

Seguridad y componentes nativos en una aplicación híbrida

Security and native components in a hybrid application

Fecha de recepción: 2022-10-04 • Fecha de aceptación: 2022-11-22 • Fecha de publicación: 2023-01-10

Dulce Rivero Albarrán¹

Pontificia Universidad Católica del Ecuador

dmrivero@pucesi.edu.ec

<https://orcid.org/0000-0003-2736-5117>

Laura Rosa Guerra Torrealba²

Pontificia Universidad Católica del Ecuador

lrguerra@pucesi.edu.ec

<https://orcid.org/0000-0001-6325-943X>

Luis Fernando Molina Oñate³

Pontificia Universidad Católica del Ecuador

lfmolina1@pucesi.edu.ec

<https://orcid.org/0000-0003-4435-5076>

Resumen

El uso de dispositivos inteligentes es cada día mayor, y, por tanto, el desarrollo de aplicaciones móviles se ha incrementado. Las empresas, conocedoras de esta realidad, están adaptando sus aplicaciones digitales para incorporar estas tecnologías. Este trabajo presenta el desarrollo de una aplicación híbrida que integra la aplicación móvil a un conjunto de funcionalidades de un módulo CRM previamente construido. La aplicación móvil contiene además un componente de seguridad de dos factores que combina una autenticación biométrica y una autenticación por conocimiento. Además, la aplicación móvil incluye funcionalidades de mensajería y comunicación con los usuarios haciendo uso del ecosistema de los teléfonos inteligentes. Para la gestión del proyecto se usó un

método ágil. Se obtuvo una aplicación móvil en fase de operación que ya se encuentra en la Play Store de Google. Para validar la usabilidad de la aplicación, luego que esta fue utilizada por un periodo de tiempo, se realizó una encuesta a los usuarios, un 71% considera que la aplicación móvil es de fácil uso y que un 78% usa la aplicación para comunicarse con sus clientes.

Palabras clave: informática y desarrollo, comunicación móvil, protección de datos, internet, autenticación

Abstract

The use of smart devices is increasing every day, and the development of mobile applications is increasingly in demand. Companies aware of this reality adapted their digital applications to incorporate these technologies. This work presents a hybrid application that integrates the mobile application to a set of functionalities of a previously built CRM module. The mobile application also contains a two-factor security component, which combines biometric authentication and knowledge authentication. In addition, the mobile application includes messaging and communication features with users, making use of the smartphone ecosystem. For project management, was used an agile method. A mobile application obtained in the operation phase is already in the Google Play Store. To validate the usability of the system a user survey was carried out. 71% consider the mobile application easy to use, and 78% use this to communicate with their clients.

Keywords: IT and development, mobile communication, data protection, internet, authentication

Introducción

Los teléfonos inteligentes, además de ofrecer servicios de telefonía y mensajería de texto, poseen las mismas prestaciones de un computador y también capacidades de comunicación. Estos ofrecen aplicaciones para realizar una variedad de actividades las cuales van desde el entretenimiento hasta el trabajo. Específicamente en el campo laboral, el uso de los dispositivos móviles ha incrementado la productividad de los empleados, como se evidencia en el estudio realizado por Frost & Sullivan para la empresa Samsung (Turek, 2016) donde se concluyó que la productividad de los empleados que utilizan teléfonos inteligentes aumentó hasta en un 34%. Por otro lado, en el trabajo realizado por Acevedo et al. (2019) se concluyó que un 62% de los encuestados en la empresa, objeto de este estudio, utilizaban las aplicaciones de teléfonos inteligentes para comunicarse entre ellos.

En la última década, los teléfonos inteligentes han alcanzado una gran popularidad, y, por tanto, un crecimiento importante, ocasionando que el desarrollo de aplicaciones móviles y a su vez de la computación móvil, haya tenido un impacto importante en el campo del desarrollo de software. La computación móvil permite a los usuarios acceder a datos, información u otros objetos en cualquier otro dispositivo, usando una red de comunicación, a medida que este cambia su ubicación geográfica (Thomas, et al., 2018).

El uso de las aplicaciones móviles es cada día más ubicuo, cambiando la forma de trabajar, de socializar y de llevar la vida. Es por ello que algunas empresas han tomado la decisión de convertir estos dispositivos en una herramienta de trabajo y, por tanto, estas requieren de un conjunto de aplicaciones móviles para que los empleados apoyen y mejoren sus procesos o actividades, combinando en algunos casos con el desarrollo de aplicaciones web, conocidas como aplicaciones híbridas (Morales y Aguado, 2022; Ibáñez et al., 2022).

Una aplicación híbrida combina las capacidades de un dispositivo móvil y sus aplicaciones nativas con elementos de aplicaciones web. Las aplicaciones móviles nativas funcionan en dispositivos móviles y se descargan de la tienda autorizada por la App Store de cada plataforma, por otro lado, las aplicaciones móviles web funcionan y se adaptan a la pantalla de los dispositivos móviles y son accesibles mediante un navegador web. Las aplicaciones híbridas se encuentran en el medio del desarrollo web y nativo, su objetivo es aprovechar los beneficios de ambos desarrollos (Contreras et al., 2019).

La seguridad es un elemento fundamental en el desarrollo de aplicaciones móviles, especialmente cuando este permite acceder a información confidencial o sensible, por lo tanto, se debe garantizar que el acceso solo sea permitido a usuarios autorizados. Los sistemas de autenticación son uno de los mecanismos utilizados para brindar esta seguridad, ya sea usando una autenticación mediante credenciales únicas (usuario y contraseña) o biométrica.

La compañía Chevyplan ha decidido incorporar a su modelo de negocio el uso de las aplicaciones móviles, esto con el fin de mejorar sus procesos e incrementar la productividad de sus empleados. Esta compañía es conocida a nivel nacional e internacional por sus planes de venta programada de vehículos Chevrolet. La empresa tiene desarrollado un conjunto de módulos que apoyan sus

procesos internos, uno de estos es el módulo de Gestión de Relación con el Cliente (CRM por sus siglas del inglés), que es usado principalmente por los asesores comerciales para el ingreso de prospectos y potenciales clientes de la empresa.

En este trabajo se presenta el desarrollo de un aplicativo móvil híbrido para el manejo del módulo CRM de la empresa ChevyPlan, el desarrollo tiene como objetivo mejorar los servicios de atención al cliente, mantener su fidelidad y, por supuesto, aumentar las ganancias de la empresa. El aplicativo cuenta con un sistema de autenticación con dos factores (2FA de sus siglas en inglés) conformado por una autenticación biométrica y otra con credencial única y, además, se incorporan características del entorno nativo como son el acceso a componentes del teléfono móvil y la recepción de notificaciones *PUSH*.

