

## DISEÑO DE SISTEMA DE AUTORIZACIÓN DE MANEJO DE RESULTADOS DE PRUEBAS DE COVID-19 PARA PLATAFORMAS DE RASTREO DE CIUDADANOS CON RIESGO DE CONTRAER EL VIRUS POR CONTACTO CON CONTAGIADOS

**Nombre de los estudiantes**  
González Meza Mónica Isabel

Trabajo de Investigación o Tesis Doctoral como requisito para optar el título de Especialista en Ingeniería de Software

Tutores  
**Paul Sanmartín**

### RESUMEN

**Antecedentes:** Actualmente, los sistemas de rastreos de posibles contagiados de COVID-19 han sido de gran utilidad en el proceso de detener la pandemia de dicha enfermedad, y sus pilares son la recolección de resultados de COVID-19 y el listado de personas con las que, las personas positivas, pudieron haber tenido contacto. Los resultados de análisis de laboratorio, al igual que cualquier otra información concerniente a la intimidad de una persona, es considerado dato sensible según la ley estatutaria 1581 del 2012, y su tratamiento está prohibido si no se cuenta con autorización previa del titular, y demás artículos incluidos en el título IV de la misma ley.

Si bien hay algunas condiciones que flexibilizan el uso de datos personales, las plataformas de rastreo pueden ser desarrolladas por terceros, lo que, en los términos de la legislación, hace referencia al título IV, artículo 13, inciso C, que hace referencia a que los datos que reúnan las condiciones preestablecidas, podrán ser compartidas a terceros únicamente autorizados por el titular o por la ley.

**Objetivos:** El objetivo general del proyecto es diseñar un sistema de autorización de manejo de resultados de pruebas de covid-19 para plataformas de rastreo de ciudadanos con riesgo de contraer el virus por contacto con contagiados, y como objetivos específicos se tienen identificar las funciones que debe tener un sistema de autorización de datos sensibles según las normativas vigentes y modelar y diseñar el sistema de autorización de datos personales, según los requerimientos

**Materiales y Métodos:** Para el cumplimiento de los objetivos de la propuesta, se emplea una metodología cualitativa, para determinar los requerimientos funcionales

basados en la revisión del marco legal colombiano en materia de protección de datos personales sensibles y los requerimientos no funcionales en base a estándares de seguridad, que pueda ser adaptado a la aplicación de rastreos de contagios por COVID-19. Los requerimientos funcionales, se basan en la revisión literaria de leyes colombianas orientadas al tratamiento de usos personales, y se emplean diagramas UML para modelar el proceso de autorización.

**Resultados:** El diseño propuesto, permitiría controlar el acceso a datos personales de iniciativas para el rastreo de contagios por COVID-19 que, mediante diferentes medios, recolectan información acerca de los contactos que pueden tener las personas durante su diario vivir.

Este sistema, estaría limitado a aquellas iniciativas que cuenten con la información depurada de los contactos que se hayan dado entre individuos con sus respectivas fechas, y no debe suponerse que la plataforma realizaría identificación de las proximidades entre las personas. Esta tarea, estaría a cargo propiamente de la plataforma de rastreo de contagios.

**Conclusiones:** Aquellas aplicaciones que requieran manejar datos personales protegidos por ley, deben permitirles a los titulares realizar la administración del acceso a los mismos. Es fundamental, para un sistema de autorización de tratamientos de datos personales, contar con funciones que le permitan al usuario administrar los permisos concedidos a un tercero, incluyendo la consulta de información compartida, finalidad de los mismos, autorización y revocatoria de consentimientos. Un sistema de autorizaciones de datos personales centralizado, permitiría a los usuarios participar en diferentes medios de rastreo de contagios, con la confianza de tener control sobre el acceso a sus datos.

