Doble autenticación utilizando software móvil de lectura de código QR

Double authenyocayion using mobile QR code reader software

Recibido: diciembre 18 de 2022 | Revisado: abril 25 de 2023 | Aceptado: mayo 05 de 2023

Nicolás Vegas[1]
Christopher Cabrera[2]
José Espinoza[3]
Alberto Mendoza[4]

Resumen

En la actualidad, las empresas manejan mucha información sensible día a día, misma que puede ser deseada por personas inescrupulosas con la finalidad de obtener beneficio propio, haciendo daño a las empresas y clientes. Este artículo científico se enfoca en el desarrollo de inicio de sesión con doble autenticación, haciendo uso de las credenciales de usuario y de la lectura de un código QR mediante el software móvil complementario instalado en un dispositivo verificado. Esto brinda al lector un panorama de la seguridad de la información donde se destaca, principalmente, el uso de códigos QR encriptados, el cual, a diferencia de la lectura dactilar o detector facial es de suma accesibilidad en la mayoría de dispositivos móviles con cámara y en distintos sistemas operativos. También se puede destacar el uso de API REST para comunicar la aplicación web con la aplicación móvil. La aplicación muestra ser una forma sencilla y efectiva de mejorar la seguridad del inicio de sesión para cualquier empresa.

Palabras clave: Doble autenticación, inicio de sesión, API REST, aplicación

Abstract

Currently, companies handle a lot of sensitive information daily, which may be desired by unscrupulous people in order to obtain their own benefit, harming companies and customers. The paper focuses on the development of a login solution with double authentication, making use of user credentials and reading a QR code, through complementary mobile software installed on a verified device. The work provides the reader with an overview of information security, where the use of encrypted QR codes stands out, which, unlike fingerprint reading or facial detection, is extremely accessible on most mobile devices with cameras. and on different operating systems. You can also highlight the use of REST APIs to communicate the web application with the mobile application. The app proves to be a simple and effective way to improve login security for any business.

Keywords: Double Authentication, login, API REST, software

1 Departamento de Ingeniería de Sistemas, Universidad Nacional de Trujillo, Trujillo – Perú
2 Departamento de Ingeniería de Sistemas, Universidad Nacional de Trujillo, Trujillo – Perú
3 Departamento de Ingeniería de Sistemas, Universidad Nacional de Trujillo, Trujillo – Perú
4 Departamento de Ingeniería de Sistemas, Universidad Nacional de Trujillo, Trujillo – Perú

Autor para correspondencia
E-mail: nvegas@unitru.edu.pe

https://doi.org/10.24265/campus.2023.v28n35.04

Introducción

Actualmente, la seguridad de los datos es uno de los temas más llamativos en el campo del desarrollo de aplicaciones móviles, programas web o programas de escritorio por la cantidad de información que se está manejando en estos medios. El guardar datos tan importantes como la tarjeta de crédito en una aplicación, dirección de hogar en un registro, cuenta bancaria hace que los usuarios se vean afectados si la información se filtra. Esta situación se hace notaria, especialmente, en el Perú donde las empresas suelen tener un muy bajo nivel de seguridad y se ve reflejado en una alta tasa de fuga de información sensible, principalmente, en las entidades estatales (Alcántara, 2015).

Por otra parte, la vulnerabilidad de la información es un fenómeno que no solo se presenta en estas instituciones, sino que es un problema que se encuentra en las entidades privadas de igual forma, (Vargas, 2021). Por lo tanto, este tipo de problema conlleva a varios tipos de efectos como son los financieros y sociales para las instituciones, el cliente y hasta para el propio país (Pereira et al., 2013).