1.1 Revisión teórica

El uso de dispositivos móviles es ya generalizado y un gran porcentaje de ellos son dispositivos inteligentes (Ramírez, 2019), el número estimado de usuarios móviles en todo el mundo para el año 2023 se estima que será a los 7.330 millones (O’Dea, 2021). Por lo tanto, la demanda de aplicativos móviles será también alta, en la actualidad existen en el mercado más de 6,2 millones de aplicaciones; a diario aparecen nuevas disponibles al público en las tiendas de aplicaciones Google Play, Apple App Store y Amazon AppStore (O’Dea, 2021). Las oportunidades de negocio surgen continuamente, creando aplicaciones que van desde juegos de gran complejidad hasta aplicaciones para controlar y hacer seguimiento de las actividades del hogar, las inversiones, la salud, entre otras.

Los desarrolladores de aplicaciones móviles, para ser competitivos, incorporan continuamente funcionalidades o características a las aplicaciones, a fin de que sean más seguras o para incorporar nuevas tecnologías o capacidades para tener comportamientos más amigables o mejores funcionalidades. Se han incorporado tecnologías de realidad aumentada para ofrecer experiencias interactivas a los usuarios combinando información virtual a la información que ya se tiene del producto, se usan técnicas de multimedia, modelado 3-D, seguimiento en tiempo real interacción inteligente, entre otras (Chen et al., 2019). Todo esto con el fin de acercar el mundo digital al mundo real, permitiendo una nueva forma de interactuar con las cosas a su alrededor. Esta tecnología ha sido utilizada en aplicaciones de educación (Sala, 2021), medicina (Javaid & Haleem, 2020), manufactura, turismo (Nayyar et al., 2018), entre otras.

Aplicaciones en el sector del comercio electrónico, el entretenimiento, la enseñanza o las redes sociales han incluido funcionalidades para recomendar productos de acuerdo a los gustos de los usuarios (Kulkarni et al., 2020; Guo et al., 2018). Se han desarrollado aplicaciones en el campo de la salud que hacen uso de los sensores de los teléfonos o se conectan a sensores externos a través internet o *bluetooth* con el fin de monitorear el estado de salud del usuario (ritmo cardiaco, tensión cardiovascular) (Ranjan et al., 2019).

En la era de la industria 4.0 los clientes requieren rapidez, precisión y servicios de calidad. Por ello, las empresas necesitan mejorar la interacción con sus clientes, esto con el fin de garantizar su satisfacción y lealtad. Este objetivo se extiende y ahora, una vez que los clientes confían y se

sienten satisfechos con en una empresa, se desea mantenerla y mejorarla continuamente y este paso es aún más complejo. Para abordar esta complejidad se han desarrollados los sistemas CRM y ahora, con las nuevas tecnologías, estos sistemas se están renovando y ahora con un toque de Tecnologías de la Información, estos sistemas se mencionan con el nombre de gestión electrónica de las relaciones con los clientes (E-CRM) (Hidayat & Rachmat, 2014).

En los últimos años, los sistemas E-CRM están integrando las últimas tecnologías en sus aplicaciones, estas son: navegadores web, sistemas operativos Android, correo electrónico, centros de atención telefónica, entre otras y operan utilizando redes de Internet, por lo que las aplicaciones E-CRM están migrando a aplicaciones que se ejecutan desde un teléfono inteligente, es decir, E-CRM móviles (Padeli et al., 2020; Demo et al., 2017).

En el mundo de las aplicaciones móviles, en algunos casos se manipulan datos importantes y confidenciales que no deben ser conocidos por el público, tales como datos médicos, bancarios, personales o de sus redes sociales. Hay diversas formas para brindar seguridad a los datos, una de ellas es la criptografía, la cual asegura mantener la confidencialidad y autenticidad de los datos. Por tanto, si una aplicación móvil manipula datos confidenciales requerirá incorporar mecanismos de autenticación para garantizar la seguridad de la información.

La autenticación determina si un usuario puede acceder a un sistema o recurso. Existen cinco tipos de autenticación, estos son: por *token*, los basados en información biométrica, los basados en conocimiento, basados en la ubicación (direcciones IP) y los sistemas híbridos (Rodríguez et al., 2018). En la autenticación por *token* el usuario utiliza un objeto que le identifica ante un sistema informático y el cual contiene una llave de criptografía. La autenticación basada en conocimiento tradicionalmente utiliza contraseñas alfanuméricas, las cuales son una combinación de letras, dígitos y signos especiales. La autenticación biométrica utiliza algo que identifique de forma única al usuario, como son la cara, el iris, la voz, la firma o la huella dactilar, siendo esta última una de las más confiables y estables en la rama de la biometría (Sadaf et al., 2020; Karakaya et al., 2019; Tan & Lee, 2019).

Simram (2020) en su trabajo expresa que se está en una etapa en la que se combina el uso de laptops y dispositivos móviles, conectados entre sí, para realizar diferentes tareas, por lo que, según este autor, las aplicaciones híbridas son la solución más viable para las empresas que cuentan con software desarrollado para escritorios o laptop y que tienen la necesidad de adaptarse al mundo de las aplicaciones móviles. En su trabajo la seguridad, en este tipo de aplicaciones, es uno de los aspectos más importantes.

Existen una variedad de peligros o debilidades que se deben tener en cuenta al desarrollar aplicaciones móviles, estas incluyen almacenamiento y transmisión de datos inseguro, contraseña/claves codificadas y fuga de datos confidenciales (Alanda et al., 2020). Las dos últimas pueden ser mitigadas implementando un sistema de autenticación 2 fases y, además, encriptando la contraseña. Los riesgos de seguridad deben ser gestionados siguiendo alguna metodología. Existen diversas metodologías para la gestión de riesgos, según ISOTools Excellence (s.f.), estas son: MAGERIT, CRAMM, OCTAVE, NIST 800-03, ISO 27005 e ISO 31000.

En el mismo sentido, en la literatura se encuentran un conjunto de buenas prácticas que se pueden implementar para evitar los diferentes tipos de ataque en aplicaciones de software. Las buenas prácticas contienen una serie de metodologías, sistemas, herramientas, y técnicas aplicadas y aprobadas con resultados sobresalientes en empresas que han sido reconocidas, éstas prácticas han sido probadas y validadas, una y otra vez y merecen ser compartida con el fin de ser adoptada por el mayor número posible de personas (FAO, 2015). Algunas de estas buenas prácticas para reducir el problema de autenticación de usuarios y la substracción de información personal del usuario como la clave y nombre de usuario (*Phishing*) son: verificar los derechos de acceso solo en el sistema *backend*, además el *backend* debe verificar cada solicitud que ser haga, también propone no utiliza almacenamiento de código fuente para establecer permisos (Alanda et al., 2020).