**Palabras clave:** Autorización de tratamiento de datos, COVID-19, Datos sensibles, Rastreo de contagios

### ABSTRACT

**Background:** Currently, the COVID-19 infection tracking systems have been useful in the process of stopping the pandemic, and its pillars are the results of COVID-19 and the list of people with whom positive people have had contact. Laboratory results, like any other information on the privacy of a person, is considered sensitive data according to law 1581 of 2012, and its treatment is prohibited without prior authorization from the owner, and other articles included in the Title IV of the same law.

Although there are some conditions that make the use of personal data more flexible, the tracking platforms can be developed by third parties, which, in the terms of the legislation, refers to title IV, article 13, paragraph C, which refers to The data that meet the pre-established conditions may be shared with third parties only authorized by the owner or by law.

**Objective:** The general objective is to design an authorization system to manage the results of covid-19 tests for tracking platforms of citizens at risk of contracting the virus by contact with infected persons, and as specific objectives are to identify the functions that a sensitive data authorization system must have according to current regulations and model and design the personal data authorization system, according to the requirements

**Materials and Methods:** To meet the objectives, a qualitative methodology is used to determine the functional requirements based on the review of Colombian laws about the protection of sensitive personal data and the non-functional requirements based on security standards, which can be adapted to the application of COVID-19 infection tracing. The functional requirements are based on the review of Colombian laws regarding the processing of personal data, and UML diagrams are used to model the authorization process.

**Results:** The proposed design would allow controlling access to personal data from initiatives to track COVID-19 infections that, through different means, collect information about the contacts that people may have during their daily lives.

This system would be limited to those initiatives that have the information of the contacts between individuals with their respective dates, and it should not be assumed that the platform would identify the proximity between people. This task would be in charge of the contagion tracking platform itself.

**Conclusions:** Those applications that require personal data protected by law, must allow the owners to carry out the administration of access to them. It is essential, for a personal data processing authorization system, to have functions that allow the user to manage the permissions granted to a third party, including the consultation of shared information, their purpose, authorization and revocation of consents. A centralized personal data authorization system would allow users to participate in different means of infection tracking, with the confidence of having control over access to their data.

**KeyWords:** Data processing authorization, COVID-19, Sensitive data, Contagion tracking

#### **REFERENCIAS (colocar a cada artículo el DOI o la URL en caso de no tener DOI)**

1. Organización Mundial de la Salud (2020). El rastreo de contactos en el marco de la COVID-19, Orientaciones provisionales. Recuperado de [https://apps.who.int/iris/bitstream/handle/10665/332083/WHO-2019-nCoV-Contact\\_Tracing-2020.1-spa.pdf?sequence=1&isAllowed=y](https://apps.who.int/iris/bitstream/handle/10665/332083/WHO-2019-nCoV-Contact_Tracing-2020.1-spa.pdf?sequence=1&isAllowed=y)
2. Inter American Development Bank (2020). Del confinamiento a la reapertura: Consideraciones estratégicas para el reinicio de las actividades en América Latina y el Caribe en el marco de la COVID-19. Recuperado de <https://publications.iadb.org/publications/spanish/document/Del->

confinamiento-a-la-reapertura-Consideraciones-estrategicas-para-el-reinicio-de-las-actividades-en-America-Latina-y-el-Caribe-en-el-marco-de-la-COVID-19.pdf

3. Ley estatutaria 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Bogotá, Colombia. 17 de octubre de 2012
4. Ley estatutaria 1266 de 2008. Por la cual se dictan las disposiciones generales del Habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Bogotá, Colombia. 31 de diciembre de 2008
5. Decreto 1377 de 2013. Por la cual se reglamenta parcialmente la ley 1581 de 2012. Bogotá, Colombia. 27 de junio de 2013.
6. Superintendencia Nacional de Salud-SuperSalud (2020). Formato diseñado para realizar los Requerimientos De Seguridad Para Aplicaciones (versión 2). Recuperado de <https://docs.supersalud.gov.co/PortalWeb/planeacion/AdministracionSIG/RSFT03.xlsx>