En el Perú, ha sido noticia en reiteradas ocasiones que se vulneraron las cuentas de usuarios de RENIEC, EsSalud y otras entidades importantes debido a la baja seguridad que existe actualmente. Los hackers que hicieron esto, filtraron información como fotos, direcciones y números de teléfono aparte de reportar como fallecidos a las personas que sus clientes elegían por un precio sumamente bajo debido a la facilidad con la que accedían a estas cuentas. Los usuarios suelen usar las mismas credenciales para todas sus cuentas, esto hace que al vulnerarse estas credenciales en una página no segura se puedan usar en la página de la entidad en la que trabajan.

Al no haber una política de contraseñas seguras o una segunda autenticación, se suelen vulnerar de forma simple las cuentas de los usuarios. Con el objetivo de verificar las credenciales de los usuarios y a la vez que efectivamente estos sean los que están ingresando al sistema, se propone mejorar la seguridad y supervisión, el desarrollo de un software de doble autenticación mediante el dispositivo móvil verificado de cada usuario a través del uso de un código QR encriptado.

En este artículo, se presenta el desarrollo de un sistema de doble autenticación usando dos dispositivos, uno será la computadora desde donde se busca acceder y el otro un dispositivo móvil que contará con una aplicación que permitirá escanear el QR mostrado por la computadora permitiendo así recién el acceso con el objetivo de evitar así algún tipo de filtración de datos. De esta manera, el modelo sirve como un medio de seguridad para los sistemas de administración y seguridad de las empresas o instituciones.

Método

Para el desarrollo del proyecto se hizo uso de la metodología de desarrollo ágil Scrum. En el desarrollo de Software existen cambios constantes a nivel práctico, esto generado por las nuevas tecnologías que salen a la luz día a día. Para ello, es necesario elegir una correcta metodología al momento de desarrollar una nueva tecnología, así como las herramientas que se harán uso para el desarrollo. Scrum es una metodología de

desarrollo ágil reconocida a nivel mundial que resalta el trabajo en equipo y su flexibilidad a cambios (Takeuchi, Nonaka, 1986). Las metodologías tradicionales se han concentrado principalmente, en planear las actividades desde el principio hasta el final, por ejemplo: análisis de requerimientos, diseño, construcción, pruebas y entrega.

Además, Scrum está dividido en iteraciones cortas donde el producto se desarrolla por partes dando en cada iteración un aumento de funcionalidades hasta llegar al proyecto final (Rodríguez, Dorado. 2015). Para el actual proyecto se eligió esta metodología por la facilidad y flexibilidad que permite al momento del desarrollo en grupo, repartición de tareas y retroalimentación. Nosotros dividimos el trabajo en tres sprints, cada uno con una duración de una semana, mientras que para el desarrollo se usó GitHub por la división en ramas que permite.

El primer paso de la metodología se desarrolla en la planificación o Product Backlog, donde se establecen las tareas que se realizarán, luego, se ejecutan los Sprints donde se desarrollan las tareas establecidas en el Product Backlog. Por último, la metodología cuenta con una fase de control o también denominada Burndown. En esta fase, se compara el progreso del proyecto con el ideal establecido. En resumen, esta metodología se basa en el trabajo en equipo y cambio constante, siguiendo una serie de criterios para obtener un mejor resultado en el proyecto.

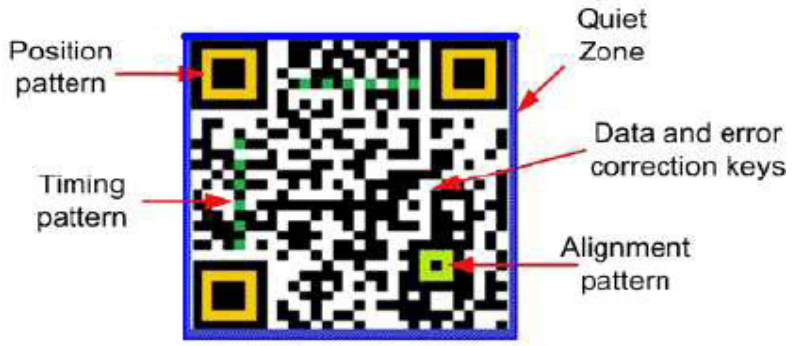
Código QR

La decisión de usar códigos QR surgió por un estudio previo que realizó el equipo para seleccionar una tecnología que se adapte a los dispositivos actuales como podrían ser los dispositivos móviles o los sensores, y que suministre datos a la capa de aplicación. Se consideraron los siguientes requisitos:

