# PLATAFORMA QUE INTEGRA LOS MONITOREOS DEL ÁREA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD DE UNA COMPAÑÍA VIGILADA POR LA SUPERINTENDENCIA FINANCIERA DE COLOMBIA

CARLA VANESSA SAYAGO ABREO

Director:

Ing. Felipe Díaz-Sánchez, Ph.D.

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERIA DE TELECOMUNICACIONES
INGENIERÍA DE TELECOMUNICACIONES
BOGOTÁ, 2019

A Dios,

Por permitirme llegar hasta este punto, haberme dado la salud y sabiduría para lograr mis objetivos y llegar a culminar esta etapa de mi vida.

A mi familia,

Por apoyarme en todo momento, por sus valores, confianza y sus consejos; por ser el pilar fundamental de la persona íntegra que soy, en mi educación académica, en la vida personal.

## AGRADECIMIENTOS

El presente trabajo fue posible gracias al equipo de Riesgos y Procesos del Grupo Bolsa de Valores de Colombia, en especial a la coordinación de Seguridad de la Información y Ciberseguridad, les agradezco profundamente el apoyo, la confianza y calidez que me brindaron desde el inicio de mis prácticas profesionales en la compañía; sin ustedes no hubiese sido factible la realización de este proyecto.

Al ingeniero Ángel Felipe Díaz, tutor de esta monografía, agradezco por hacer posible la realización de este proyecto; así mismo reconozco su tiempo, paciencia, y dedicación puesta para que esto saliera de manera exitosa.

A todos los docentes y la Universidad Santo Tomás, por formarme como una ingeniera de telecomunicaciones integra; por su paciencia, tiempo, y dedicación.

A mi familia, por ser el apoyo durante mi educación, sin ustedes no hubiese sido posible cumplir una meta más en mi vida; porque son el motor que me impulsa a ser mejor cada día.

A mis amigos, por estar conmigo en esta etapa tan bonita, agradezco sus consejos, paciencia, y compañía en los buenos y malos momentos a pesar de la distancia.

A Dios, por regalarme un logro más, la oportunidad de vivirlo y disfrutarlo junto a los seres más queridos.

**TABLA CONTENIDO**

## ACRÓNIMOS

BS: British Standards

BSI: British Standards Institution

C.E.: Circular Externa

DLP: Data Loss Prevention

IEC: International Electrotechnical Commission

ISO: International Organization for Standardization

KPI: Key Performance Indicator

MinTIC: Ministerio de Tecnologías de la Información y las Comunicaciones

SFC: Superintendencia Financiera de Colombia

SGSI: Sistema de Gestión de Seguridad de la Información

SOC: Security Operation Center

TIC: Tecnologías de la Información y las Comunicaciones

## RESUMEN

Las entidades vigiladas por la Superintendencia Financiera de Colombia deben cumplir con los requerimientos de normativas como la Circular Básica Jurídica y Circular Externa 007/18, las cuales tienen como objetivo principal velar por la protección del cliente. Entre las necesidades principales, se encuentra la seguridad de la información, por esto una empresa privada del sector financiero cuenta con un Sistema de Gestión de Seguridad de la Información bajo el estándar ISO/IEEC 27001:2013. En la norma técnica y jurídica antes mencionada, se exige tener una constante validación del cumplimiento de los requerimientos, para esto se cuenta con los monitoreos; ellos se encuentran sistematizados en el lenguaje de programación R, pero su disponibilidad, integridad y confidencialidad está en riesgo, pues no está protegido el código fuente, por tal razón se ha diseñado e implementado una plataforma de monitoreos a través de Python para la ejecución de los mismos, en la cual se evita el error humano y se minimizan los riesgos.



*Palabras clave:* Confidencialidad; Disponibilidad; Integridad; Python; R.



## ABSTRACT

The entities supervised by the Financial Superintendence of Colombia must accomplish with the requirements of the law such as Basic Legal Circular and External Circular 007/14, it aim is ensure about client protection. One of the most important need is the information security, hereby a private company in the financial sector has an Information Security Management System (ISMS) under the standard ISO/IEC 27001:2013. Those technical and juridical rule require to the companies a frequent validation of compliance about requirement, this is the reason about the monitoring. They are systematized through the programming language R, but their availability confidentiality and integrity are at risk because the code is not protected. For that reason, we have been designed and implemented a monitoring platform in Python for the execution of them, with this solution, the human error is avoided and the risk is minimized.



*Keywords:* Availability; Confidentiality; Integrity; Python; R.

## INTRODUCCIÓN

En Colombia el uso de las Tecnologías de la Información y las comunicaciones (TIC) han tenido un crecimiento exponencial, lo cual es sinónimo de crecimiento para el país, pero a su vez, implica una mayor expansión de las vulnerabilidades y la exposición a los ciberataques. De acuerdo a una encuesta en el 2018 del BID y Finnovista, aproximadamente el 80% de las compañías Fintech en América Latina consideran los ciberataques una amenaza para su negocio, tan solo la mitad de este grupo, cuentan con un plan de contingencias en caso de un ataque. Los riesgos cibernéticos son una amenaza que se encuentra presente para cada una de las compañías. [1]

Es por esto, que una compañía vigilada por la Superintendencia Financiera de Colombia (SFC), cuenta con un equipo de seguridad de la información y ciberseguridad, dentro de la gerencia de riesgos; este grupo de personas se dedican a controlar, vigilar y salvaguardar la información de la compañía, para lograr esto, es necesario apoyarse de algunas herramientas que facilitan la vista de algunas vulnerabilidades. Los monitoreos son uno de los instrumentos más importantes para las labores de seguridad de la información y ciberseguridad, pues por medio de ellos, es posible ver los resultados de los controles que se llevan a cabo, y así mismo ejecutar los planes de acciones pertinentes.

Esta compañía cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI), hace un tiempo se sistematizaron algunos monitoreos a través del lenguaje de programación R; para que un usuario ejecute dichos procesos, es necesario parametrizar directamente con el código fuente, tras este procedimiento es posible que la integridad del código fuente se pierda, así mismo, la disponibilidad del monitoreo está en riesgo, y al estar a la vista de todo aquel que realice el monitoreo, se pierde su confidencialidad. Además de lo anterior, se requiere un conocimiento detallado del diseño y programación del código que ejecuta el monitoreo.

De acuerdo a lo anterior, se encontró la necesidad de implementar una plataforma que integre los monitoreos, manteniendo su integridad, confidencialidad, disponibilidad, y que sea intuitiva para los usuarios que no conozcan del lenguaje de programación.

En el desarrollo del proyecto se evidenció que de todos los monitoreos sistematizados en la compañía, los que ofrecían información más relevante en la gerencia de riesgos son los de las aplicaciones y sistemas propios de la compañía; así mismo se constató que para una empresa del sector financiero las principales necesidades son las internas, es decir los requerimientos no funcionales.

A través del documento se presenta como solución la implementación de una plataforma que integra los monitoreos de esta compañía, para desarrollar este proyecto fue necesario seguir una serie de cinco pasos, la identificación de los monitoreos, el levantamiento de requerimientos para la plataforma, la realización de la arquitectura de la solución, la implementación de la solución y la validación de los requerimientos. El desarrollo de este proyecto se llevó a cabo en 22 semanas y la elaboración del documento se realizó en un periodo de 17 semanas.

Con este proyecto se redujeron los tiempos de ejecución de los monitoreos, y a su vez fue posible mantener los mismos códigos fuentes, con la protección de su integridad, disponibilidad, y confidencialidad; así mismo se realizó una plataforma intuitiva para el usuario, la cual podrá ser ejecutada por cualquiera de los miembros del equipo de seguridad de la información y ciberseguridad, aun cuando no conozcan del lenguaje de programación R o Python.

# 1 MARCO GENERAL DEL PROYECTO

El ente regulador del sector financiero, la Superintendencia Financiera de Colombia (SFC) exige a las compañías algunos requerimientos mínimos de seguridad de la Información, en busca de proteger a los usuarios. La compañía objeto de estudio de este proyecto es vigilada por la SFC, cuenta con la coordinación de seguridad de la Información y ciberseguridad, en la Gerencia de Riesgos. Dicha coordinación sigue los lineamientos establecidos por la SFC y la norma internacional ISO/IEC 27001:2013.

Dentro de las constantes labores de seguridad de la información se encuentran los monitoreos, por medio de ellos se puede hacer seguimiento a las medidas preventivas que se han tomado para salvaguardar la información de la compañía. Hace unos años se decidió sistematizar algunos procesos de monitoreos utilizando el lenguaje de programación R, con el objetivo de evitar la intervención humana, disminuyendo así la probabilidad de error. Sin embargo, para que un usuario ejecute dichos procesos, requiere interactuar directamente con el código fuente, ya que debe parametrizarlos; tras este procedimiento es posible que la integridad del código fuente se pierda, debido a la edición del mismo. Así mismo, la edición de dicho código podría imposibilitar la ejecución del mismo en futuras oportunidades, colocando en riesgo la disponibilidad del monitoreo. Por otra parte, el código fuente se encuentra a la vista de todo aquel que realice el monitoreo, perdiendo así toda su confidencialidad. Adicionalmente se requiere un conocimiento detallado del diseño y programación del código que ejecuta el monitoreo, el cual solo es manejado por las personas que conocen del mismo; en caso de que se requiera ejecutar por otra persona de la compañía, es posible que se le presenten dificultades y no logre obtener los resultados deseados.

Con base en lo anterior, se vio la necesidad de implementar una plataforma que integre los monitoreos de seguridad de la Información en el área de Riesgos de una compañía vigilada por la Superintendencia Financiera de Colombia, manteniendo su integridad, confidencialidad y disponibilidad.

## 1.1 OBJETIVOS

Implementar una plataforma que integre los monitoreos de seguridad de la información y ciberseguridad en el área de Riesgos de una compañía vigilada por la Superintendencia Financiera de Colombia (SFC), manteniendo su integridad, confidencialidad y disponibilidad.

- Identificar los diferentes tipos de monitoreo del área de ciberseguridad existentes en la compañía.
- Levantar los requerimientos para la elaboración de la plataforma, teniendo en cuenta la norma ISO/EIC 27001:2013 acogida por la coordinación de seguridad de la información y ciberseguridad de la compañía.
- Realizar la arquitectura de la plataforma para la integración de monitoreos del área de seguridad de la información y ciberseguridad de la compañía.
- Implementar la arquitectura de la solución que integra los monitoreos del área de seguridad de la información y ciberseguridad de la compañía.
- Validar los requerimientos establecidos para la plataforma por medio de una lista de cumplimiento de requerimientos.

## 1.2 ALCANCE

El alcance de este proyecto es la implementación de una plataforma local en Python que integre 10 monitoreos de seguridad de la Información en el área de Riesgos de una compañía vigilada por la SFC, teniendo en cuenta la ISO/IEC 27001:2013.

Los aspectos puntuales que comprende el alcance de dicha plataforma son:

- Una interfaz gráfica e intuitiva en Python la cual permite al usuario seleccionar el monitoreo a realizar, y así mismo protege la integridad, disponibilidad y confidencialidad.
- Diez interfaces gráficas, una para cada monitoreo. En cada una de ellas se solicitan los documentos específicos, se realiza el monitoreo y finalmente si el usuario lo desea se envían por correo electrónico los resultados al coordinador de seguridad de la Información y ciberseguridad. Estos se encontrarán en la red corporativa, a la cual solo los miembros de seguridad de la Información tendrán acceso.

- Diez códigos fuente en R, los cuales reciben la información suministrada a Python. Estos se encontrarán en la red corporativa, a la cual solo los miembros de seguridad de la Información tendrán acceso.
- Un manual de cómo ejecutar cada uno de los monitoreos desde la interfaz gráfica.

## 1.3 METODOLOGÍA

Este trabajo se llevó a cabo bajo la metodología utilizada en esta compañía, y fue adaptada de acuerdo a los requerimientos específicos del proyecto; así mismo fue evaluada y aprobada por el coordinador de seguridad de la información y ciberseguridad, jefe inmediato del practicante.

La metodología se basa en conocer a fondo el funcionamiento de la compañía y las labores del área, para así identificar el problema y los requerimientos para solucionar el mismo, posteriormente se realiza la solución, se implementa y se hacen las pruebas pertinentes; de allí salen las cinco tareas principales de este proyecto; en la Figura 1. se presenta el comportamiento de estos.

