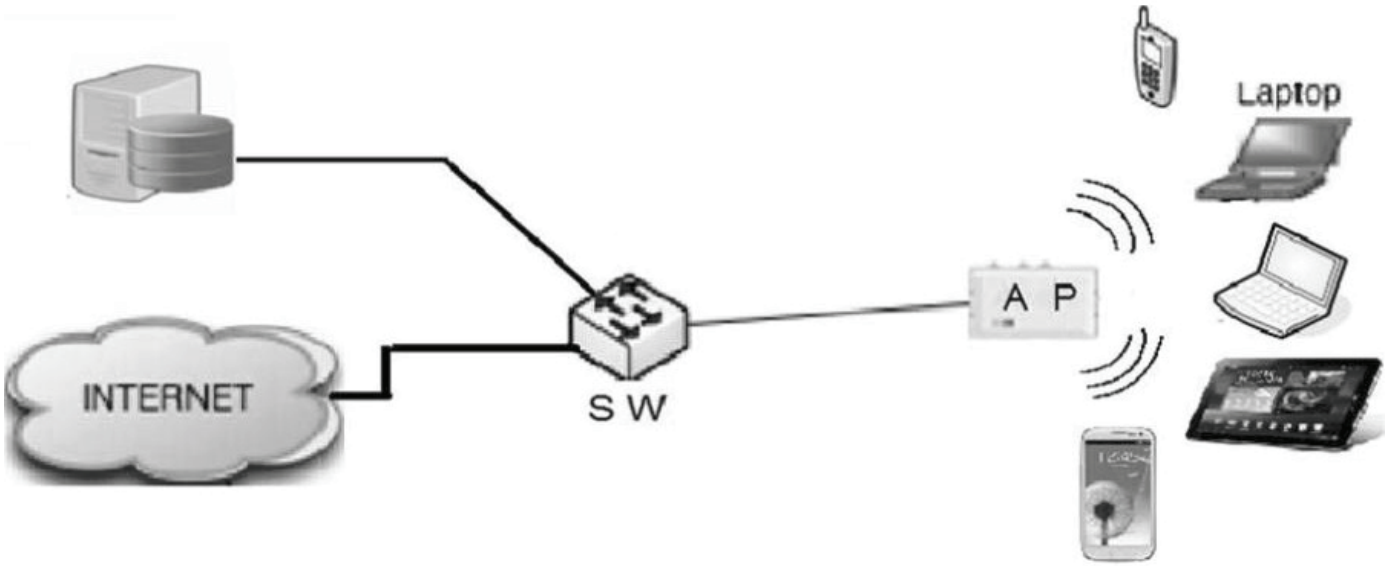

Figura 2. Prototipo topología de red para PacketFence.

Una vez configurado exitosamente el PacketFence se procede a realizar las pruebas con diferentes tipos de usuarios y de dispositivos conectados a la red. NAC, funciona como solución integrada que provee un mecanismo de autenticación para los dispositivos que deseen conectarse a una red de tipo LAN o WLAN. Los beneficios de un NAC incluyen el reconocimiento de los usuarios, sus dispositivos y sus roles en la red.

Se llega a los resultados que para la empresa la autenticación de usuarios permite mayor seguridad de sus datos y garantiza 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 establecer VLAN por grupo.

En el caso de BYOD, se puede observar que esta metodología está orientada no solo a ofrecer seguridad a las redes cableadas e inalámbricas de una organización, sino que también, se tiene en cuenta la privacidad de los usuarios por medio de mecanismos que permiten controlar el flujo de información entrante y saliente de la organización la información y la privacidad del usuario final quedan en la concientización y manejo de las buenas prácticas de los recursos tecnológicos en la empresa.

Teniendo en cuenta la literatura consultada, la aplicación de la prueba y los resultados obtenidos, se elaboró el siguiente esquema Figura 3, 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.

Figura 3. Esquema de privacidad.
Fuente: Elaboración propia.

Así mismo, se hace un paralelo entre el Smart Campus y la Smart City y su relación implícita.