- Ser de código libre y gratis.
- No depender de un solo sistema operativo o sensor.
- Altamente accesible a través de la cámara de cualquier dispositivo móvil.
- Sencillo de implementar en dispositivos móviles y bases de datos ya desarrolladas.
- Sencillo de usar por desarrolladores.

Un código QR (Quick Response) o también conocido como código abierto es un sistema de almacenamiento de información en una matriz de puntos blancos y negros que en conjunto forman un código de barras bidimensional que se puede presentar de forma impresa o en una pantalla de tal forma que son interpretables por aparatos capaces de captar imágenes y que cuenten con el software adecuado para desencriptación de estos (Huidobro, J., 2019).

Figura 1
Componentes de un código QR



En sus inicios, los códigos QR se desarrollaron para ser aplicados en la industria japonesa de componentes de automóviles, pero a lo largo de los años su uso se ha ido expandiendo, llegando a servir como carta en restaurantes, ingreso a páginas web o método de validación para entrada a cuentas privadas. Un código QR puede almacenar información final o ser un intermediario; en el caso de ser información final, se obtendrán datos al escanear un QR ya sea como el número de teléfono de alguien, una dirección o un JSON. De otro modo, en caso de ser intermediario, nos redireccionará a una URL donde podremos encontrar información variada. (Leiva-Aguilera, J, 2012)

Estos códigos están compuestos por distintas partes, el elemento más pequeño (cuadrado negro o blando) es llamado módulo, los códigos QR están formados por una combinación de módulos, patrones de detección de tiempo, patrones de detección de posición, un código de corrección de errores y un área de datos. (Figura 1) Los patrones de detección de posición de los QR están ordenados en tres esquinas, en el caso de los Micro QR solo tienen uno.

Utilización del Código QR

La popularización de los dispositivos móviles, como los Smartphone, tablets, etc., han facilitado la creación de distintas alternativas dentro del marketing móvil como por ejemplo, la tecnología NFC o los códigos bidimensionales (Andrés G. 2012). En este proceso de avance tecnológico, se ha ido fortaleciendo el uso de los códigos QR hasta volverse parte del uso diario. Lo estándar para los códigos QR es almacenar información, esto permite darle diversos usos, entre ellos, la posibilidad de ser usados como medio de seguridad de información ya sea como un método de encriptación de información dando un doble candado a nuestra información que deseamos enviar o una vía de autenticación.

Asimismo, la posibilidad de almacenar información en un QR permite el envío de código JSON creando una estructura capaz de cargar con la información de verificación de un usuario, como por ejemplo: el nombre del usuario, el dispositivo donde se conecta, la fecha, hora, etc., en base a esto la encriptación de un código que distingue el inicio de sesión es posible de tal manera que se cree un código que sea necesario leer para el ingreso de cada usuario y este deba

ser leído por una aplicación móvil capaz de desencriptar esa información y mostrarla en pantalla.

En la actualidad, los dispositivos y las habilidades informativas de las tecnologías móviles cuentan con una alfabetización informacional a través de los dispositivos móviles que permiten obtener todo tipo de información ya sea por medio de la red o por medio local (León M. 2013). Esto incluye la posibilidad de abstraer información de manera sencilla por medio del uso de la cámara de nuestro dispositivo móvil, por ello es que la aplicación de los código QR se han visto en aumento, dando posibilidad a nuevos usos en las tecnologías actuales.