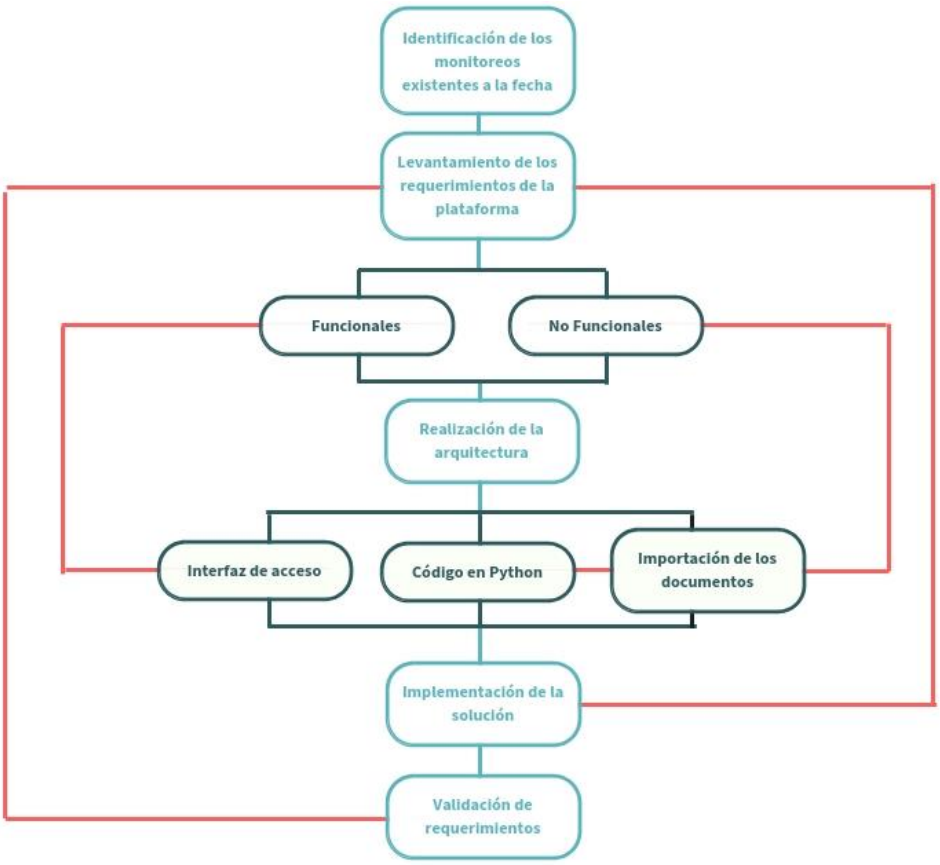



Figura 1 Comportamiento de las etapas del proyecto

*Fuente: Elaboración propia*

La identificación de los monitoreos existentes hace referencia a realizar cada uno de los monitoreos establecidos en la compañía para de esta forma conocer los insumos, el resultado, y su problemática principal; A continuación, se realiza el levantamiento de los requerimientos, es decir, con base en la problemática que existe, se identifica de forma específica cada uno de los aspectos que se deben tener en cuenta con esta solución, en este caso será una plataforma que integre todos los monitoreos y se presente al usuario como una interfaz gráfica; posteriormente se diseña la arquitectura de la plataforma siendo esta la etapa en donde se generan los diferentes códigos que integran los monitoreos en R, con su interfaz gráfica en Python, teniendo en cuenta cada uno de los requerimientos, y así pasar a la tarea de la implementación; finalmente se realiza la validación de los requerimientos, que consta de hacer pruebas y verificar a través de una lista de cumplimiento que cada uno de los requerimientos responda a las necesidades. En la Figura 2. se presentan todas las tareas y subtareas.

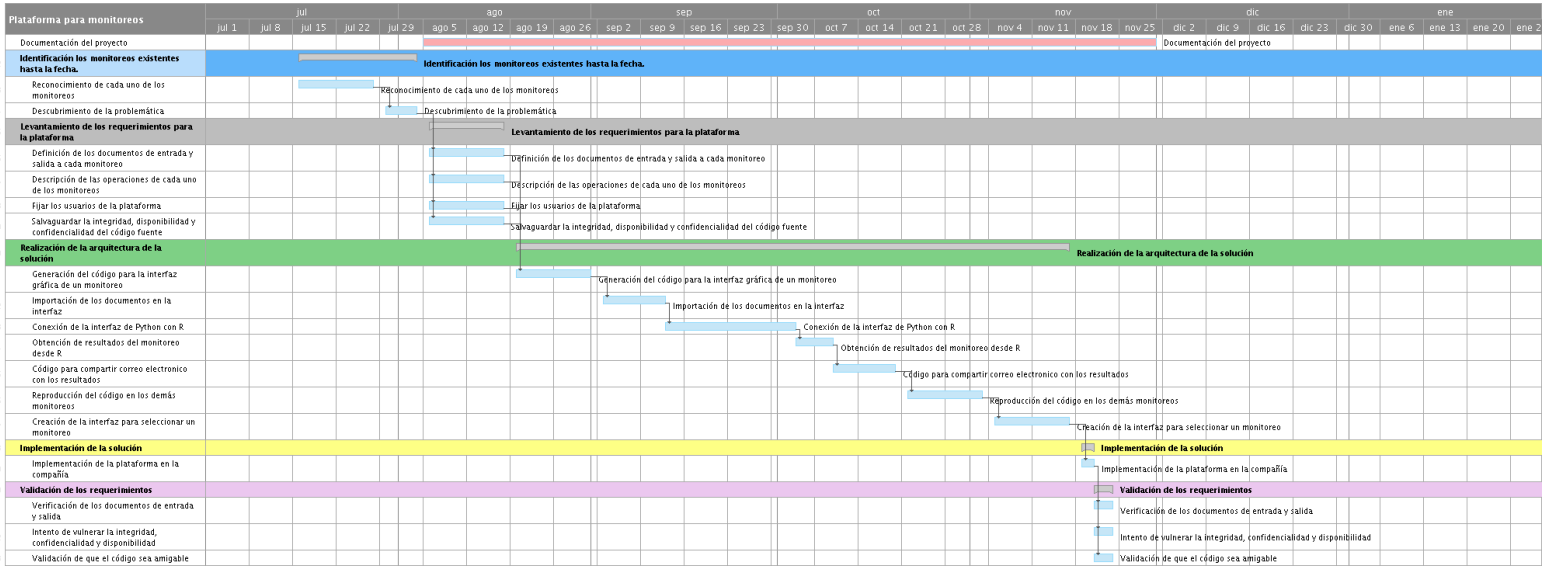



Figura 2 Diagrama de Gantt del proyecto

*Fuente: Elaboración propia*

# 2 MARCO TEÓRICO

En este capítulo se aborda el marco conceptual, teórico, jurídico y estado del arte de este proyecto, el cual se enfoca en cinco aspectos principales, la evolución de los sistemas de gestión de seguridad de la información, la norma ISO/IEC 27001:2013, el desarrollo de la seguridad de la información y ciberseguridad, las normativas de seguridad de la información y ciberseguridad del sector financiero en Colombia, y las características de Python y R como lenguajes de programación para la plataforma de monitoreos.

## 2.1 EVOLUCIÓN DE LOS SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Cada compañía debe tomar la decisión de implementar un Sistema de Gestión de seguridad de la Información (SGSI) de acuerdo a las necesidades, objetivos, requisitos, procesos, tamaño y estructura de la organización.

La ISO/IEC 27001 es una norma que "*especifica los requisitos para establecer, implementar mantener y mejorar continuamente de gestión de seguridad de la información dentro del contexto de la organización. La norma también incluye los requisitos para la valoración y el tratamiento de los riesgos de seguridad de la información, adaptados a las necesidades de la organización*" [2].

Este estándar es actualmente el único aceptado para internacionalmente para la implementación de un SGSI, pero no es el primero, es el resultado de la evolución de aproximadamente 10 normas, desde la 1901 – Normas "BS", hasta la ISO 27001:2007, a continuación, se presenta una línea cronológica de todas las normas antecesoras a la ISO/IEC 27001:2013. [3]

- 1901 – Normas "BS": Esta es una norma creada por la compañía British Standards International, son los actuales estándares ISO 9001, ISO 14001 u OHSAS 18001.
- 1995- BS 7799-1:1995: Era una recomendación de buenas prácticas para ayudar a las empresas británicas a administrar la Seguridad de la Información.

- 1998 – BS 7799-2:1999: Es una versión certificable de la norma anterior, en ella se establecía los requisitos para implantar un Sistema de Gestión de Seguridad de la Información.
- 1999 – BS 7799-1:1999: Es la revisión de la anterior norma.
- 2000 – ISO/IEC 17799:2000: ISO tomó la norma británica BS 7799-1, y experimento algunos cambios.
- 2002 – BS 7799-2:2002: Se publicó una nueva versión que permitió la acreditación de empresas.
- 2005 – ISO/IEC 27001:2005 e ISO/IEC17799:2005: Se revisa la ISO 17799 y aparece el estándar ISO 27001 como norma internacional certificable.
- 2007 – ISO/IEC 27001:2007: Se publica la nueva versión.
- 2009 – ISO/IEC 27001:2007/1M:2009: Se publica un documento adicional de modificaciones.
- 2013 – ISO/IEC 27001:2013: Es la nueva y más reciente versión de la ISO 27001 que trae cambios significativos en su estructura, evaluación y tratamiento de los riesgos.

## 2.2 ISO/IEC 27001:2013

La norma ISO 27001:2013 soporta el SGSI para el cumplimiento de los objetivos estratégicos con el fin de estandarizar los procesos que mantengan controlados los riesgos, estableciendo, implementando, manteniendo y mejorando los requisitos que debe tener nuestra organización para estar en línea con los nuevos retos que emergen en seguridad de la información y ciberseguridad. [2]

Una organización que cuente con un SGSI, es una compañía que tiene implementados diferentes controles para la protección de la confidencialidad, integridad y disponibilidad de sus activos. Es por esto que la ISO/IEC 27001:2013 dedica una sección para presentar la gestión de activos, aquí se especifican los controles que se deben llevar a cabo para la responsabilidad por los activos, la clasificación de la información y el manejo de medios. [2]

La clasificación de la información es una de las labores más importantes, pues gracias a ella se asegura que cada activo cuente con los niveles de protección adecuados. De acuerdo a la norma, son tres los controles que se llevan a cabo para clasificar los activos,

el primero es que la información se clasifica de acuerdo a los requisitos legales y/o normativos, su valor, la criticidad y la susceptibilidad a divulgación o modificaciones no autorizadas; el segundo, el etiquetado de información, en este se define que el etiquetado de información debe ser conforme al esquema de clasificación de activos de la organización; el tercero y último es el manejo de los activos, este hace referencia a que cada compañía genera un esquema de clasificación de activos, de acuerdo a sus necesidades de negocio. [2][4]

Por otra parte, la norma ISO/IEC 27001:2013, en la sección adquisición desarrollo y mantenimiento de los sistemas se aborda la seguridad en los procesos de desarrollo y de soporte; los requerimientos allí presentados buscan asegurar que la seguridad de la información se encuentre implementada dentro del ciclo de vida del desarrollo de software, es decir, que los softwares que se desarrollen dentro y fuera de la organización, pero sean para ella, cumplan con todos los requisitos de seguridad de la información, salvaguardando así la integridad, disponibilidad y confidencialidad del activo.[2][4]

Así mismo, diferentes autores han escrito documentos enfocados a la implementación de un sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2013, como lo es el caso de Juan Carlos Oidor Gonzalez, autor de “DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION-SGSI BAJO LA NORMA ISO/IEC 27001 PARA LA EMPRESA “EN LINEA FINANCIERA” DE LA CIUDAD DE CALI-COLOMBIA”, en este artículo, se presenta el diseño de un sistema de gestión de seguridad de la información a través de la metodología MAGERIT y de acuerdo a la norma ISO/IEC 27001:2013 para una compañía del sector financiero en Colombia, a través del documento se presentan los pasos que se siguieron para desarrollar este sistema de gestión, entre estos la identificación de los activos de la empresa y la valoración de los riesgos sobre ellos, la cual fue una de las labores más complejas e importantes en el desarrollo de ese proyecto; finalmente, como conclusión se obtiene que la empresa descubrió su información como el activo más importante, y así mismo, se generó un valor agregado en la compañía, no solo para ella y sus colaboradores, sino para sus clientes también. [5]

## 2.3 DESARROLLO DE LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

La seguridad de la información ha evolucionado a lo largo del tiempo, pues cada nueva tecnología, cada nuevo avance, significan nuevas amenazas, y nuevos objetos de estudio para esta área, uno de los ejemplos más recientes de esto es el desarrollo de Cloud Computing; diferentes estudios se han realizado para mostrar los retos a los que se enfrentan las compañías con esta nueva tecnología.

“A cybersecurity model in cloud computing environments”, un artículo, el cual presenta una medida de ciberseguridad centrada en el usuario, para implementar en Cloud Computing, y cómo se puede usar para analizar la computación en la nube como un modelo de negocio; dicha medida se basa en un modelo cuantitativo que mide la seguridad, permitiendo de esta forma a los proveedores de servicios en la nube y los suscriptores de la nube cuantificar los riesgos que corren con la seguridad de sus activos y tomar decisiones con base en esto.[6]

Pero Cloud Computing no es la única de las tendencias actuales, compañías como Deloitte, realizan estudios para conocer la evolución de la seguridad de la información en Latinoamérica, como lo es el caso de “La Evolución de la Gestión de Cyber Riesgos y Seguridad de la Información”, una encuesta realizada en el año 2016 sobre Tendencias de Cyber Riesgos y Seguridad de la Información en Latinoamérica. Esta encuesta se realizó en 13 países de Latinoamérica, en los cuales está incluido Colombia, participaron 7 industrias diferentes, las tendencias principales que se encontraron en esta investigación fueron: [7]

- 4 de cada 10 organizaciones sufrieron una brecha de seguridad en los últimos 24 meses.
- Menos del 20% de las organizaciones cuentan con un SOC (Security Operation Center).
- La mayor barrera que afrontan los oficiales de seguridad de la información es el presupuesto por parte de las altas directivas.
- Menos del 10% de las organizaciones cuentan con un tablero con indicadores (KPIs).