1.2. Encriptación AES (*Advanced Encryption Standards*)

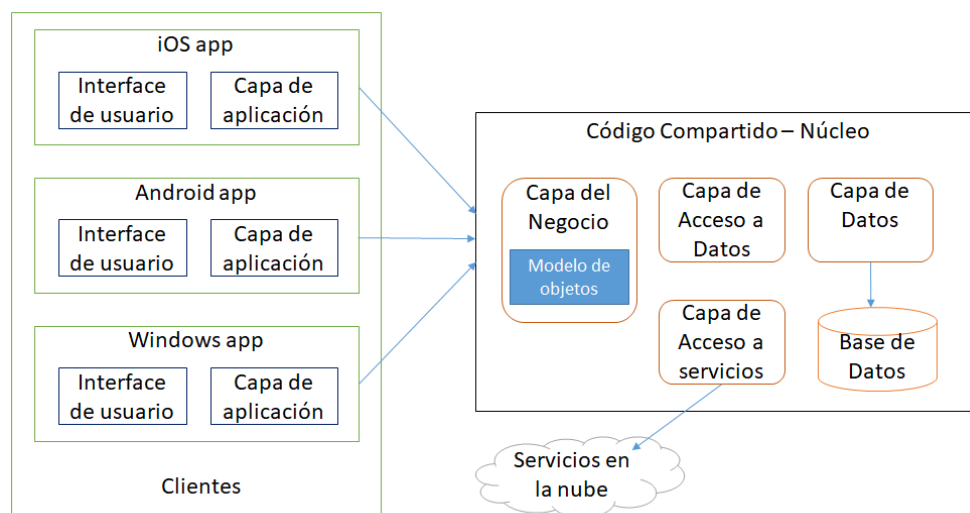
La encriptación AES es un algoritmo criptográfico de simetría y cifrado de bloque considerado como *inexpugnable* para ataques de fuerza bruta con súper computadoras o ataques de cualquier tipo de hacker. Existen 3 algoritmos de encriptación, AES-128, AES-192 y AES-256, cada número representa la cantidad de bits usados en la encriptación (128, 192 y 256 bit respectivamente). En cuanto al tiempo de procesamiento AES-128 tiene un tiempo de procesamiento relativamente más rápido en comparación con los otros dos algoritmos. En cuanto al uso del CPU utilizado para el proceso de cifrado y descifrado de archivos, AES de 192 bits utiliza menos CPU que los otros dos algoritmos (Andriani et al., 2018).

1.3 Certificado PKCS (*Public-Key Cryptography Standards*)

En un grupo de estándares de criptografía de clave pública concebidos y publicados por los laboratorios de RSA en California, es un formato codificado en BASE64 ASCII utilizado para almacenar datos firmados o encriptados. Los archivos generados por PKCS#7 pueden encontrarse en diversos formatos, por ejemplo, DER (*Distinguished Encoding Rules*) el cual se encuentra en formato binario y solo contiene información del certificado, no una clave privada o el formato PEM (*Privacy Enhanced Mail*) generalmente en formato de texto, puede poner certificado o clave privada, o ambos (Palacios & Delgado, 2006).

1.4 Arquitecturas híbridas

Una arquitectura híbrida está compuesta por dos partes, la parte cliente o visual que es desarrollado dependiendo del sistema operativo móvil ya sea iOS, Android o Windows Phone y se encarga de consumir los servicios de la otra parte. El núcleo o parte lógica contiene el código que es compartido por el cliente y contiene la lógica del negocio, los servicios de acceso a los datos y a los servicios alojados en la nube y la base de datos que será compartida por los clientes (ver *Figura 1*).

Figura 1*Arquitectura de una Aplicación Híbrida*

Metodología

El presente trabajo es un tipo de investigación aplicada, ya que busca resolver el problema de acceso a el módulo CRM, independientemente del lugar donde se encuentren los usuarios. Se llama también de tipo tecnológico, porque su producto no es un conocimiento puro, sino tecnológico.

Para el desarrollo de la aplicación móvil se seleccionó la metodología ágil programación extrema (XP por sus siglas del inglés), esta permite el desarrollo y gestión de proyectos de una manera flexible, eficiente, de bajo riesgo y con calidad, además el desarrollo se realiza de forma incremental pudiendo obtener en las primeras iteraciones una versión del producto (Lindstrom, 2003).

XP establece cinco fases (Ambler, 2018), de las cuales se ejecutaron cuatro, en la fase de exploración se realizó el modelado inicial, tanto de requisitos, como el arquitectónico; en la fase de planificación se estableció, junto a los usuarios, la fecha de inicio para el desarrollo de la primera versión de la aplicación; es decir, la versión que contenía las historias de usuario prioritarias. La fase de iteración fue la que requirió mayor esfuerzo, en ella se realizó el desarrollo de cada versión, incluidos el modelado, la programación, las pruebas y la integración de cada versión y finalmente, en la fase de producción se realizaron un conjunto de pruebas para certificar que el sistema estaba listo para pasar a producción. A continuación, se describen las fases de exploración y la de iteración.

2.1 Fase de exploración

Para conocer qué actividades o tareas se requerían automatizar se realizaron una serie de entrevistas con los posibles usuarios (asesores de ventas) y el equipo de desarrollo, como resultado, se obtuvo una lista de historias de usuarios (ver *Tabla 1*). Cada historia fue analizada y en caso de ser necesario refinada; es decir, divididas en un conjunto de funcionalidades de granularidad más fina. Por ejemplo, al analizar la historia no funcional se identificó que era un requerimiento no funcional y al refinarlo se obtuvo el diagrama de casos de uso de la *Figura 2*. Asimismo, al analizar la historia de usuario YY se identificó como un requisito funcional y al refinarlo se obtuvo el diagrama de la *Figura 3*. Los casos de uso se desglosaron en un conjunto de historias de usuarios, asignando a cada una una prioridad, la cual sirve como criterio en la fase de planificación.