A fin de crear aplicaciones seguras o nuevos métodos en la ciencia de la seguridad de la información se propone aquí la creación de un nuevo método de autentificación que permita mejorar la seguridad de los datos, evitar las entradas por fuerza bruta al sistema y mantener una integridad en los sistemas de información. Esto permitirá disminuir los riesgos de las organizaciones de que se filtren datos importantes o se pueda alterar algún registro, por la poca posibilidad de que algún hacker pueda ingresar a la cuenta de algún empleado.

Al contar con la necesidad del uso del dispositivo móvil registrado en la aplicación que se encuentra aislado por completo del sistema de la organización, el ciber atacante tendrá que contar con el dispositivo para lograr ingresar a la cuenta. Otra de las funcionalidades que favorece el uso de esta tecnología es la posibilidad de denegar el acceso a la cuenta y mostrar el IP del intento de acceso, dando pista de quién está intentando acceder a la información, quedando este registro guardado para ser analizado posteriormente.

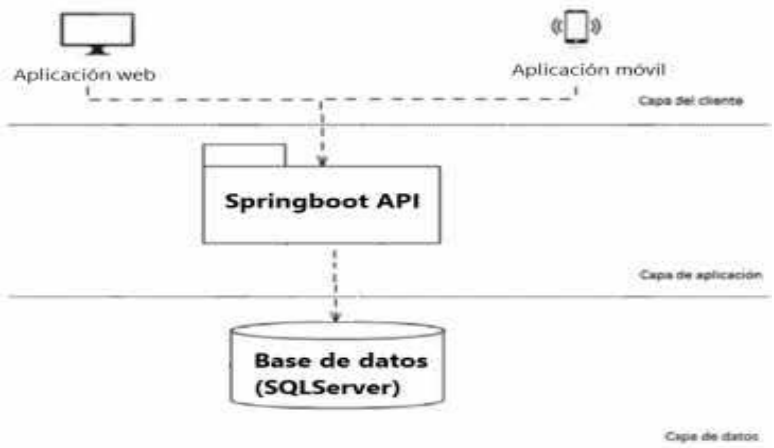
Resultados

Descripción de la aplicación desarrollada

La solución propuesta en este trabajo es una aplicación de doble autenticación (Figura 2), la cual se conecta a la base de datos de la empresa en la que los usuarios trabajan para que puedan acceder a su sistema mediante el ingreso de credenciales y la lectura del código QR desde un dispositivo verificado.

Figura 2

Arquitectura de la aplicación



Para el desarrollo de esta solución se trabajó con dos aplicaciones: una web y otra móvil. Para la aplicación web se trabajó con React, afianzado con Bootstrap 5 y otros componentes como react-qr-code para la generación y encriptación del código QR. Por la parte de la aplicación móvil, se desarrolló con Kotlin, haciendo uso de una arquitectura MVVM (Model View ViewModel). Estas dos aplicaciones se encuentran enlazadas con un API trabajado con Springboot que se encarga de la desencriptación del código QR y el envío de respuestas para la validación del ingreso de sesión.

Por último, se hizo uso de una base de datos en SQLServer para el almacenamiento de los datos de las sesiones, usuarios y solicitudes de inicio de sesión. El sistema operativo elegido para la aplicación móvil fue Android por la facilidad que otorga el desarrollo en Kotlin y el manejo de sus versiones resultó ser más asequible para la investigación, además de ser gratuito y contar con accesibilidad al uso de cámara.

Figura 3
Login de aplicación web

El proceso que se desarrolló para la autenticación empieza en el login del aplicativo móvil donde se requiera un usuario y contraseña, una vez creado el usuario se procede a ingresar al aplicativo para que se guarde el token del dispositivo que posteriormente será usado para la validación (Figura 3). El token del dispositivo móvil es almacenado en la base de datos, guardándolo con un respectivo ID y su token que servirá para enviar las notificaciones de ingreso de sesión al dispositivo.