Por otra parte, en esta encuesta realizada por Deloitte, encontramos que 1 de cada 10 organizaciones han sufrido brechas de seguridad con un impacto significativo en su economía y reputación en los últimos 24 meses (Figura 3), esto se debe a que las compañías no contaban con capacidades adecuadas para monitorear su estado de seguridad. [7]

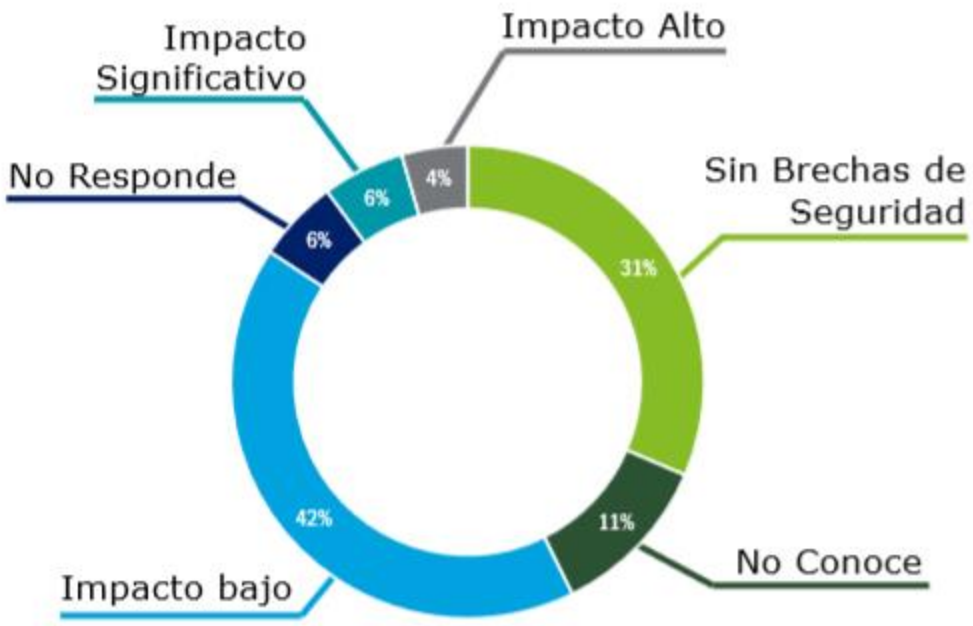



Figura 3 Impacto de las brechas de seguridad

*Fuente: La Evolución de la Gestión de Cyber Riesgos y Seguridad de la Información, Deloitte [7]*

Así mismo, BID y Finnovista realizaron una encuesta en el 2018 para Latinoamérica, específicamente en el sector financiero; en dicho estudio se examina la percepción de riesgo de ciberseguridad de las compañías (Figura 4), y a su vez el estado de preparación en el que se encuentran para enfrentar un ataque. La conclusión a la que se llega es que, en términos generales, aproximadamente 2 de cada tres empresas cuentan con planes de contingencia, pero también se percibe, que los segmentos de pagos, bance digital, y seguridad y fraude son los que cuentan con un mejor sistema de contingencia. [1]

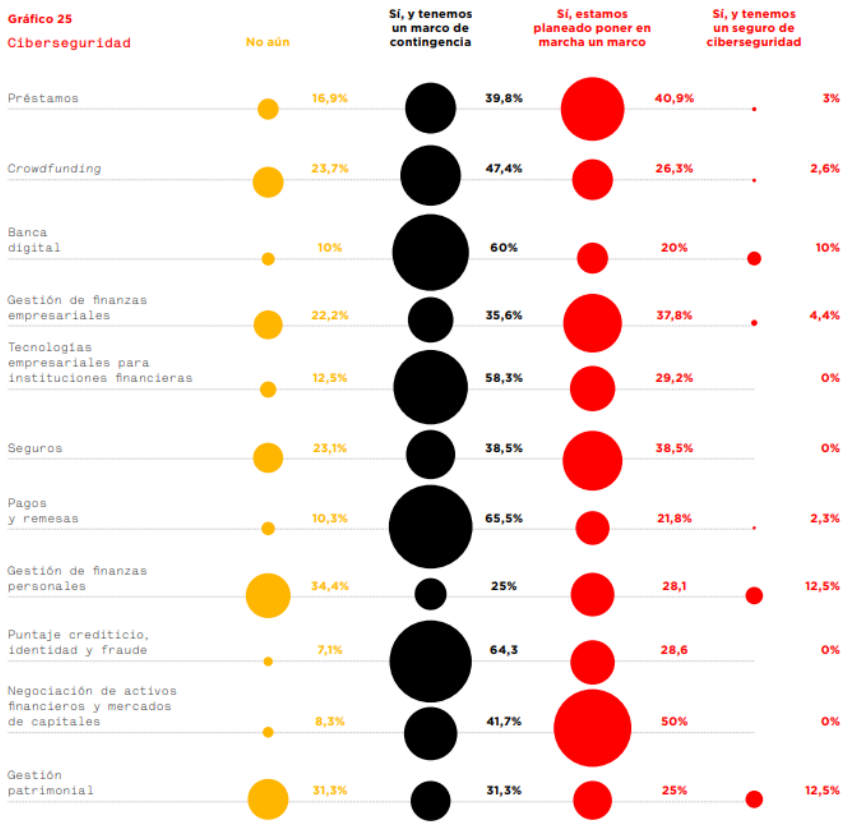



Figura 4. Percepción de riesgo de ciberseguridad de las compañías.

*Fuente: Ecuesta BID y Finnovista 2018*

De igual manera, autores escriben sobre este tema, y no solo en América latina, sino también en Colombia, como es el caso de “Lineamientos, tendencias y estrategias sobre ciberseguridad y ciberdefensa en Colombia”, un documento que se enfoca en presentar las diferentes normativas legales y lineamientos para los ciberataques, y así mismo las tendencias de delincuencia cibernética en Colombia desde el 2009 al 2014 (Figura 5); finalmente se propone un plan estratégico para fortalecer la ciberseguridad en el país, liderado por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC). [8]

| POR CONDUCTA DELICTIVA | 2009 | 2010 | 2011 | 2012 | 2013 | 2014 |
|---|---|---|---|---|---|---|
| Artículo 269A. Acceso abusivo a un sistema informático | 6 | 3 | 1 | | 8 | 4 |
| Artículo 269C. Interceptación de datos informáticos | | 1 | 1 | 1 | 1 | |
| Artículo 269F. Violación de datos personales | 1 | 1 | | | | |
| Artículo 269G. Suplantación de sitios web para capturar datos personales | 1 | | | | | |
| Artículo 269I. Hurto por medios informáticos y semejantes | 212 | 401 | 841 | 2343 | 3448 | 1830 |
| Artículo 269J. Transferencia no consentida de activos | 7 | 1 | | 1 | 206 | 104 |
| **Total general** | **227** | **407** | **843** | **2345** | **3663** | **1938** |

Figura 5. Registro de delitos informáticos

*Fuente: Coloque el autor de la figura o el documento de origen*

## 2.4 NORMATIVA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD EN EL SECTOR FINANCIERO

En Colombia cada compañía se encuentra vigilada por un ente gubernamental, la Superintendencia Financiera, es la entidad encargada de supervisar los sistemas financiero y bursátil encargada de propender por la solvencia, disciplina y supervisión del Sistema Financiero de Colombia. Como encargada de la supervisión, es quien genera las normativas que rigen a las compañías del mercado bursátil. [9]

La ciberseguridad es un aspecto que le compete por completo a la SFC, pues los ciberataques en el entorno, suelen poner en juego la economía no solo de los individuos, sino del país; es por esto, que la Superintendencia Financiera de Colombia presenta unas normas específicas a las entidades vigiladas, para regular su sistema de gestión de seguridad de la información y ciberseguridad, dicha normativa legal esta detallada en cuatro secciones diferentes, la Circular 029, 042, 052 un anexo a la Circular Básica Jurídica, conocida como the Circular de Ciberseguridad SFC CE 007 de Junio de 2018. Con la publicación de esta última (Circular Externa 007), las exigencias del gobierno son más estrictas, y cumplir con estas regulaciones debe ser una prioridad para las compañías, pues

en caso de no ser así se pone en juego no solo una multa, sino la reputación de la misma. [10][11][12][13]

Todas estas normativas, les exigen a las entidades mantener un control permanente de las medidas que se toman para salvaguardar la información de los clientes y la compañía; los monitoreos son una parte fundamental de dichos controles, pues a través de ellos es posible conocer el estado en el que se encuentra la información, y los peligros que se encuentran alrededor.

## 2.5 PLATAFORMA

Python es un lenguaje de programación orientado a objetos, de código abierto, moderno e interpretado; se implementa en todo tipo de ingeniería de software, desde análisis de datos, hasta computación distribuida, así mismo es utilizado para interfaces gráficas de usuario. Entre sus características más destacadas, se encuentra su sintaxis, la cual es concisa pero natural tanto para arreglos como para no arreglos, lo que hace que los programas sean extremadamente claros y fáciles de leer; además, las estructuras de datos y la naturaleza del lenguaje orientada a objetos hacen que el código Python sea más robusto y menos frágil. [14]

R es un sistema para computación con énfasis en estadística y gráfica, el cual proporciona un lenguaje de programación de código abierto, gráficos de alto nivel, interfaces con otros lenguajes y facilidades de depuración, entre otras cosas; la sintaxis del lenguaje tiene una similitud superficial con C, pero la semántica es de la variedad FPL (lenguaje de programación funcional). Una de las principales características de R es su capacidad para procesar grandes volúmenes de datos, convirtiéndose así en uno de los lenguajes más implementados para la minería de datos. [15][16]

En diferentes documentaciones se realizan comparaciones entre ambos lenguajes de programación, pues sus características son muy buenas en ambos casos, y es posible implementarlas en enfoques similares, como es el caso de “Big Data Visualization: Allotting by R and Python with GUI Tools”, un proyecto que busca diseñar una guía de análisis de Big Data entre las dos herramientas principales (R y Python), y de esta forma ayudar a los no programadores a elegir la más funcional para sus necesidades; esto basados en que el

crecimiento de la información masiva va creciendo de forma exponencial, y las empresas actualmente tienen acceso a una enorme cantidad de conocimiento, este se ve reflejado en datos, actualmente llamamos Big Data. Existen diferentes metodologías para realizar el análisis de una gran cantidad de información, en este documento se plantea que la mejor forma es a través de técnicas de visualización, pues mediante este proceso se puede obtener gran información en tiempo real, y así mismo de forma interactiva. A través de todo el documento se presenta genera una guía visualización de Big Data por medio de R y Python, utilizando las diferentes librerías y propiedades de cada uno de estos lenguajes de programación, obteniendo como resultado una base de datos de consulta para desarrollar la visualización de big data en R y Python, permitiendo a los desarrolladores elegir el que más se ajuste a sus necesidades, así mismo se concluyó que Python primero hace la reconstrucción notable y R viene con una fuente más rica y más objetiva en la visualización de Big Data, siendo ambos dos lenguajes de programación óptimos para visualizar grandes cantidades de información en las organizaciones. [17]

Adicionalmente, uno de los aspectos más importante al momento de seleccionar un lenguaje de programación sobre el cual trabajar es su documentación, en el artículo “Survival Analysis within Stack Overflow: Python and R” se presenta una comparación de diferentes factores como lo es el recuento de eventos, el tiempo en horas hasta la primera respuesta, el tiempo hasta la respuesta aceptada en el sitio web número uno de programadores Stack Overflow, respecto al lenguaje de programación R y Python. A través del documento se hace una revisión de la literatura, se presenta el método por el cual se hizo el estudio, y al final se presentan los resultados y las conclusiones, en las cuales la comunidad de Python parece ser más activa, o sea, Python presenta la mejor tasa de respuesta general, y por otra parte, la comunidad R demostró una mejor calidad en las respuestas, es decir, presenta la mejor tasa de respuesta aceptada. [18]

Por otra parte, cada uno de estos lenguajes de programación cuenta con un gran repositorio de proyectos que se han realizado con diferentes finalidades y por medio de diferentes metodologías, en el caso específico de Python, encontramos “Intruder monitoring system for local networks using Python”, documento en el cual se presenta una solución enfocada hacia seguridad de la información, desarrollada dentro del lenguaje de programación Python creado para el uso en redes LAN; la finalidad de este código es ejecutarse en

hardware de bajo costo, el programa está diseñado para ejecutar un escaneo a pedido y notificar al propietario a través de alarmas en caso de intrusiones, todo esto teniendo presente los principios de seguridad de la información, integridad, disponibilidad y confidencialidad, así como el Ciber kill. En el documento se describen el diseño del software, llegando a la conclusión de que los aspectos de seguridad de la información como lo es la disponibilidad, confidencialidad e integridad son primordiales al momento de implementar medidas de este tipo. [19]

Así como Python, R también cuenta con documentación de software que se ha diseñado para análisis de datos, como lo es el caso de "Web-Log Trend Pattern Analysis with Temporal Approach", en el cual trata sobre el enfoque temporal de la minería de weblog en el sitio web de la NASA basado en el análisis de tendencias temporales mediante el análisis de los patrones interesantes extraídos; para analizar el weblog se ha utilizado R-Studio, y por medio de él se extrae el patrón de tendencia basado en el tiempo de permanencia de los usuarios, lo que crea un patrón particular; el principal objetivo de dar una idea de cómo una industria concluye o examina el comportamiento de sus usuarios. A través del documento se presenta la metodología de análisis, y los resultados del programa, así mismo se concluye que la técnica de minería de datos se utiliza para extraer patrones interesantes y por medio de un análisis es posible tener beneficios como lo es una asignación eficiente de recursos, y obtener un pronóstico de las acciones de los usuarios. [20]

Después de conocer todo el potencial que trae consigo cada uno de ambos lenguajes de programación, es posible plantearse la posibilidad de unirlos a través de rpy2, una librería que permite un acceso simple y eficiente a R desde Python, obteniendo así lo mejor de la ingeniería de software.

# 3 PLATAFORMA PARA INTEGRAR MONITOREOS

En el presente capítulo se describe el detalle del desarrollo de una plataforma que integra los monitoreos de una compañía vigilada por la Superintendencia Financiera de Colombia, la cual incluye identificación de los monitoreos, levantamiento de requerimientos para la plataforma, realización de la arquitectura de la solución, implementación de la solución y validación de los requerimientos; este conjunto de actividades se llevó a cabo en 22 semanas.

## 3.1 IDENTIFICACIÓN DE LOS MONITOREOS

Esta actividad tuvo una duración de 2 semanas, su objetivo fue realizar un acercamiento a las actividades habituales que se realizaban en el área de seguridad de la información y ciberseguridad de una compañía vigilada por la SFC.

Se encontraron principalmente dos tipos de labores, las extraordinarias y las periódicas; cuando se genera un incidente de seguridad de la información o ciberseguridad, o llega algún requerimiento de parte de las altas directivas de la compañía, o entidades supervisoras de la misma, se realizan actividades extraordinarias, pero a su vez, existen las periódicas, o rutinarias, las cuales tienen la función de llevar trazabilidad de la compañía, y se realizan con una frecuencia establecida, una de las principales labores periódicas son los monitoreos.

Actualmente los monitoreos son un proceso sistematizado, los cuales tienen como objetivo principal recolectar, analizar y utilizar información para hacer seguimiento del cumplimiento de las políticas de la seguridad de la información y ciberseguridad. Cada uno de los monitoreos se realizan con una frecuencia determinada, dependiendo de la criticidad del mismo.

El proceso de monitoreo consta de tres pasos, la recolección de los insumos, la ejecución del monitoreo, y el análisis de resultados; en caso de que los resultados no son los esperados la creación y ejecución de planes de acción en busca la mitigación de las vulnerabilidades y los riesgos de la compañía.