Tabla 1

Historias de Usuario

# Historia	Descripción
1	Como administrador quiero tener una traza del número de chat que un asesor tiene con sus clientes
2	Como asesor de ventas quiero comunicarme a través de mensajes o de llamadas telefónicas con mis potenciales clientes
3	Cada asesor quiero consultar su lista de clientes o buscar un cliente en específico
4	Como asesor de venta necesito tener almacenada la información personal y económica de mis clientes
5	Como asesor de venta necesito acceder a través de la aplicación móvil a las funcionalidades del módulo CRM a fin de poder generar prospectos, gestionar los prospectos de cada cliente, gestionar las solicitudes y mandar a imprimir un contrato
6	Como usuario general me gustaría que la aplicación sea fácil de usar, de manera que los usuarios externos y los empleados puedan aprender a usarla rápidamente
7	Como usuario externo necesito poder enviar notificaciones a su asesor de ventas y consultar información general
8	Como desarrollador se requiere que la aplicación permita anexar nuevas funcionalidades y/o modificar las existentes sin que ello amerite realizar cambios significativos en los módulos ya desarrollados
9	Como usuario general requiero que la aplicación móvil pueda ejecutarse en cualquiera de los sistemas operativos que hay en el mercado (IOS, Android, Windows)
10	Como asesor de ventas requiero que únicamente él pueda acceder a la información de sus clientes.
11	El administrador del sistema requiere que para que el sistema no se degrade en tiempos de respuesta se permita un acceso simultáneo de 1000 usuarios

Figura 2

Casos de Uso para el Ingreso Seguro al Sistema

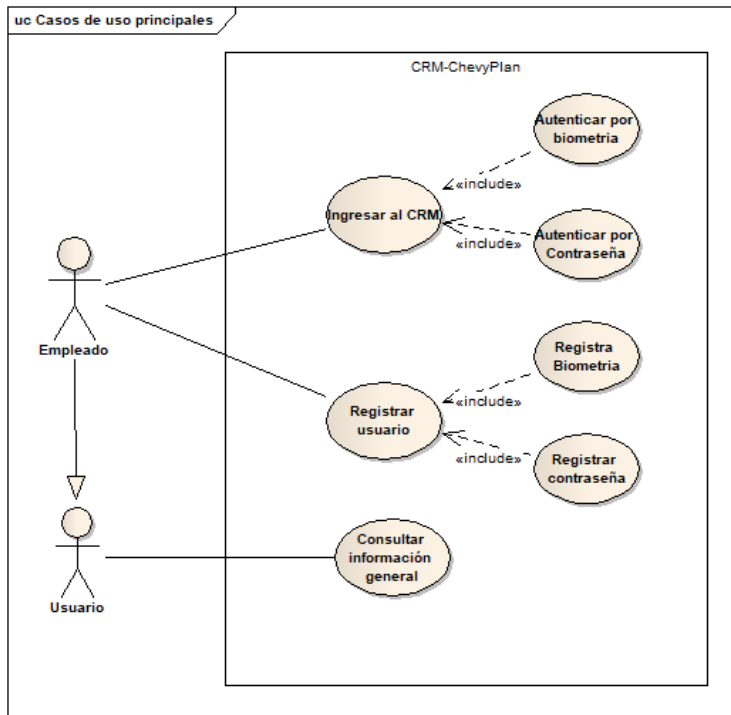
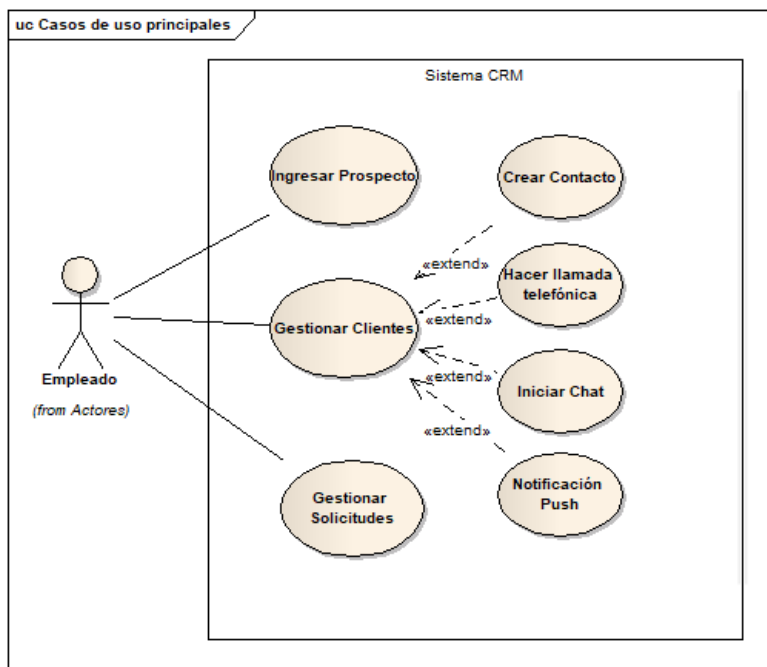


Figura 3

Casos de Uso con las Funcionalidades de la Aplicación Móvil



Adicionalmente, en esta fase se modeló la arquitectura inicial de software, la cual a medida que se desarrolló la aplicación se fue completando y en caso de ser necesario re-factorizando.

2.2 Fase de iteración

En esta fase se ejecutaron tres iteraciones, cada una tuvo una duración de tres semanas. La interfaz de la aplicación móvil se construyó usando HTML5, CSS, JavaScript y XAML (*eXtensible Application Markup Language*), como *framework* de desarrollos móviles se usó Xamarin, la construcción del núcleo se programó en el lenguaje C# y para la comunicación se utilizó el protocolo de las arquitecturas orientadas a servicios SOAP (por sus siglas en inglés).

En la primera iteración se desarrollaron las funcionalidades de ingreso seguro al sistema, en la segunda iteración se elaboraron las fachadas para las funcionalidades de ingresar prospecto, agregar contactos y enviar mensajes; en la última iteración se desarrollaron el resto de las funcionalidades.

Se realizó una autenticación 2FA, realizando como primer paso una autenticación por contraseña y luego la autenticación biométrica (ver *Figura 4*). Para el registro por clave se verifica que la clave cumpla con el patrón establecido (combinación de caracteres, dígitos y símbolos especiales), para posteriormente encriptar y almacenar. Para el desarrollo del módulo de registro y autenticación biométrico se utilizó el algoritmo AES-128 y los datos se almacenaron en el formato PKCS#7, las tareas que se ejecutan para el registro y autenticación biométrica se muestran en el diagrama de actividades de la *Figura 5*.