Figura 4
Solicitud de acceso de aplicación móvil

Luego, se procede a iniciar sesión en la aplicación web, una vez confirmado que tanto el usuario y contraseña sean los correctos. Dentro de la base de datos se guarda en la tabla de acceso: la fecha del ingreso, el identificador del acceso, una clave aleatoria y el token del dispositivo. Una vez realizado este proceso, la API desarrollada realizará dos acciones, primero enviará la notificación al dispositivo móvil registrado por medio de Firebase Messaging. Para ese acceso preguntará si se desea admitir el acceso o denegarlo, mostrando a la vez el IP del

dispositivo del cual se está intentando acceder como se muestra en la Figura 4. Por otro lado, se enviará un JSON a la página web con el identificador del acceso y la clave secreta con una encriptación AES (Advanced Encryption Standard). La aplicación web haciendo uso del plugin QR Validator interpretará el JSON recibido como si fuera un código QR para poder mostrarse en la pantalla del dispositivo y a la vez mostrando un temporizador de un minuto para validar el acceso.

Por último, en el dispositivo móvil, en caso se apruebe el acceso, se le pedirá leer el QR, una vez leído el QR, es enviado a la API para ser desencriptado y validará si el acceso es correcto o no. Una vez validado, se recibe una notificación a la web para conceder el permiso de inicio de sesión. En caso contrario, aparecerá una notificación de dispositivo rechazado en la aplicación web.

Validación de la solución propuesta

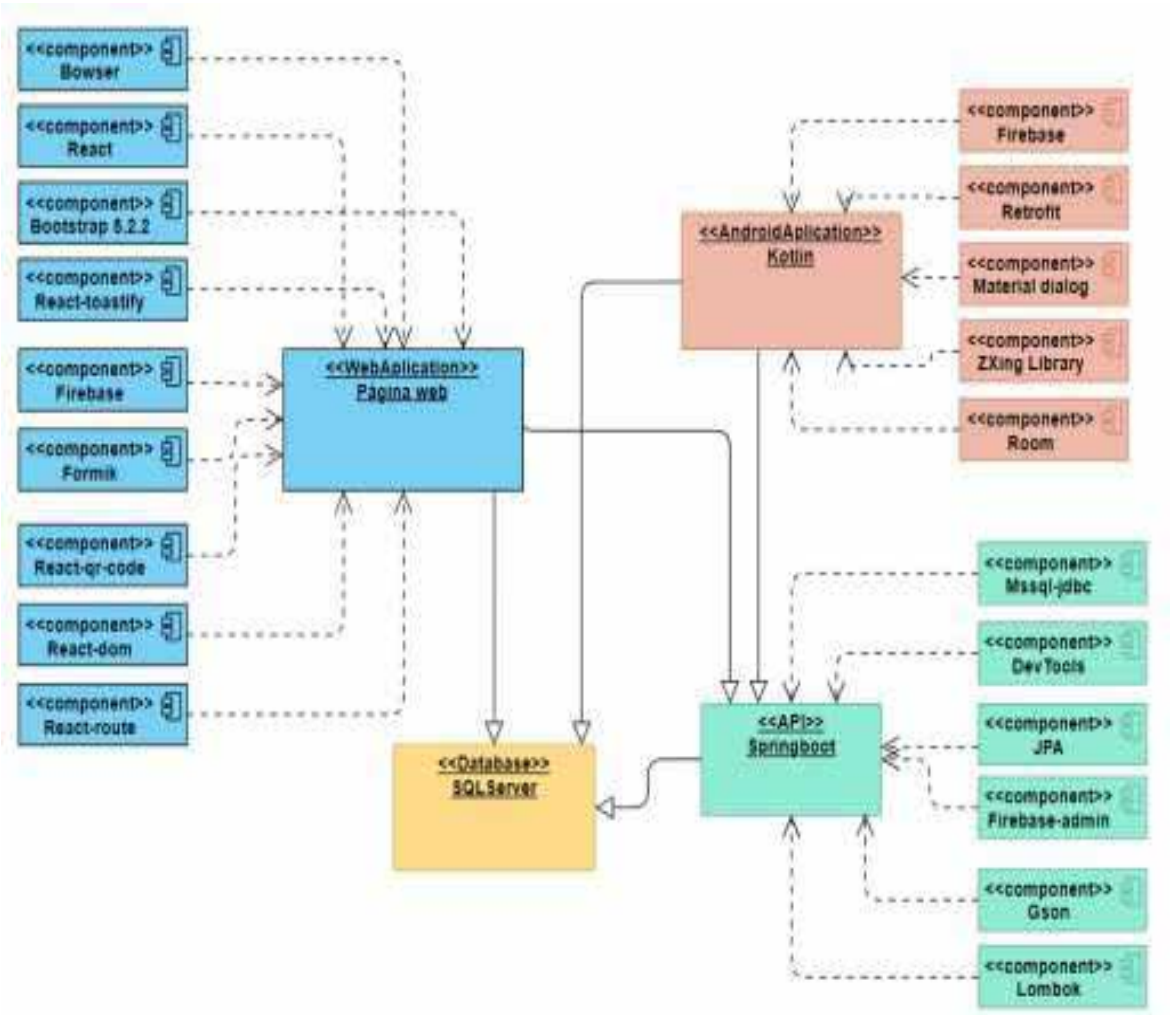
La aplicación de prueba desarrollada muestra un ejemplo de cómo se realizaría una autenticación en dos pasos basada en dos dispositivos y el escaneo de un código QR que contendría los datos necesarios para el inicio de sesión, así como la información necesaria para el seguimiento en caso de un posible hackeo.