En dicha empresa, se realizan 15 monitoreos, de los cuales 10 se encuentran sistematizados en el lenguaje de programación R, para la ejecución de los mismos existen tres frecuencias (mensuales, trimestrales y semestral), esto se estableció con base en los requerimientos de la ISO/IEC 27001:2013, así mismo cada uno de los monitoreos recibe una diferente cantidad de insumos, en algunos casos resulta útil comparar los resultados con los del periodo anterior, lo cual conlleva a un insumo más. La recopilación de esta información se presenta en la Tabla 1.

Tabla 1. Clasificación de los monitoreos, e insumos que reciben.

| **Monitoreo** | **Frecuencia** | **Número de insumos que recibe** | **Comparación con el periodo anterior** |
|---|---|---|---|
| Monitoreo 1 | Mensual | 1 | No |
| Monitoreo 2 | Trimestral | 5 | Si |
| Monitoreo 3 | Mensual | 3 | Si |
| Monitoreo 4 | Mensual | 2 | Si |
| Monitoreo 5 | Mensual | 2 | Si |
| Monitoreo 6 | Trimestral | 5 | Si |
| Monitoreo 7 | Mensual | 2 | Si |
| Monitoreo 8 | Trimestral | 3 | Si |
| Monitoreo 9 | Trimestral | 3 | Si |
| Monitoreo 10 | Semestral | 2 | No |

*Fuente: Elaboración propia*

La información presentada en la Tabla 1., es el primer paso para comenzar a desarrollar el proyecto, pues con base en ella se desarrolla la plataforma.

## 3.2 LEVANTAMIENTO DE LOS REQUERIMIENTOS PARA LA PLATAFORMA

El levantamiento de los requerimientos es una de las etapas fundamentales en proyectos de este tipo, pues de esta forma pueden prevenirse imprecisiones que puedan llevar el proyecto al fracaso; esta labor se lleva a cabo en un tiempo de 2 semanas, en las cuales se hicieron consultas con el equipo de seguridad de la información y ciberseguridad para conocer más a fondo las necesidades que se tenían, así como las directrices a seguir en el desarrollo de este proyecto.

La plataforma que integra todos los monitoreos sistematizados de seguridad de la información y ciberseguridad consta de dos tipos de requerimientos, los funcionales y los no funcionales. Los requerimientos funcionales hacen referencia a las descripciones del desarrollo que debe tener el proyecto, la información que se va a manejar, y el comportamiento que tendrá la solución. Por otra parte, los requerimientos no funcionales son los que se enfocan hacia las necesidades de la organización, teniendo en cuenta que esta compañía vigilada por la SFC se encuentra certificada en la ISO/IEC 27001:2013, estos requerimientos serán de acuerdo a lo que se describe en esta norma.

Los requerimientos funcionales de este proyecto describen los datos que deben ser ingresados a la plataforma, los resultados, las operaciones que va a realizar cada uno de los monitoreos, y quienes serán los usuarios; a continuación, se presentan estos requerimientos:

- La plataforma consta de una ventana principal, la cual direcciona al monitoreo que el usuario desee realizar.
- La ventana principal tendrá 10 botones, uno por cada monitoreo.
- A cada uno de los monitoreos se les ingresa el número de insumos que requieran (Tabla 1), en caso de ser comparados con el periodo anterior, reciben un insumo adicional.
- Cada uno de los monitoreos tiene como resultado una imagen con gráficas o un grafo, y así mismo un Excel con las novedades.
- El usuario carga los insumos en la ventana del monitoreo, genera el monitoreo, Python ejecuta el monitoreo de R, y guarda los resultados en una ruta específica,

Python extrae la ruta con los resultados y se la presenta al usuario, o envía por correo la información alojada allí.

- Si el usuario lo desea, las gráficas junto con el Excel se enviarán por correo electrónico al correo del coordinador de seguridad de la información y ciberseguridad.
- El usuario principal de la plataforma de monitoreos será el practicante de seguridad de la información y ciberseguridad, pero a su vez cualquier integrante del equipo podrá ejecutarlo cuando sea necesario.
- La plataforma de monitoreos será intuitiva, y podrá ser ejecutada por cualquier persona, así no conozca la lógica del mismo.

Por otra parte, se encuentran los requerimientos no funcionales, en este proyecto se basan en la ISO/IEC 27001:2013, la cual dice que los activos de información deben estar clasificados de acuerdo a su disponibilidad, integridad y confidencialidad, siendo los monitoreos un activo de información sensible en la compañía, se deben proteger estos tres pilares en la plataforma de monitoreos; a continuación, se presentan estos tres requerimientos:

- La plataforma presentará al usuario únicamente una interfaz gráfica a la cual se le cargarán los insumos y ella indicará dónde se encuentran los resultados, de esta forma se protege la confidencialidad del código fuente en R, pues nadie podrá ver el procesamiento del monitoreo.
- Siempre que sea necesario ejecutar un monitoreo se podrá realizar, pues no se le realizarán configuraciones que resulten perjudiciales para el mismo; a su vez el proceso de monitoreos podrá ejecutarse por cualquiera del equipo de seguridad de la información sin necesidad de conocer del lenguaje de programación R, preservando así la disponibilidad de ellos.
- El código será editado únicamente por el encargado del mismo cuando se realice una mejora al monitoreo, pues la plataforma no permite que el usuario visualice ni edite el código, manteniendo así la integridad del mismo.

## 3.3 REALIZACIÓN DE LA ARQUITECTURA DE LA SOLUCIÓN

Después de clasificar y definir cada uno de los requerimientos de la plataforma, el siguiente paso es realizar una arquitectura que integre los diez monitoreos sistematizados que se realizan en seguridad de la información y ciberseguridad. Esta actividad se divide en 7 subtareas, la generación del código para la interfaz de cada uno de los monitoreos, la importación de los insumos, la conexión entre Python y R, la obtención de los resultados del monitoreo, el envío de correos electrónicos, la reproducción de este código en los otros 9 monitoreos, y la creación de la ventana principal. Los resultados de las interconexiones realizadas en estos 7 pasos se presentan en la Figura 6.

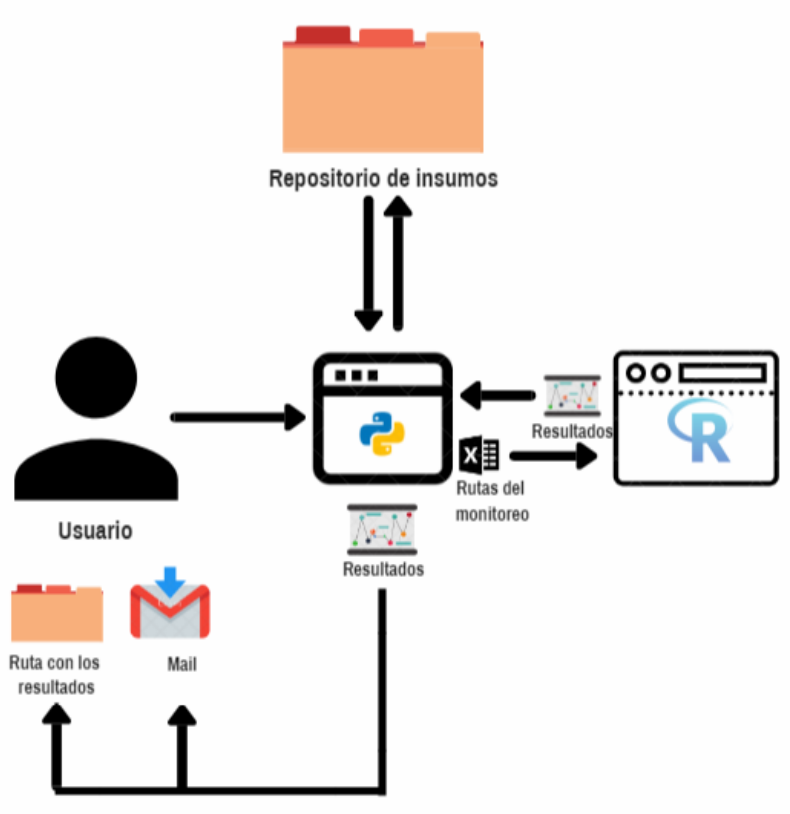



Figura 6. Diagrama de conexiones de la plataforma.

*Fuente: Elaboración propia*

En primer lugar, se debe definir el lenguaje de programación en el cual se llevará a cabo el proyecto, en este caso es Python, pues cuenta con una gran cantidad de ventajas, entre las cuales se encuentra que es gratuito, cuenta con un amplio repositorio de documentación en línea, así mismo cuenta con librerías que lo convierten compatible con R.

### 3.3.1 Generación de la interfaz gráfica

La generación de la interfaz gráfica es el primer paso para el desarrollo de la arquitectura, para esto se utiliza la librería tkinter, pues viene preinstalada con Python, por lo cual cuenta con una documentación completa, y así mismo es simple y fácil de utilizar.

A continuación, se define la estructura general de la interfaz gráfica para cada una de las acciones; en primera instancia se carga cada uno de los insumos por medio de un botón que direccionaría a la ventana de dialogo para seleccionar el documento, inmediatamente abajo, se ingresa el nombre de la hoja sobre la cual se trabajará, en caso de ser un Excel el insumo, y en la parte inferior se encuentra un botón para ejecutar el monitoreo, y otro para obtener la ruta con los resultados o enviar por correo electrónico los mismos.

Con base en esta definición, se realiza un esqueleto de la interfaz gráfica para un monitoreo, Figura 7, con todos estos controles, pero sin ninguna función.

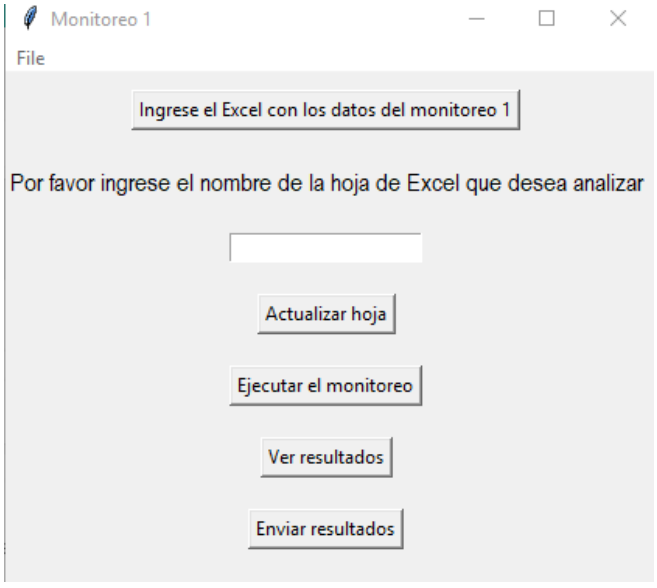



Figura 7. Esqueleto de la interfaz gráfica de la plataforma.

*Fuente: Elaboración propia*

### 3.3.2 Importación de los insumos del monitoreo

Con el esqueleto de la interfaz gráfica, el siguiente paso es la asignación de las funciones a cada uno de los controles, así que se genera una función por medio de la cual sea posible abrir una ventana de dialogo y se seleccionen únicamente archivos del tipo del insumo (en su mayoría .xlsx), Figura 8, y Python obtenga la ruta de dicho documento.

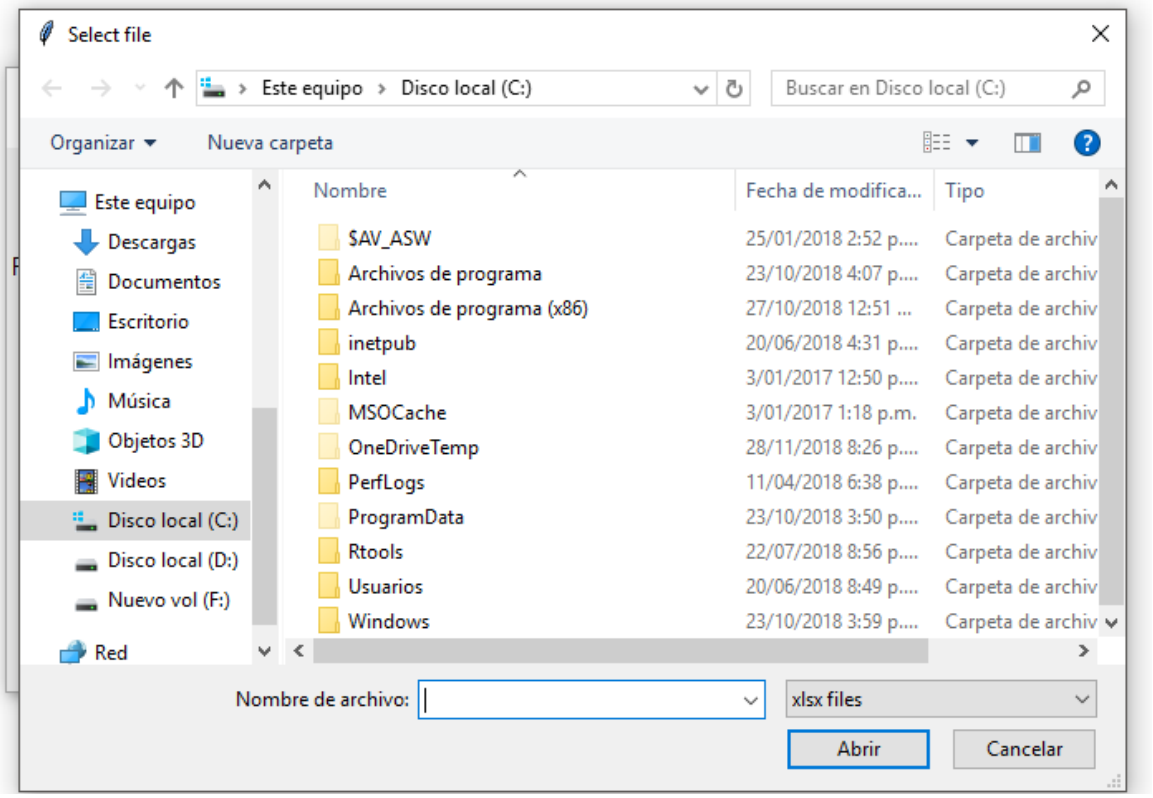



Figura 8. Ventana de dialogo para seleccionar el insumo de tipo xlsx.