Figura 4

Diagrama de Secuencias para la Autenticación 2FA

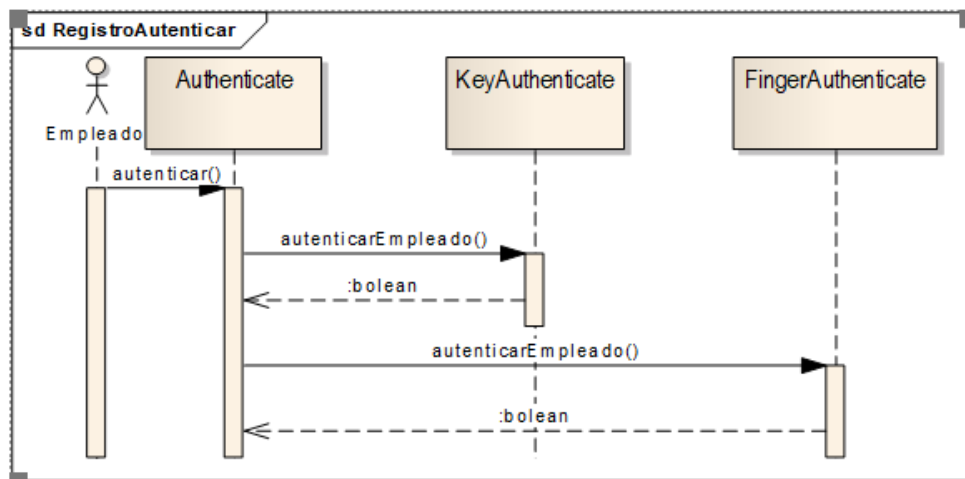
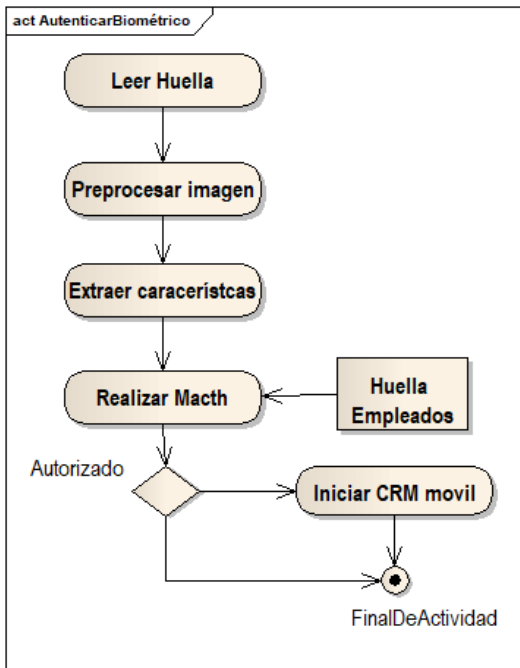


Figura 5

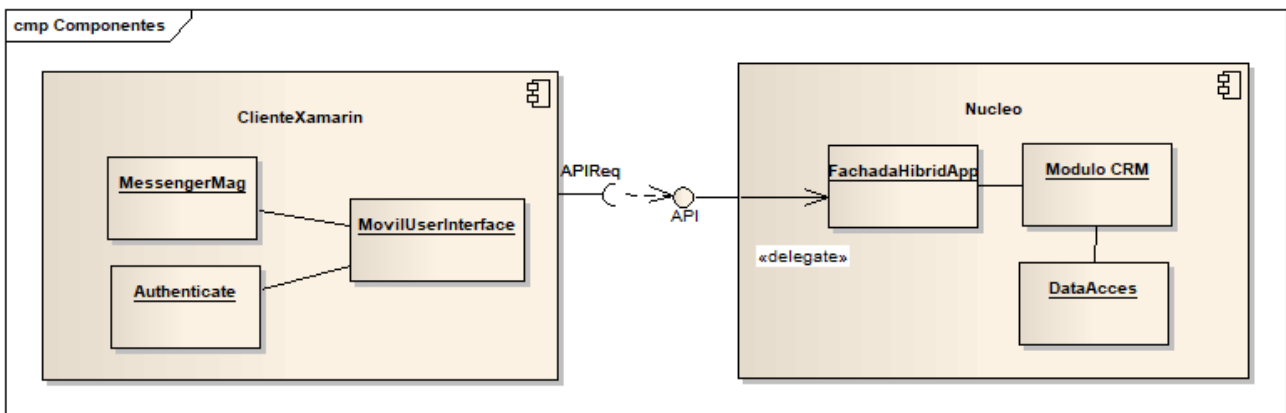
Diagrama de Actividades del Módulo de Autenticación Biométrica



En la iteración dos se realizó el diseño arquitectónico de las funcionalidades para el manejo del sistema CRM. En esta iteración se diseñó la interfaz de la aplicación, la arquitectura de software y con el fin de llevar el registro de acciones que realiza cada usuario, se anexó un nuevo requisito. En la tercera iteración se programaron las funcionalidades restantes y se completó el diseño arquitectónico (ver *Figura 6*) y el modelado de datos. Además, en cada iteración se realizaron las pruebas funcionales y de aceptación necesarias para certificar el funcionamiento de la aplicación.

Figura 6

Diagrama de Componentes de la Aplicación Móvil

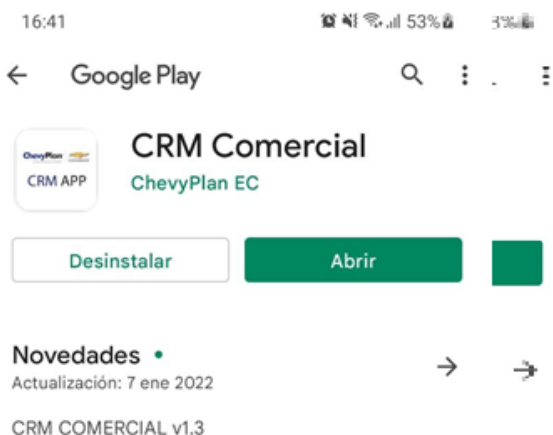


Resultados

Finalizada la fase de producción, la aplicación se subió a la *Google Play Store* a fin de que los usuarios puedan descargar la aplicación, tal como se muestra en la *Figura 7*.