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, 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 el presente documento una 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. De igual manera la arquitectura de todo contexto sensible debe atender a los principios y estándares de privacidad, teniendo en cuenta la regulación jurídica del país de origen.

BYOD es una solución empresarial para la optimización de los procesos en una institución o compañía. Sin embargo, es importante tener en cuenta la implementación de las políticas y mecanismos de privacidad, para llevar a buen término el propósito del programa ya que un único enfoque en la información empresarial es la seguridad, dejando de lado la privacidad de los usuarios que entran a hacer uso de las aplicaciones 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 gestión y control de acceso en la red para mejorar la productividad de la institución.

Referencias

[1] A. Westin, «Privacy and Freedom,» 3 1 1968. [En línea]. Available: http://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr.

[2] D. J. Solove, «A Taxonomy of Privacy,» *University of Pensylvania Law Review Vol. 154 No.3,* pp. 477-560, 2006.

[3] P. Douridh, «What We Talk About When Talk About Context,» *Personal and Ubiquitous Computing,* pp. 19-30, 2004.

[4] K. Wan, «A Brief History of Context,» *International Journal of Computer Science Issues Vol.6, No.2,* pp. 33-42, 2009.

[5] N. Macdonald y et.al, «The Future of Information Security Is Context Aware and Adaptative,» Gartner RAS Core Research Note G00200385, Stamford, 2010.

[6] P. A. Haya Coll, «Tratamiento de información contextual en entornos inteligentes,» Tesis Doctoral; Universidad Autónoma de Madrid, Madrid, 2006.

[7] L. R. Hervás y J. Bravo Rodriíguez, *Modelado de contexto para la visualización de información en ambientes inteligentes,* Toledo, La Mancha: Universidad de Castilla - La Mancha, 2009.

[8] A. Schmidt, «Interaction Design Foundation,» 26 07 2015. [En línea].

[9] Intelligent Community Forum (ICF), «The Smart21 Communities - Smart 21 of 2016,» 11 2015. [En línea].

[10] A. K. Dey, «Understanding and using Computing,» *Personal and Ubiquiotous Computing,* pp. 4-7, 2001.

[11] International Telecomunication Union - ITU, «Protección de datos y privacidad en la nube ¿Quién es el propietario de la nube?,» https://itunews.itu.int/Es/3702-Proteccion-de-datos-y-privacidad-en-la-nube-BR-Quien-es-el-propietario-de-la-nube.note.aspx, 2013.

[12] World Wide Web Consortium, «W3C Standards,» 3 12 2015. [En línea]. Available: http://www.w3c.es/estandares/.

[13] M. Ackerman y T. &. W. D. Darrell, «Privacy in Context,» *Human-Computer Interaction,* 2001.

[14] Gartner, «Gartner,» 17 12 2015. [En línea]. Available: www.gartner.com/doc/3206817?srcId=1-3931087981.

[15] IBM, «La adopcion de BYOD ¿es una amenaza para las empresas?,» [En línea]. Available: colombia.com/tecnología/informatica/sdi/48477/la-adopcion-de-byod-es-una-amenaza-para-las-empresas.

[16] Inverse Inc. , «Administration Guide for PacketFence Ver 5.5.0.,» Vols. %1 de %2GNUFree DocumentationLicense, p. 11, 2015.

Sobre los Autores

Mabel Yadira Cogollo. Docente Universidad Autónoma de Bucaramanga. Santander, Colombia. Programa de Ingeniería de Sistemas.

José Gregorio Hernández. Docente Universidad Autónoma de Bucaramanga. Santander, Colombia. Departamento de Tecnologías de Información Y Comunicaciones.

Este artículo se cita:

IEEE M. Y. Cogollo and J. G. Hernández, "Estudio de las técnicas de privacidad basadas en ambientes sensibles al contexto," Revista Colombiana de Computación, vol. 17, pp. 42-60, 2016.

APA Cogollo, M. Y., & Hernández, J. G. (2016). Estudio de las técnicas de privacidad basadas en ambientes sensibles al contexto. Revista Colombiana de Computación, 17(2), 42-60.