*Fuente: Elaboración propia*

Así mismo se escriba el nombre de la hoja en la cual se encuentra la información para el monitoreo, y se oprima el botón “Actualizar hoja”, en caso de que el botón se oprima y no se cargará el Excel antes, o no se coloque nada en el campo de Hoja, aparecerá un letrero al usuario con la información que hace falta, Figura 9.

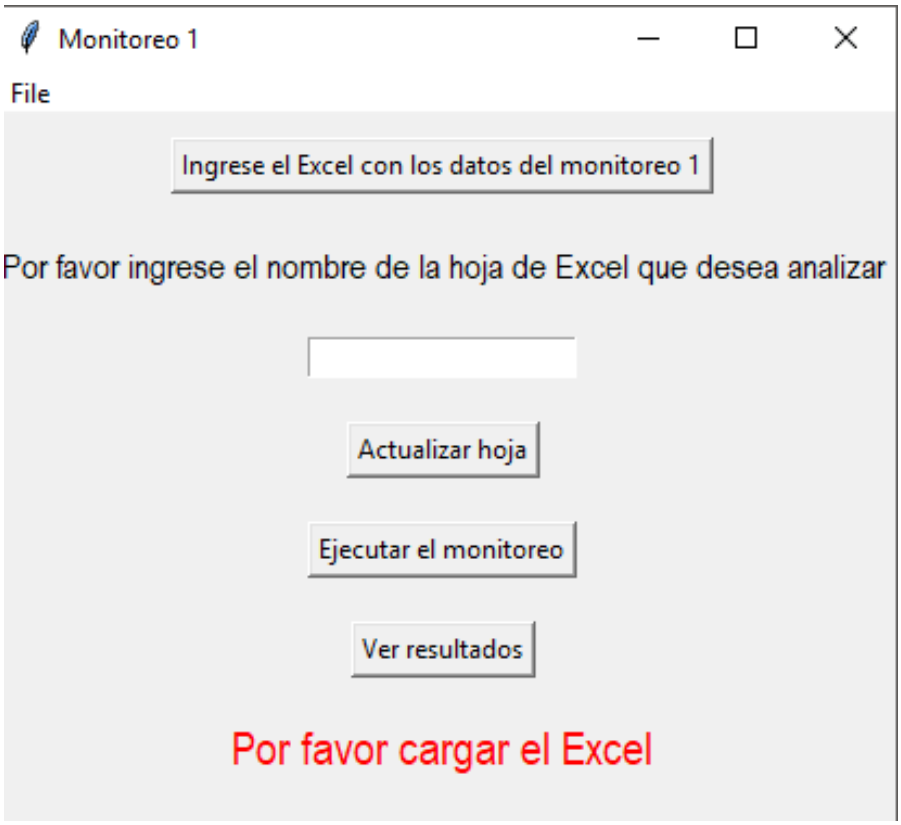



Figura 9. Error al no ingresar el insumo.

*Fuente: Elaboración propia*

Estos datos (ruta del Excel y hoja sobre la cual se trabajará), se escribirán en un documento de Excel, el cual se guarda en la carpeta del código con el nombre del monitoreo.

### 3.3.3 Conexión de Python con R

Para llevar a cabo la conexión entre R y Python fue necesario instalar la librería rpy2, la cual no se instala en Windows por medio de “pip install” en el símbolo del sistema, sino que se debe descargar un archivo .whl e instalarla por medio de él.

El procedimiento para llevar a cabo esta conexión, consta de dos pasos principales; el primero es por medio de la librería rpy2, la cual permite a través de un comando ejecutar cualquier programa de R, especificando la ruta en la cual él se encuentra; por otra parte, el código de monitoreo en R se edita para que lea y extraiga la información del Excel generado por Python con las rutas y la hoja que se va a leer, y asigne esta información como las variables sobre las cuales va a trabajar y ejecutar el monitoreo.

### 3.3.4 Obtención de los resultados del monitoreo desde R

Después de ejecutar el monitoreo de R, los resultados se generan la ruta que se tenga programada, por lo tanto, es necesario modificar el código para que coloque la ruta de los resultados en el Excel que leyó inicialmente, y posteriormente Python lee la información que R añadió y se la presenta al usuario; finalmente Python elimina el archivo de Excel con las rutas e información del monitoreo, haciendo este procedimiento transparente para el usuario.

### 3.3.5 Envío de correos electrónicos con los resultados

En esta compañía vigilada por la Superintendencia Financiera de Colombia se utiliza la Gsuite, la cual a través de una API de Google, y unas librerías como lo son docx, base64, httplib2, email.mime, mimetypes, oauth2client, apiclient, permite enviar correos desde Python.

Para enviar los resultados por medio de correo electrónico, se aplicó el procedimiento de la API de Google, se estableció como remitente el correo corporativo del practicante de seguridad de la información y ciberseguridad, como destinatario el correo corporativo del coordinador, asunto el nombre del monitoreo y los archivos adjuntos son los que se encuentran en la ruta que leyó anteriormente Python del Excel.

### 3.3.6 Reproducción de este código en los demás monitoreos

Los cinco pasos anteriores fueron ejecutados en un solo monitoreo, el siguiente paso es implementar el mismo código en los otros 9 monitoreos, con las variaciones del número de insumos que entran al monitoreo, el nombre del Excel generado por Python, y el cambio de la ruta en el cual se leerá dicho Excel.

### 3.3.7 Creación de la ventana principal

El último paso es la creación en Python de una interfaz gráfica la cual tengo 10 botones, uno por cada monitoreo, y al oprimir cada uno de estos botones me abra la interfaz gráfica del monitoreo especifico.

Con este paso finalizado, tenemos el diagrama de flujo (Figura 10) que representa la secuencia de procedimientos que se llevan a cabo en el monitoreo, y de esta obtener el resultado.

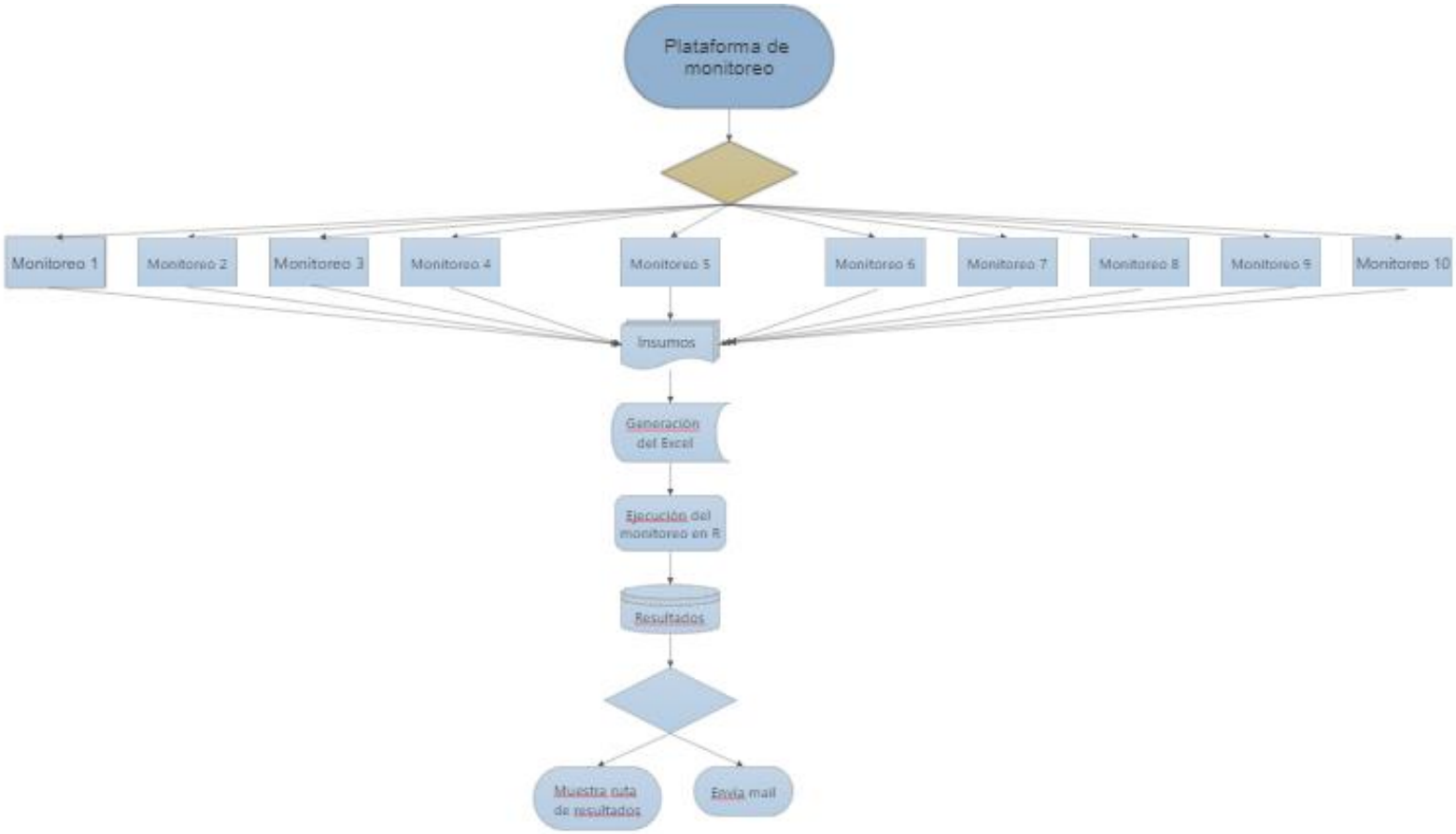



Figura 10. Diagrama de flujo de la solución.

*Fuente: Elaboración propia*

## 3.4 IMPLEMENTACIÓN DE LA SOLUCIÓN

El siguiente paso después de realizar una plataforma para integrar todos los monitoreos, es la implementación de esta solución; ella se llevó a cabo en el equipo del practicante de seguridad de la Información y ciberseguridad, y los códigos e insumos se almacenarán en la red corporativa, pues de esta forma todos los integrantes del equipo podrán hacer uso de ellos cuando sea necesario.

El primer paso de la implementación es la definición de las rutas en las cuales se encontrará cada uno de los códigos fuente. La red corporativa cuenta con una carpeta para cada una de las áreas, la cual tiene el acceso restringido únicamente a los colaboradores del equipo; Monitoreos es una carpeta que se encuentra dentro de seguridad de la información, allí se crea una carpeta por cada uno de los 10 monitoreos sistematizados que existen en la compañía, y se tienen carpetas por año y mes, con los insumos y resultados respectivos, llevando así la trazabilidad de los mismos. En monitoreos se encuentra “monitoreos.py”, la interfaz principal (Anexo A), en donde se encuentran 10 botones, al seleccionar cada uno se presenta una segunda ventana, con la interfaz propia de cada monitoreo (Anexo B), el código de la segunda ventana, junto con los R, se encuentran dentro de cada una de las respectivas carpetas del monitoreo, como se presenta en la Figura 11.

Posteriormente, con las rutas definidas, solo queda cambiarlas en los códigos, y hacer las pruebas pertinentes para validar que todo el funcionamiento este en orden.

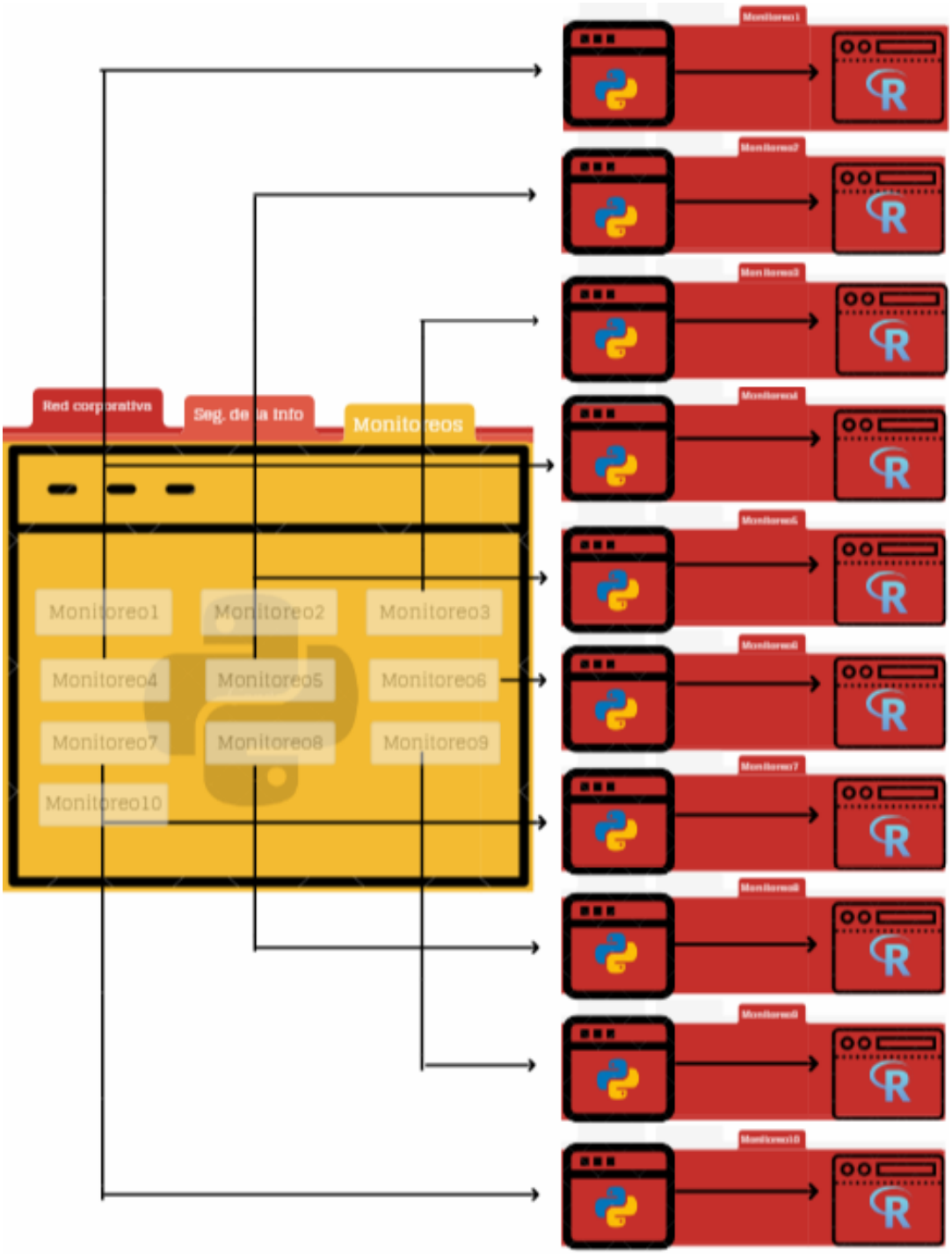



Figura 11. Diagrama de scripts.