Figura 7

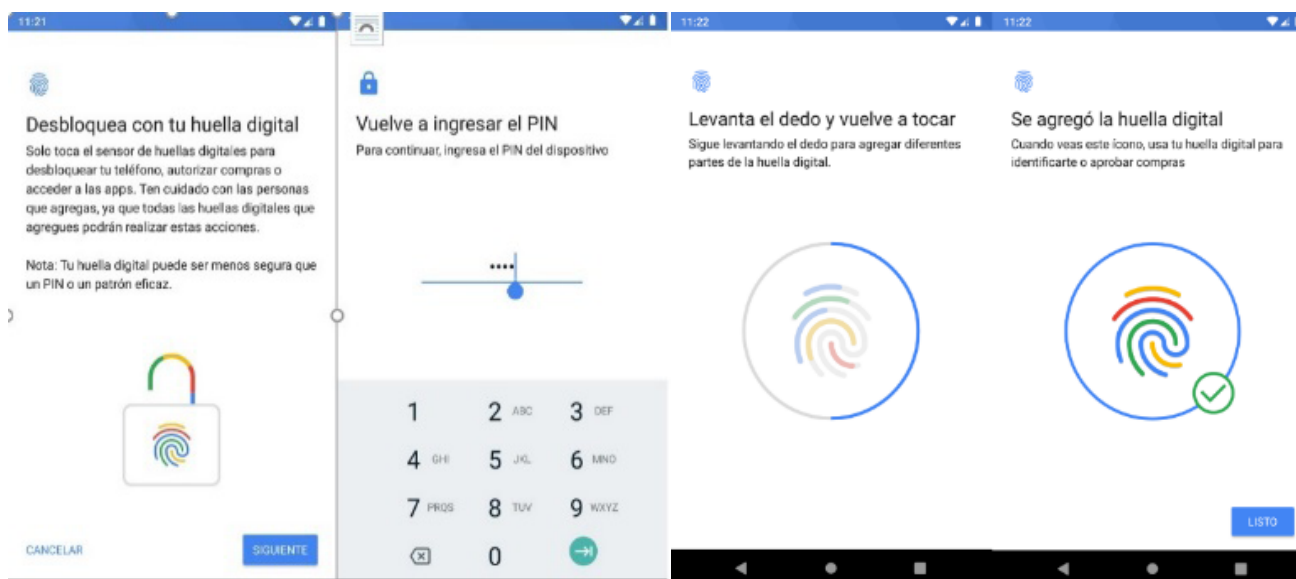
Aplicación Publicada en la Google Play Store



Una vez instalada la aplicación en el teléfono móvil, los empleados se deben registrar para acceder al módulo CRM. Para el registro y almacenamiento de los datos de autenticación la aplicación solicita el nombre de usuario, su clave y la huella, La *Figura 8* muestra la secuencia de interfaces que se presentan para hacer el registro de la huella digital.

Figura 8

Secuencia de Interfaces para el Registro de la Huella Digital



Luego de hacer el registro, el empleado podrá ingresar a la aplicación móvil. Inicialmente, la aplicación presenta el conjunto de funcionalidades que ofrece la aplicación, la *Figura 9* presenta la interfaz de la pantalla inicial, En ella podrá acceder a las funcionalidades del módulo CRM para ingresar nuevos prospectos, gestionar sus contactos (clientes), gestionar las solicitudes realizadas por cada cliente o generar los contratos.

Figura 9

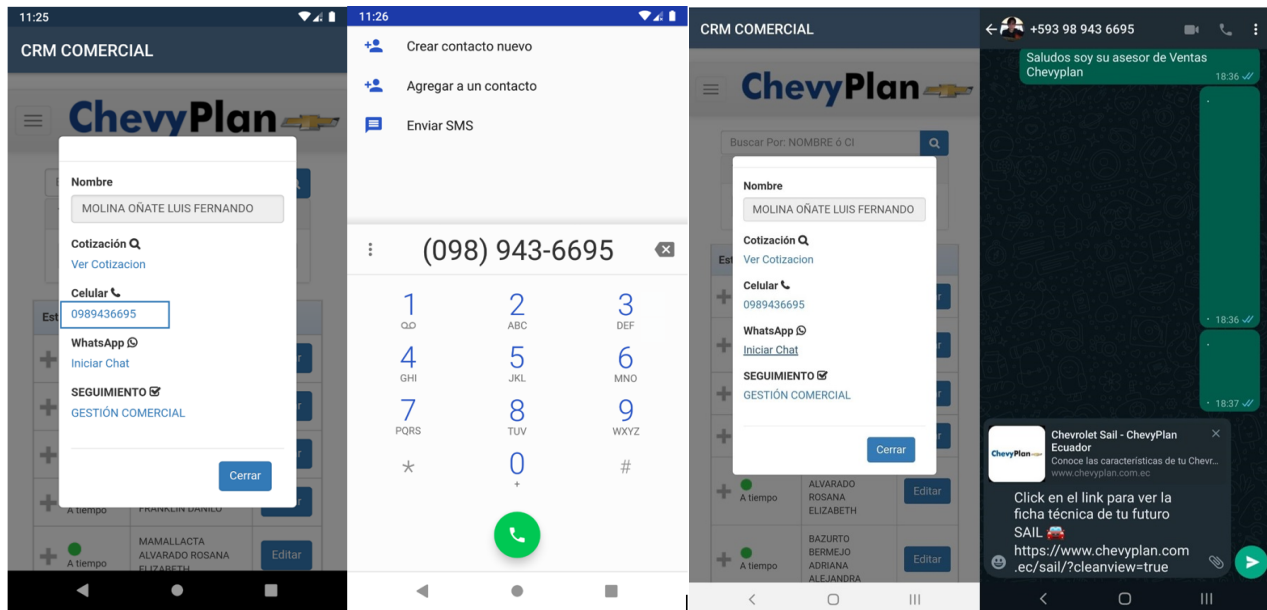
Pantalla de Inicio de la Aplicación Móvil