Esta aplicación se basa en el formato de peticiones y respuestas de la API desarrollada que se realiza a través de una página web y un dispositivo móvil. Para el servidor en el caso de las pruebas fue necesario el uso de Ngrok. Además, las operaciones realizadas por la aplicación completa constan de las siguientes descripciones: 1. Creación de sesión, 2. Validación de sesión, 3. Creación de QR, 4. Inicio de sesión.

Diseño de la aplicación

La aplicación estará formada por componentes que en conjuntos y gracias a la estructura trabajada serán capaces de intercambiar información en todo momento sin tener limitaciones en la cantidad de recepción y envío de información; como se mencionó anteriormente, consta de tres partes: una aplicación web, una móvil y una API. El desarrollo de la aplicación web se basó en React y sus distintos componentes como React-qr-code que permitió la codificación del código QR, o React-route que permitió el ruteo de las direcciones de la página web. Para el desarrollo de la parte Frontend del aplicativo, se usó Bootstrap en su versión 5.2.2 y Formik para el desarrollo de formularios, Figura 5. En el desarrollo de la aplicación móvil se usó ROOM para la conexión a base de datos, el escaneo del código QR fue implementado haciendo uso de ZXing Library y para el uso de la API se usó Retrofit, permitiendo el intercambio de información entre la aplicación web y móvil.

Figura 5
Diagrama de componentes de la aplicación



Por último, la API donde se realiza tanto la codificación como la encriptación de los ingresos de sesión se desarrolló principalmente en Springboot; haciendo uso de Gson se pudo realizar la creación de JSON que pueda ser interpretado por la aplicación web para la creación del código QR, mientras que la conexión a la base de datos fue implementada con mssql-jdbc. En conjunto, el uso de estas librerías y la conexión entre la API y base de datos entre ellas fueron la estructura en la que se desarrolló la aplicación de prueba con una base sencilla donde se tiene como objetivo que pueda ser implementada en bases de datos ya desarrolladas teniendo una implementación simple y eficaz para mejorar la seguridad de las aplicaciones de administración de información en las empresas.