*Fuente: Elaboración propia*

## 3.5 VALIDACIÓN DE LOS REQUERIMIENTOS

Este es el último paso del desarrollo de este proyecto, pero no el menos importante, pues en el caso de que aquí alguno de los requerimientos no se cumpla, significa que la plataforma pueda tener problemas en un futuro.

A continuación, se presenta cada uno de los requerimientos y su validación:

- Ventana principal: Para validar este requerimiento es necesario después de crear la ventana que direcciona a los diferentes monitoreos, probar con cada uno de los botones que funcionara, en la Figura 12, se presentan dos ejemplos, monitoreo 1 y monitoreo 2.

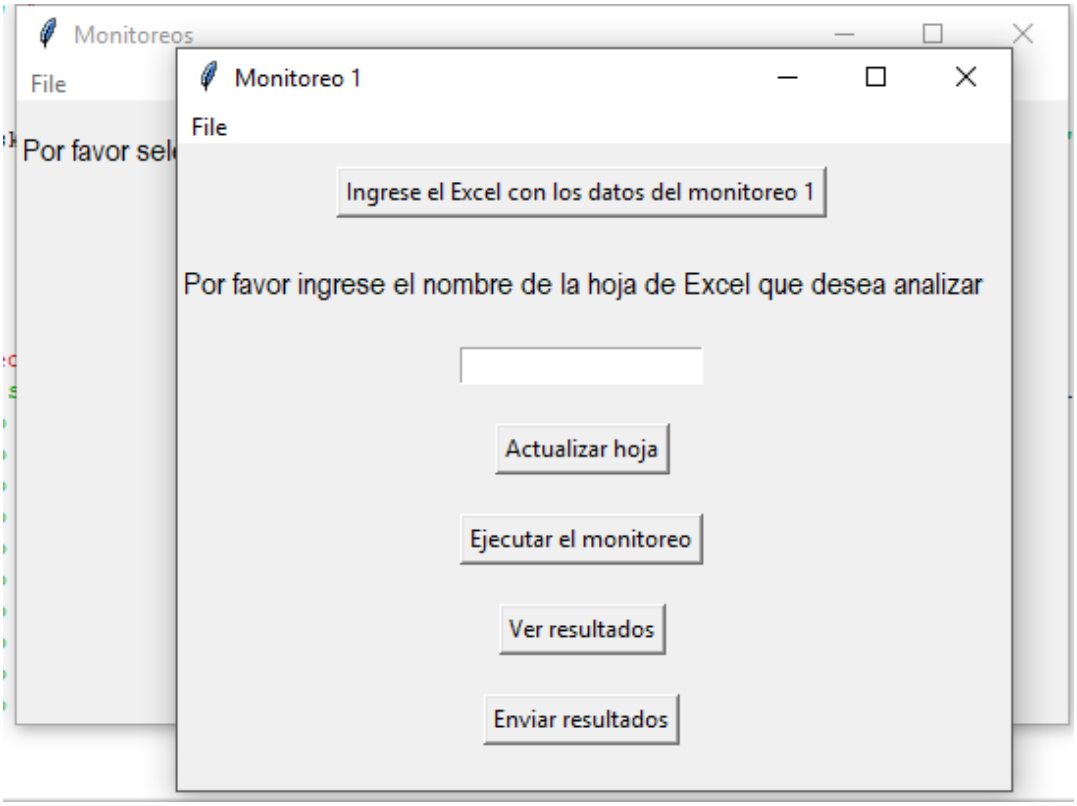
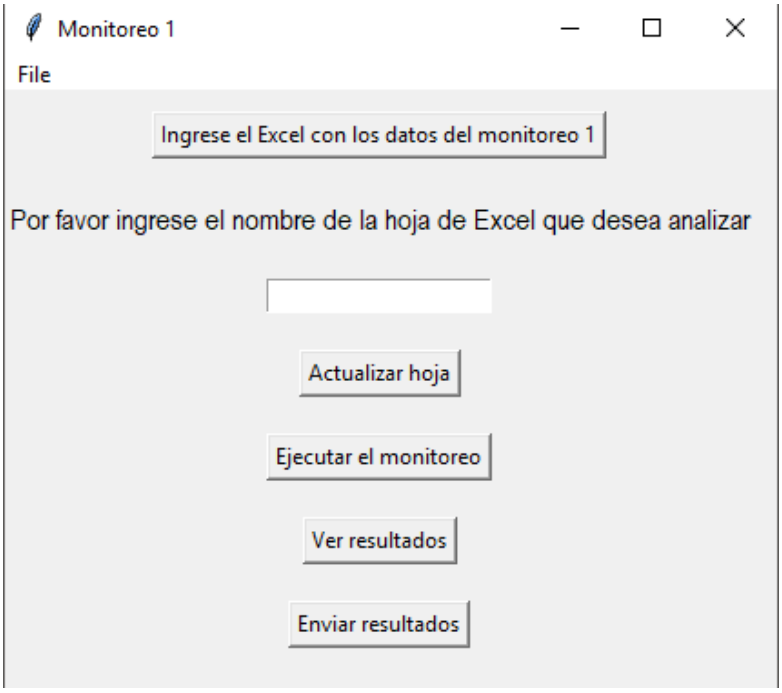


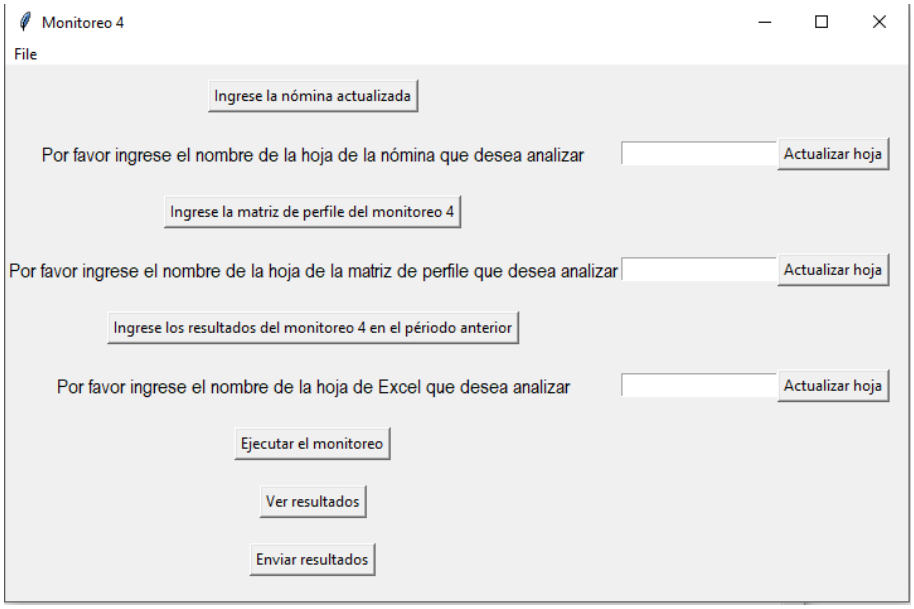

Figura 12. Validación de la ventana principal con 2 monitoreos.

*Fuente: Elaboración propia*

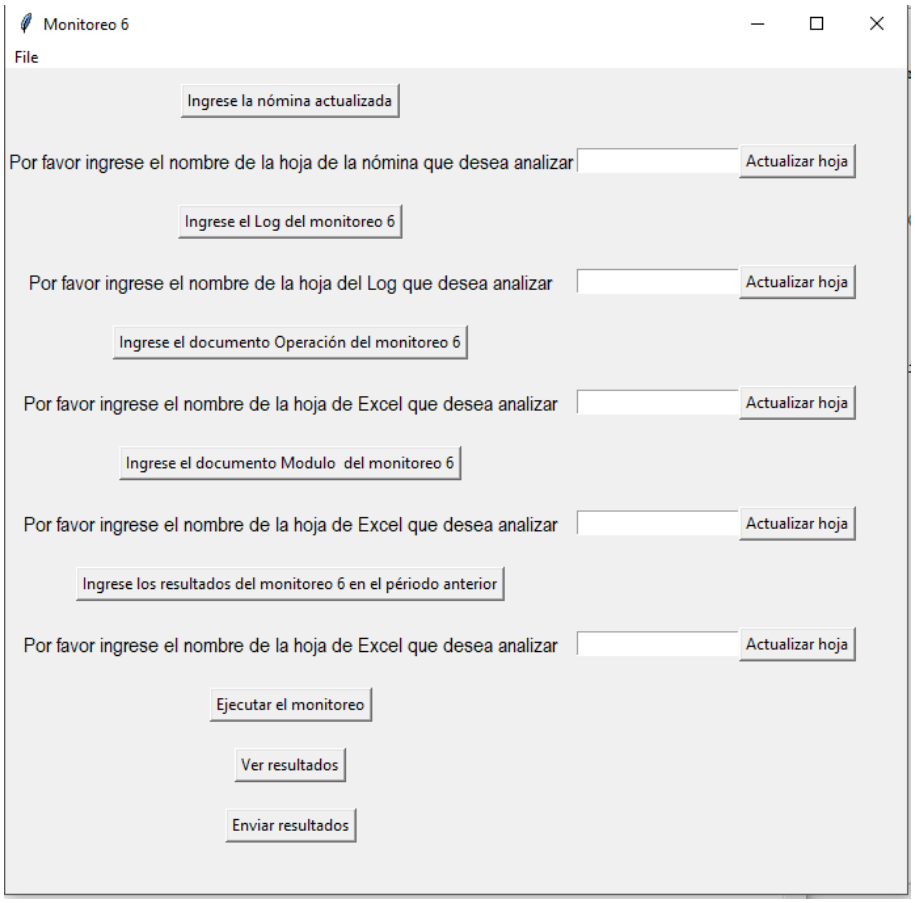
- A cada uno de los monitoreos se les ingresa el número de insumos que requieran: La validación de este requerimiento consiste abrir la interfaz de los diez monitoreos, ejecutarlos, y verificar que tengan de entrada la cantidad de insumos que se presentan en la Tabla 1., en la Figura 13, se presentan un ejemplo por cada cantidad de insumos presentados en la Tabla 1.




a. 1 insumo




b. 3 insumos




c. 5 insumos

Figura 13. Cantidad de insumos.

*Fuente: Elaboración propia*

- Resultados del monitoreo: Cuando el monitoreo se termina de ejecutar por R, automáticamente los resultados se guardan en la ruta que tenga definido el programa, la forma más fácil de verificar si el monitoreo se ha ejecutado correctamente, es ingresar a dicha ruta y mirar si hay documentos nuevos, y que la información allí sea correcta.
- Visualización de los resultados: Posterior a la verificación de los resultados, es necesario que el usuario sea capaz de verlos sin necesidad de buscar la ruta en el código de R, por lo tanto, cuando finalice el monitoreo, el usuario podrá seleccionar el botón ver los resultados, y se le presentará la ruta; la validación de este requerimiento se hizo a través de una prueba de este procedimiento, Figura 14.

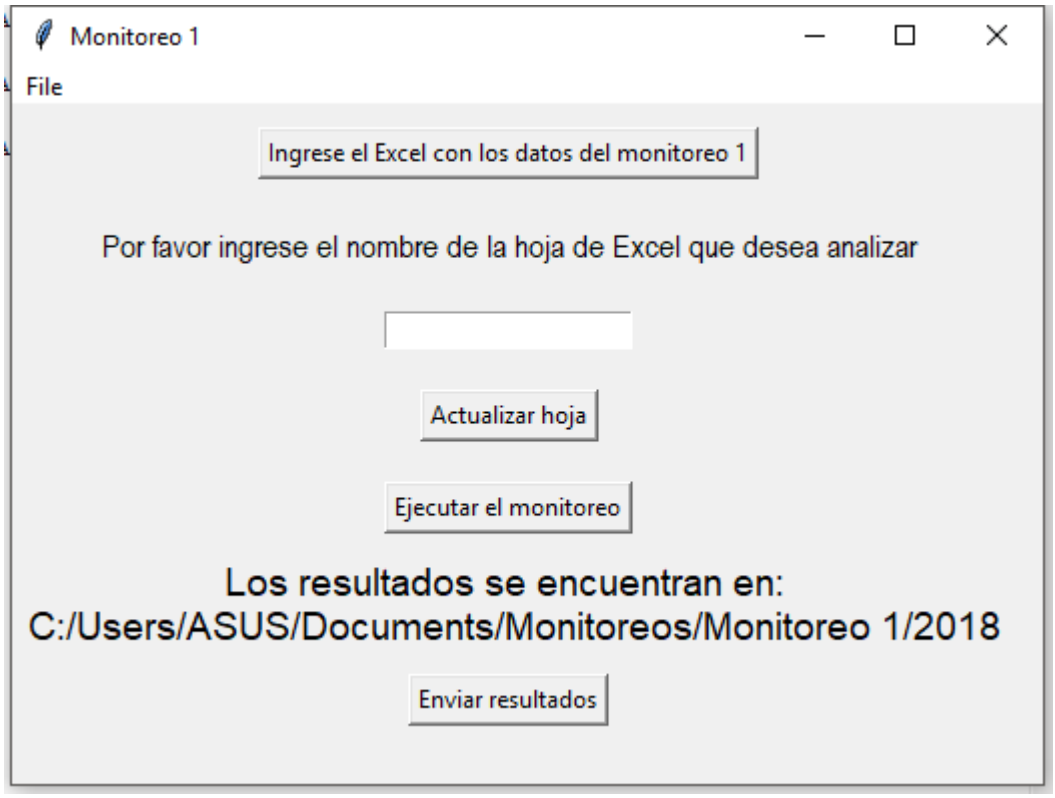



Figura 14. Visualización de resultados.