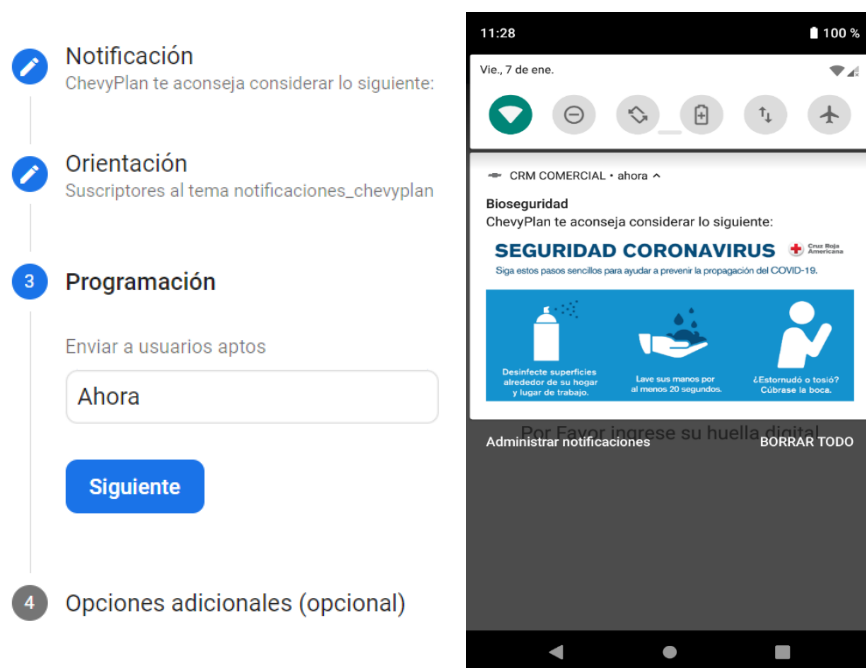
Uno de los requisitos iniciales era que el usuario pudiera comunicarse con el cliente, tanto a través de llamadas telefónicas, como de envío de mensajes de WhatsApp. La *Figura 10* muestra las interfaces para hacer una llamada telefónica, para su construcción se usó el Plugins de Xamarin para usar los componentes básicos de un dispositivo móvil, en este caso el teléfono y la interfaz para la comunicación a través de WhatsApp.

Figura 10

Comunicación entre la Aplicación y el Componente nativo Dial Telefónico y WhatsApp.



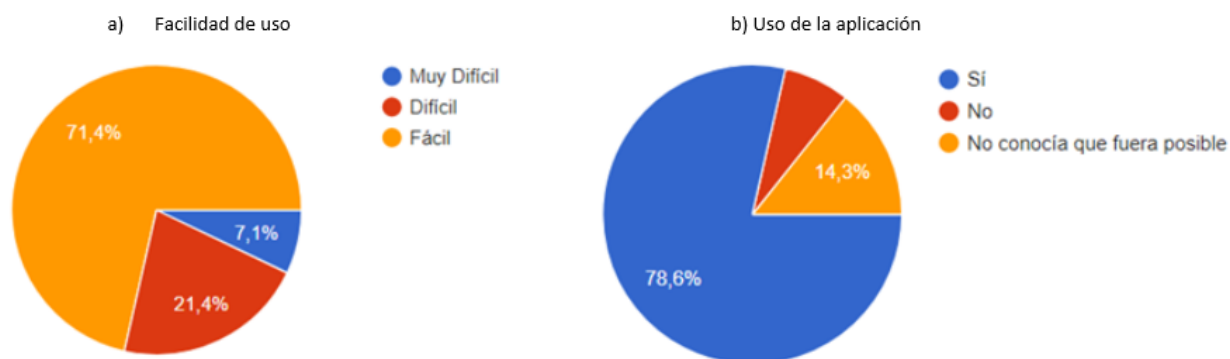
Al contar con una aplicación móvil, el uso de notificaciones y boletines informativos para comunicarse con los usuarios es una buena alternativa, debido a que no es necesario configurar el correo electrónico. Es por ello que las notificaciones *Push* fue un requisito que se incluyó en el sistema, en la *Figura 11* se presenta una de las interfaces que se construyeron para el proceso de envío de notificaciones, esta muestra la configuración de la notificación y la notificación *Push* recibida por el usuario.

Figura 11*Configuración de Notificación y Notificación PUSH Recibida*

Finalmente, para evaluar la aceptación que la aplicación tenía entre los asesores, se encuestaron 65 empleados de un total de 85 empleados que trabajan como asesores de ventas en los diferentes puntos de venta, para ello se utilizó un nivel de confianza del 95%, una varianza de 0,5 y un error del 5%. Los empleados se seleccionaron de forma aleatoria, la encuesta permitió verificar que, en términos de usabilidad (fácil de usar, difícil y muy difícil), el 71% de los usuarios consideraban que la aplicación es de fácil uso. Además, la encuesta refleja que un 78% de los empleados está usando la aplicación para gestionar sus clientes. La *Figura 12* muestra los resultados obtenidos con la pregunta relacionada a la facilidad de uso de la herramienta.

Figura 12

Resultados a las Preguntas de: a) *Facilidad de Uso* b) *Uso de la Aplicación*



Conclusiones

Los teléfonos inteligentes son una herramienta que permiten realizar una variedad de actividades, por lo que las empresas se están moviendo a este tipo de tecnologías, desarrollando aplicaciones que funcionen en estos dispositivos, potenciando de esta forma el trabajo a distancia y reduciendo la necesidad que tienen los empleados de tener una computadora de escritorio para realizar sus actividades. Para ello, el desarrollo de aplicaciones híbridas es una forma efectiva para construir estas aplicaciones, ya que se aprovechan las funcionalidades que ya han sido programadas como servicios permitiendo ahorrar tiempo y dinero. Es por esto que la aplicación móvil desarrollada en este trabajo espera mejorar la productividad de sus empleados y brindar un servicio más personalizado a sus clientes. Este objetivo aún no se ha podido medir, ya que la aplicación tiene solo unos meses en el mercado.

El uso de la doble autenticación garantiza el acceso sólo a personas autorizadas y a pesar que se añade un paso adicional para el ingreso, el tiempo que se consume en la verificación de la huella es tan pequeño que no afectó el tiempo de ingreso al sistema. Sin embargo, es necesario revisar periódicamente los mecanismos de autenticación y encriptación de datos. Por ahora, el uso de la biometría es una manera segura y rápida de autenticación para que los usuarios tengan un rápido acceso al sistema.

Un problema de la aplicación móvil se debe a que esta es una herramienta de trabajo y sólo debería ser utilizada en horas laborables, es decir, que esta debería estar configurada de modo que no se lleve la oficina a la casa. La aplicación necesita manejar un horario de atención a los clientes y así evitar los clientes estén enviando comentarios en horas no laborables.