Aplicación de pruebas unitarias

Para realizar pruebas unitarias a la aplicación desarrollada y demostrar el funcionamiento de este, se crearon una serie de usuarios y se probó desde distintos dispositivos móviles registrados con cada cuenta. Los resultados obtenidos se pueden observar en las Figuras 4 y 5 donde se muestra la vista al iniciar sesión desde la aplicación web y la vista en la aplicación móvil una vez ya recibida la notificación de acceso.

En todas las pruebas, se obtuvieron resultados satisfactorios, demostrando que la propuesta muestra consistencia y aumento de seguridad.

Evaluación del uso de la solución propuesta

Tras realizar las pruebas de la aplicación desarrollada, se comprobó la resistencia de seguridad que presenta la autenticación por medio de QR, pues al contar con una encriptación al iniciar sesión hace que sea difícil de vulnerar y la necesidad de contar con el dispositivo móvil asociado a la cuenta disminuye el riesgo de algún hackeo de cuenta. En ese contexto, es necesario preservar la información e integridad de un sistema informático. Es algo importante para toda organización puesto que puede traer pérdidas tanto económicas como de tiempo, sin ignorar el peligro que conlleva el acceso no autorizado a alguna cuenta de usuario (Alegre R. 2011), es por ello que el desarrollo de nuevas tendencias y métodos para resguardar la información ha ido en aumento en los últimos años. Añadir una segunda validación para el ingreso a una cuenta agrega una defensa más que cuenta con una capacidad de vulneración muy baja, por lo que la solución propuesta es viable para casi cualquier base de datos por su fácil implementación, gracias a la API desarrollada.

Conclusiones

La aplicación desarrollada permite crear y gestionar una solución inteligente y segura a partir de la comunicación mediante una API desarrollada desde cero 0 la cual se comunica con la base de datos de la empresa seleccionada. De esta forma, se comparan las credenciales introducidas con los datos de inicio de sesión almacenados en la base de datos de la empresa que utilice nuestra solución. La aplicación móvil resulta ser efectiva para realizar el proceso de doble autenticación debido a la capacidad de desencriptar el código QR para completar el segundo paso de inicio de sesión. La solución mejora, notablemente, la seguridad de las empresas que la utilizan, sean entidades privadas de renombre o entidades del estado.

Esta es una simple pero efectiva forma de tener una seguridad más robusta en cualquier login.

Agradecimientos

A la revista peruana CAMPUS y a la Universidad de San Martín de Porres, por darnos la capacidad de compartir nuestra solución a todos los lectores. A los profesores y compañeros de la carrera de Ingeniería de Sistemas de la Universidad Nacional de Trujillo, Perú, por el constante apoyo en la realización del presente trabajo.

Referencias

Alcántara Flores, J. C. (2015). Guía de implementación de la seguridad basado en la norma ISO/IEC27001, para apoyar la seguridad en los sistemas informáticos de la Comisaría del Norte PNP en la ciudad de Chiclayo.

Alegre Ramos, M. D. P., & García-Cervigón Hurtado, A. (2011). *Seguridad informática*. Editorial Paraninfo.

Andrés García, J. C., & Okazaki, S. (2012). El uso de los códigos QR en España. *Distribución y consumo*.

Huidobro, J. M. (2009). Código qr. *Bit, dic.-ene*, *172*, 47-49.

Leiva-Aguilera, J. (2012). Introducción y algunos usos de los códigos QR. *Anuario ThinkEPI*, *6*, 309-312.

León-Moreno, J. A., & Caldera-Serrano, J. (2013). Códigos QR en las bibliotecas. *Ciencias de la Información*, *44* (1).

Pereira, R. T., Romero, A. C. and Toledo, J. J.(2013). Descubrimiento de perfiles de deserción estudiantil con técnicas de minería de datos. *Revista vínculos,10* (1):373- 383.

Rodríguez, C., & Dorado, R. (2015). ¿Por qué implementar Scrum? *Revista Ontare*, *3*(1), 125-144.

Vargas Suarez, D. A. (2021). Sistema para el registro y control de los profesionales del Colegio Colombiano de Archivistas.