*Fuente: Elaboración propia*

- Resultados a través de correo electrónico: Para validar este requerimiento, se ejecutó un monitoreo, y se envió por correo electrónico los resultados, con correo remitente y de destino el del practicante de seguridad de la información y ciberseguridad, Figura 15.

```
import send_email

sendInst = send_email.send_email(service)
message = sendInst.create_message_with_attachment('carla.sayago@bvc.com.co','carla.sayago@bvc.com.co',
                                                  'Resultados desde python','PTI', 'resultados SOC-Sep 18.png' )
sendInst.send_message('me',message)
```

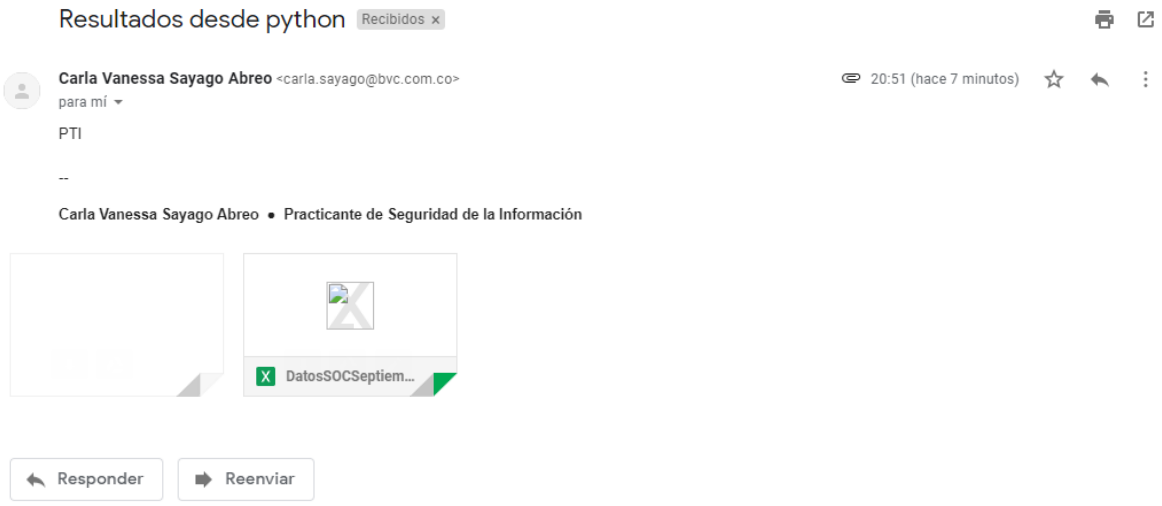



Figura 15. Código y correo con los resultados.

*Fuente: Elaboración propia*

- Usuarios de la plataforma: La verificación de este requerimiento se realiza desde el computador de otro integrante del equipo de seguridad de la información y ciberseguridad, diferente al practicante, y consiste en hacer un monitoreo desde su equipo a través de la plataforma.
- Plataforma intuitiva: Se les solicita a 5 personas del área de riesgos y procesos de la compañía que ejecuten el programa, se les indicaron donde estaban los insumos, al final los resultados del monitoreo fueron correctos.
- Confidencialidad: La validación de este requerimiento se hace cuando se le pide a las 5 personas ejecutar el código, y ellos solamente ven la interfaz gráfica, es decir no ven el procesamiento detrás de Python y R.
- Disponibilidad e integridad: Para validar estos requerimientos, se les pidió a las 5 personas de riesgos y procesos seleccionar diferentes botones en el orden que quisieran, y así mismo que ingresaran datos erróneos, para posteriormente ejecutar el monitoreo y verificar si los resultados continuaban siendo los mismos; después de esta actividad, el monitoreo continuaba ejecutándose sin problema alguno. Demostrándose así la integridad del código, pues nadie puede cambiar su contenido, y la disponibilidad, pues aunque se ingresen datos erróneos, el monitoreo no se ve afectado.

# 4 CONCLUSIONES

En el presente trabajo se presenta la implementación una plataforma que integre los monitoreos sistematizados de seguridad de la información y ciberseguridad en el área de riesgos de una compañía vigilada por la Superintendencia Financiera de Colombia, manteniendo su integridad, confidencialidad y disponibilidad, y así mismo optimizando el procedimiento de monitoreos. A continuación, se presentan las conclusiones del proyecto, y los posibles trabajos a futuro para desarrollar en la compañía como resultado de esta solución.

## 4.1 CONCLUSIONES

- A través de la revisión de los monitoreos se lograron identificar fallas en la integridad, disponibilidad y confidencialidad de los mismos, las cuales ponen en riesgo la información de la compañía y colaboradores de la misma, ya que, los datos que son manipulados en cada uno de los monitoreos se encuentra expuesto ante cualquier ataque, el cual podría llegar a perjudicar la reputación de la empresa.
- Se lograron establecer los requerimientos funcionales y no funcionales con base en las fallas de seguridad de la información en los monitoreos, dichas demandas permitieron crear una solución que cumplieron con todas las necesidades presentes en esta labor; hallando que los requerimientos no funcionales son más relevantes en esta compañía, puesto que se encuentra certificada en la norma ISO/IEC 27001:2013, y todos los lineamientos deben ser enfocados a proteger la disponibilidad, integridad y confidencialidad de la información.
- Se realizó una arquitectura para darle solución a las fallas existentes en el procedimiento de los monitoreos. El diseño de ésta se hizo a partir de cada uno de los requerimientos, tanto funcionales como no funcionales satisfaciendo a cabalidad las demandas de dicha función, la cual está a cargo de la coordinación seguridad de la información y ciberseguridad de la compañía.
- Mediante la implementación de la arquitectura fue posible optimizar el procedimiento de los monitoreos, así mismo, proteger la seguridad de la información de los éstos,

además de los datos que se manejan en ellos, esto a través de su confidencialidad, integridad y disponibilidad.

- A partir de la validación de los requerimientos establecidos se determinó que una plataforma de monitoreos es óptima como solución ante las fallas de seguridad de los monitoreos, así mismo ayuda a la compañía en pro de reducir el tiempo de ejecución de los mismos, y preservar su integridad, disponibilidad y confidencialidad.

## 4.2 TRABAJOS FUTUROS

Como continuación de este trabajo de grado implementado en una compañía vigilada por la Superintendencia Financiera de Colombia, se presentan algunos trabajos a futuro para diseñar e implementar como resultado de este proyecto, ya que por sobrepasar el alcance de esta monografía no fue posible realizar.

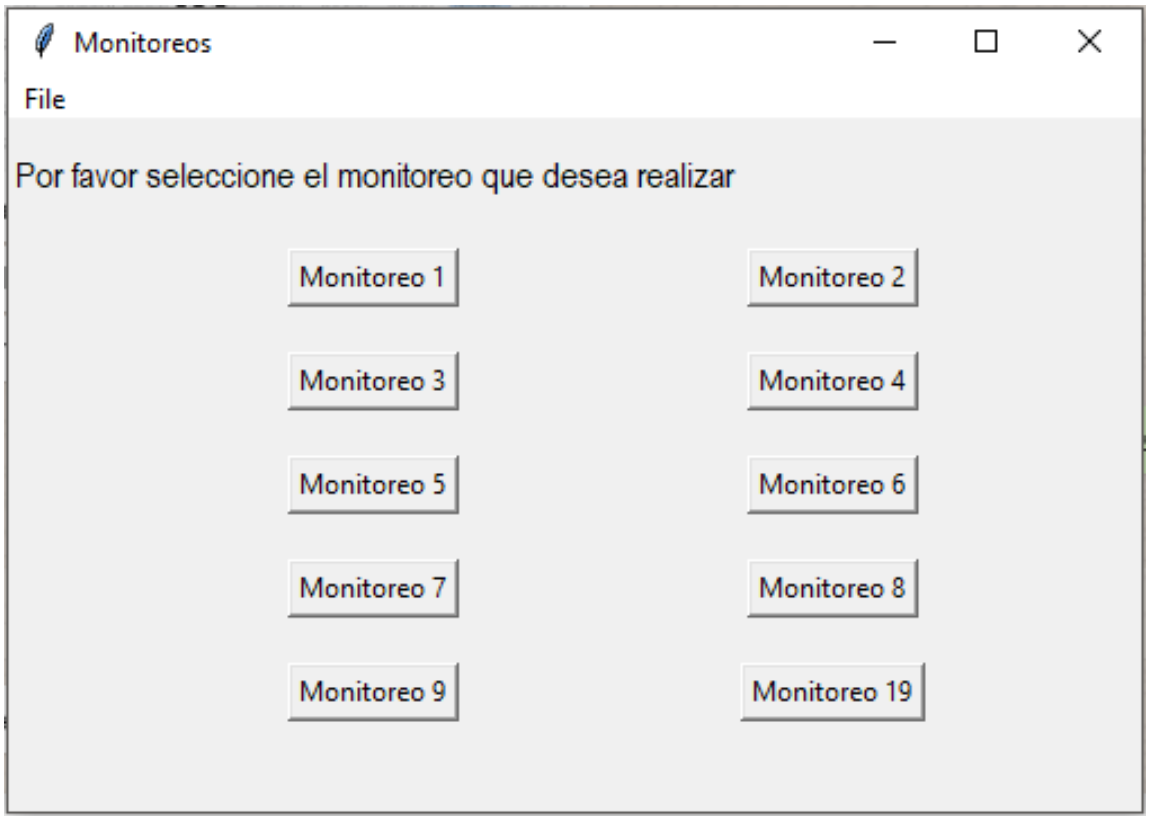
Con la reducción de tiempos en el momento de ejecutar los monitoreos, es posible generar nuevos monitoreos, ya sea sistematizándolos, o creándolos desde cero, para aportarle así un valor agregado a la compañía; algunos de los monitoreos podrían ser:

- DLP (Data Loss Prevention) para controlar la fuga de información a través del correo electrónico y la Gsuite.
- Activos de información, para controlar las modificaciones, creaciones o eliminaciones de los mismos.
- USB, para de esta forma controlar la información que los colaboradores de la compañía con autorización a este dispositivo cargan en el mismo
- Instalación de aplicaciones, para de esta forma controlar qué tipo de aplicaciones instalan los colaboradores, y si alguno lo hace sin los permisos.
- Acceso a las páginas web, pues en muchos casos los colaboradores acceden a sitios web no autorizados.

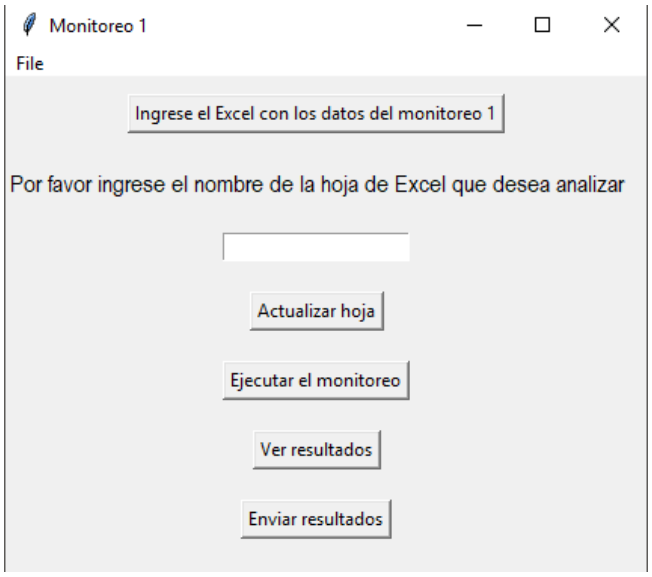
Una vez diseñados estos monitoreos podrían ser implementados en el lenguaje de programación R, y crear una interfaz propia en Python para añadirse a la plataforma integrada de monitoreos.

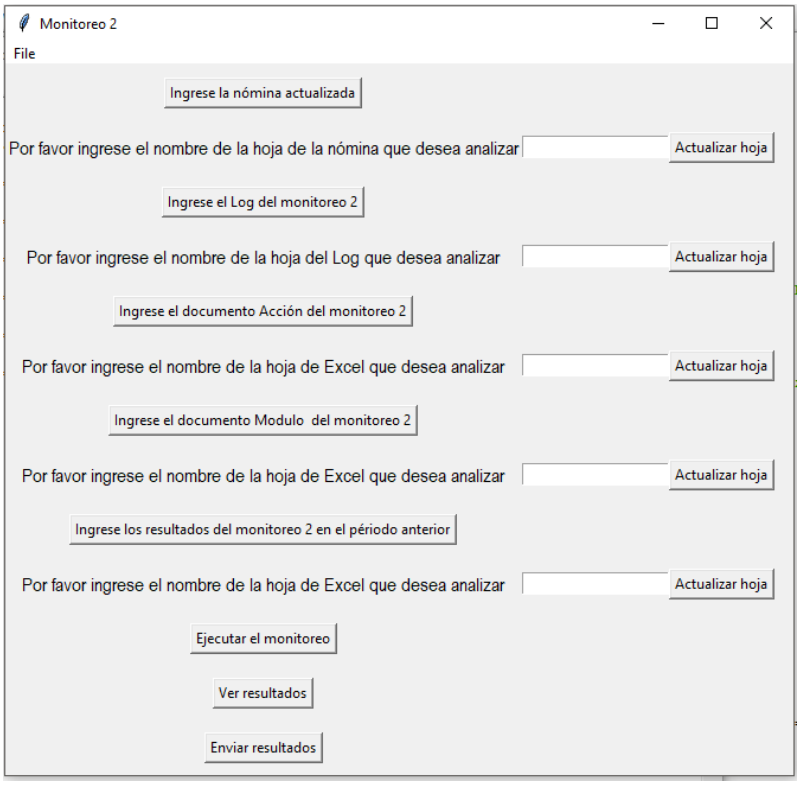
Así mismo, cada vez que se presente una oportunidad de mejora al monitoreo, esta podrá ser efectuada a través código fuente en R, y será un cambio transparente para el usuario, pues para él solo serán evidentes los cambios dentro de la plataforma de monitoreo.