Referencias

- Acevedo, L., Chávarro, N., y Ramírez, J. (2019). *Smartphones en el desempeño de los empleados de la gerencia de transmisión y distribución de EPM Empresas Públicas de Medellín* [Tesis de Especialización, Corporación Universitaria Minuto de Dios Repositorio]. <https://hdl.handle.net/10656/11480>
- Alanda, A., Satria, D., Mooduto, H., & Kurniawan, B. (2020). Mobile application security penetration testing based on OWASP. In *IOP Conference Series: Materials Science and Engineering*, 846(1). <https://doi.org/10.1088/1757-899X/846/1/012036>
- Ambler, S. (2018). *AM throughout the XP lifecycle*. Ambyssoft Inc. <http://www.agilemodeling.com/essays/agileModelingXPLifecycle.htm>
- Andriani, R., Wijayanti, S., & Wahyu, F. (2018). Comparison of AES 128, 192 And 256 Bit Algorithm for Encryption and Description File. En *2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE)*, (pp. 120-124). IEEE. <https://doi.org/10.1109/ICITISEE.2018.8720983>
- Chen, Y., Wang, Q., Chen, H., Song, X., Tang, H., & Tian, M. (2019). An overview of augmented reality technology. *Journal of Physics: Conference Series*. 1237(2). <https://doi.org/10.1088/1742-6596/1237/2/022082>
- Contreras, J., Peña, O., y Santillan, G. (2019). Aplicaciones híbridas para dispositivos móviles como herramienta en el sector empresarial. *Revista Ciencia Administrativa*, 5, 146 - 152.
- Guo, Y., Yin, C., Li, M., Ren, X., & Liu, P. (2018). Mobile e-commerce recommendation system based on multi-source information fusion for sustainable e-business. *Sustainability*, 10(1), 147. <https://doi.org/10.3390/su10010147>
- Hidayat, R. (2014). Goods Expedition Information System Using ECRM Method to Improve Customer Service. *Global Sisfotek Journal*, 4(2), 41-45.
- Ibáñez, A., Montesinos, M. C., Morales, C., y Pacheco, E. (2022). Uso de Dispositivos Electrónicos en las Actividades Laborales durante la Pandemia COVID-19. En *Congreso Internacional de Investigación Academia Journals*, (pp. 220-225). Academia Journals.
- ISOTools Excellence. (s.f.). La norma ISO 9001 2015 ¿En que se basa el ciclo PHVA? <https://www.isotools.com.co/la-norma-iso-9001-2015-se-basa-ciclo-phva/>
- Javaid, M., & Haleem, A. (2020). Virtual reality applications toward medical field. *Clinical Epidemiology and Global Health*, 8(2), 600-605. <https://doi.org/10.1016/j.cegh.2019.12.010>

- Karakaya, N., Alptekin, G. I., & İncel, Ö. (2019). Using behavioral biometric sensors of mobile phones for user authentication. *Procedia Computer Science*, 159, 475-484. <https://doi.org/10.1016/j.procs.2019.09.202>
- Kulkarni, P. V., Rai, S., & Kale, R. (2020). Recommender system in elearning: a survey. In Springer (Ed.) *Proceeding of International Conference on Computational Science and Applications*, (pp. 119-126). https://doi.org/10.1007/978-981-15-0790-8_13
- Morales, A., y Aguado, C. (2022). *Transformación digital en las empresas: Un enfoque desde la administración de la teoría a la práctica*. Ecoe Ediciones.
- Nayyar, A., Mahapatra, B., Le, D., & Suseendran, G. (2018). Virtual Reality (VR) & Augmented Reality (AR) technologies for tourism and hospitality industry. *International journal of engineering & technology*, 7(2), 156-160.
- O’Dea, S. (2021). Forecast number of mobile users worldwide from 2020 to 2025 (in billions). *Statista* <https://www.statista.com/statistics/218984/number-of-global-mobile-users-since-2010>.
- Organización de Naciones Unidas para la Alimentación y Agricultura. (2015). Plantilla de buenas prácticas. *FAO* <https://www.fao.org/3/as547s/as547s.pdf>
- Padeli, P., Mulyati, M., Faisal, M., & Debora, S. (2020). E-CRM Mobile Applications To Improve Customer Loyalty (Case Study: PT Supermal Karawaci). *Aptisi Transactions on Management (ATM)*, 4(1), 41-48. <https://doi.org/10.33050/atm.v4i1.1083>
- Ramírez, R. (2019). *Métodos para el desarrollo de aplicaciones móviles*. Universidad Oberta de Catalunya.
- Ranjan, Y., Rashid, Z., Stewart, C., Conde, P., Begale, M., Verbeeck, D., Boettcher, S., Hyve, T., Dobson, R., Folarin, A., & Consortium, R.-C. (2019). RADAR-base: open source mobile health platform for collecting, monitoring, and analyzing data using sensors, wearables, and mobile devices. *JMIR mHealth and uHealth*, 7(8). <https://doi.org/10.2196/11734>
- Rodríguez, O., Legón, C., y Socorro, R. (2018). Seguridad y usabilidad de los esquemas y técnicas de autenticación gráfica. *Revista Cubana de Ciencias Informáticas*, 12, 13-27. http://scielo.sld.cu/scielo.php?pid=S2227-18992018000500002&script=sci_arttext&tlng=pt
- Sadaf, S., Singh, V., & Iyappan, I. (2020). Robust biometric authentication system with a secure user template. *Image and Vision Computing*, 104. <https://doi.org/10.1016/j.imavis.2020.104004>
- Sala, N. (2021). Virtual Reality, Augmented Reality, and Mixed Reality in Education: A Brief Overview. En *Current and Prospective Applications of Virtual Reality in Higher Education*, (pp. 48-73). IGI Global. <https://doi.org/10.4018/978-1-7998-4960-5.ch003>

- Simram, S. (2020). Rest House Hybrid Mobile Application using Ionic Tool. *International Research Journal of Engineering and Technology*, 7(4), 45-50.
- Tan, T. N., & Lee, H. (2019). High-secure fingerprint authentication system using ring-LWE cryptography. *IEEE Access*, 7, 23379-23387. <https://doi.org/10.1109/ACCESS.2019.2899359>
- Turek, M. (03 de agosto de 2016). Employees Say Smartphones Boost Productivity by 34 Percent: Frost & Sullivan Research. *Insights samsung* <https://insights.samsung.com/2016/08/03/employees-say-smartphones-boost-productivity-by-34-percent-frost-sullivan-research/>



Copyright (2023) © Dulce Rivero Albarrán, Laura Rosa Guerra Torrealba y Luis Fernando Molina Oñate



Este texto está protegido bajo una licencia internacional [Creative Commons](#) 4.0.

Usted es libre para Compartir—copiar y redistribuir el material en cualquier medio o formato — y Adaptar el documento — remezclar, transformar y crear a partir del material—para cualquier propósito, incluso para fines comerciales, siempre que cumpla las condiciones de Atribución. Usted debe dar crédito a la obra original de manera adecuada, proporcionar un enlace a la licencia, e indicar si se han realizado cambios. Puede hacerlo en cualquier forma razonable, pero no de forma tal que sugiera que tiene el apoyo del licenciante o lo recibe por el uso que hace de la obra.

[Resumen de licencia](#) – [Texto completo de la licencia](#)