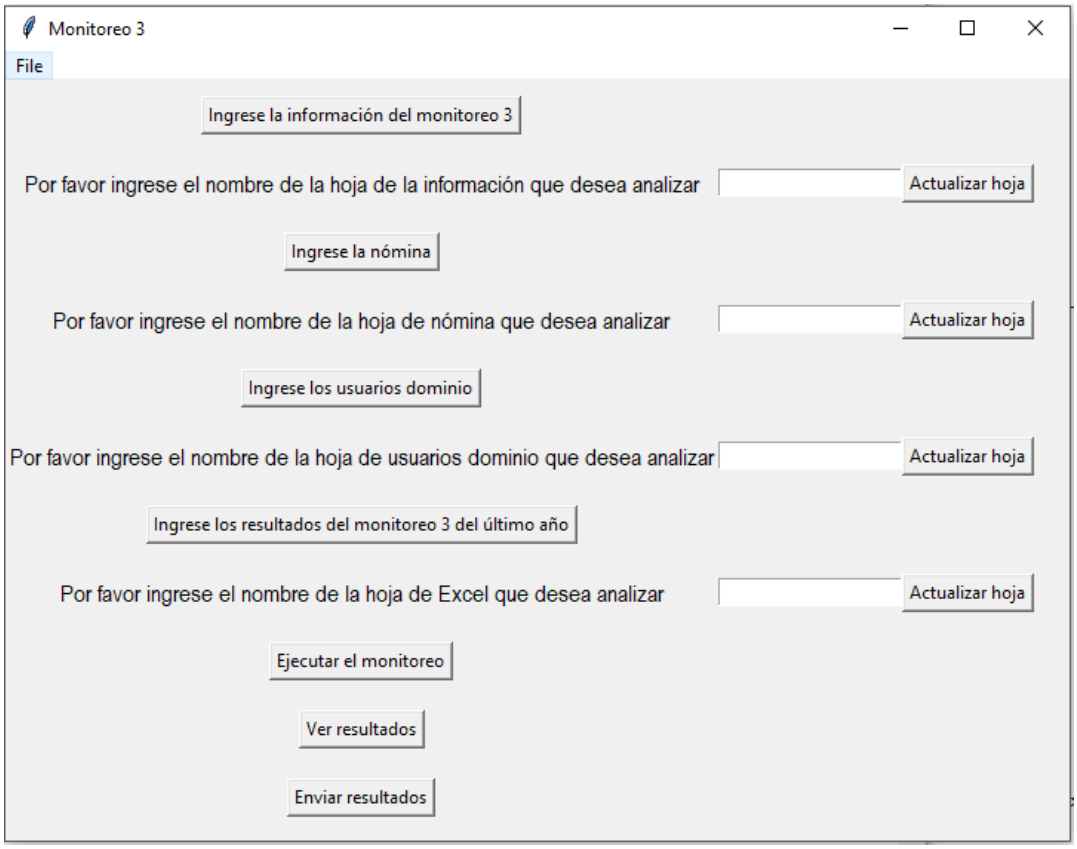
## ANEXO A: INTERFAZ GRÁFICA DE LA VENTANA PRINCIPAL

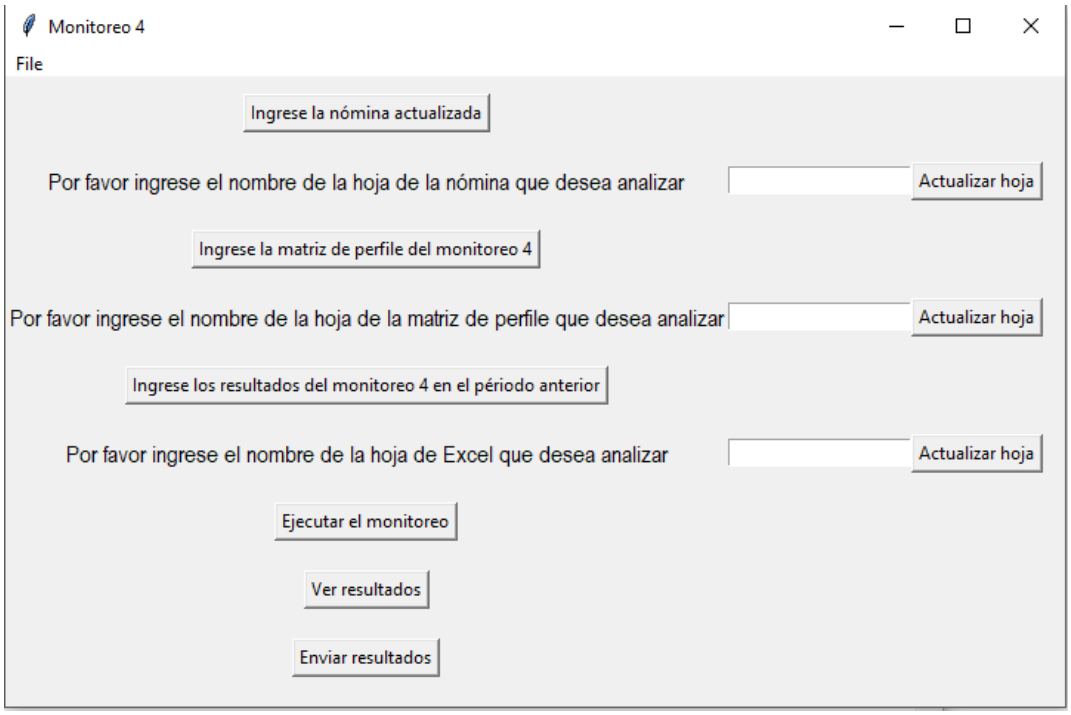


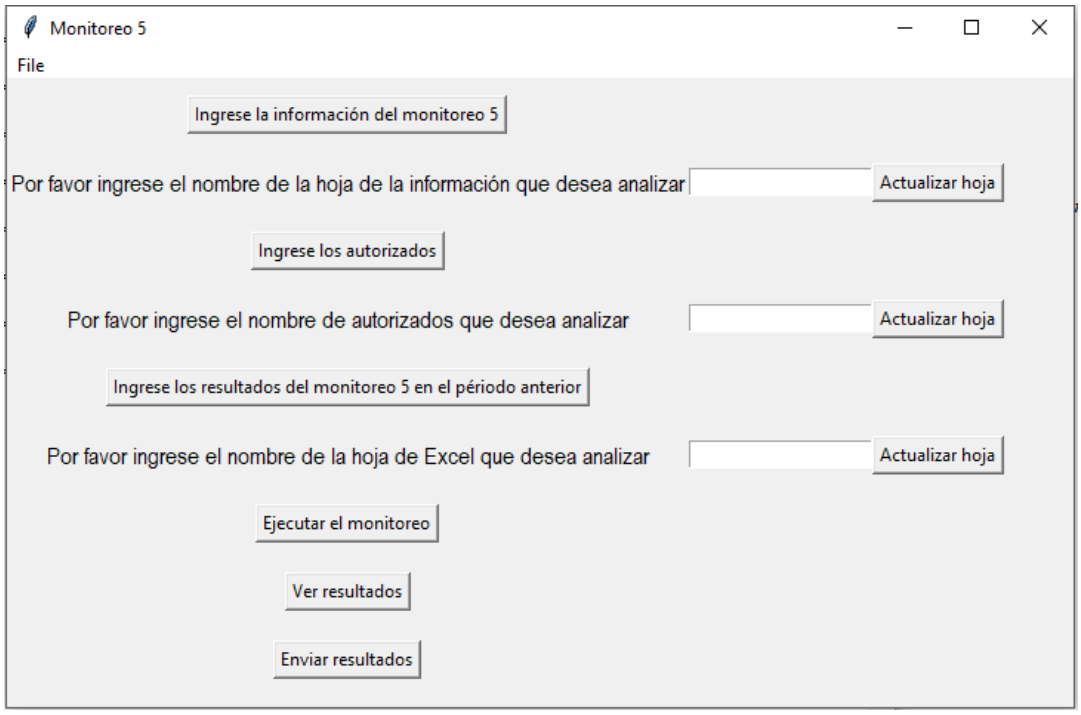
## ANEXO B: INTERFAZ GRÁFICA DE CADA MONITOREO

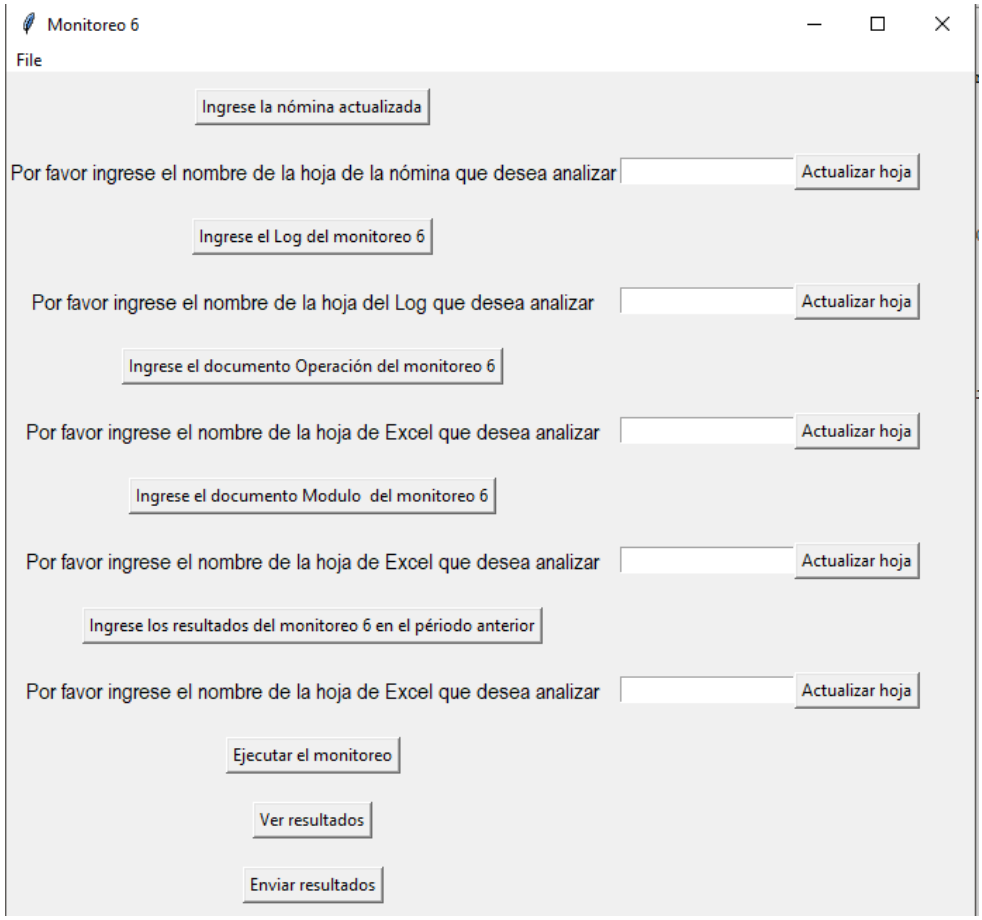


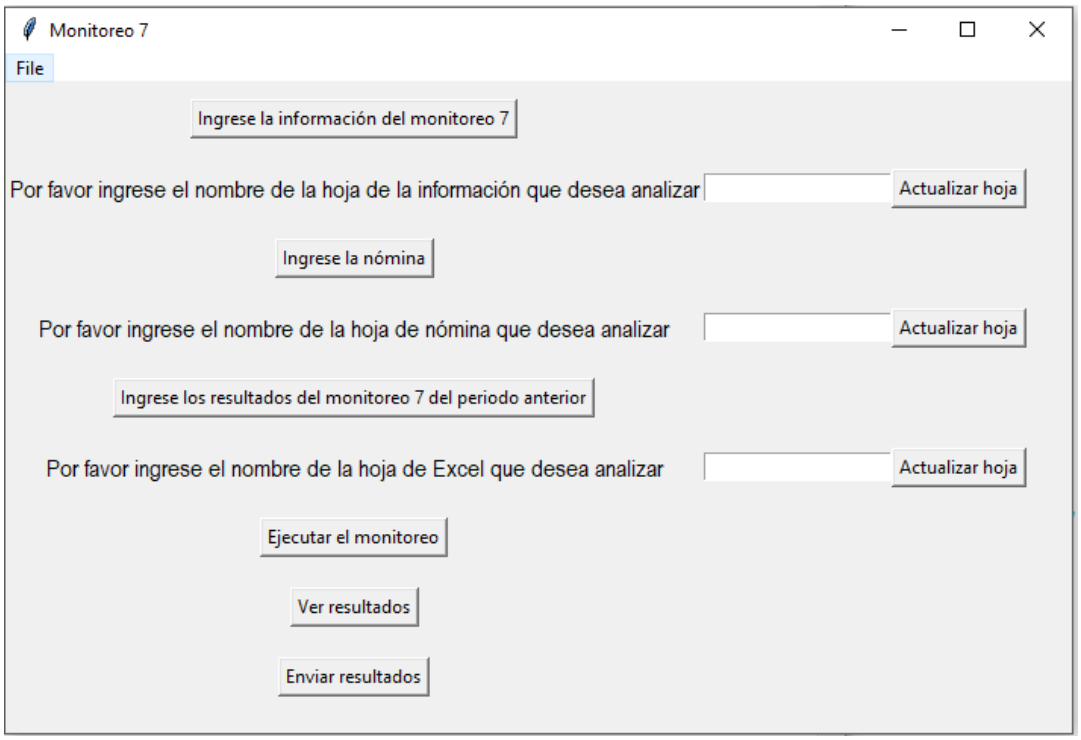



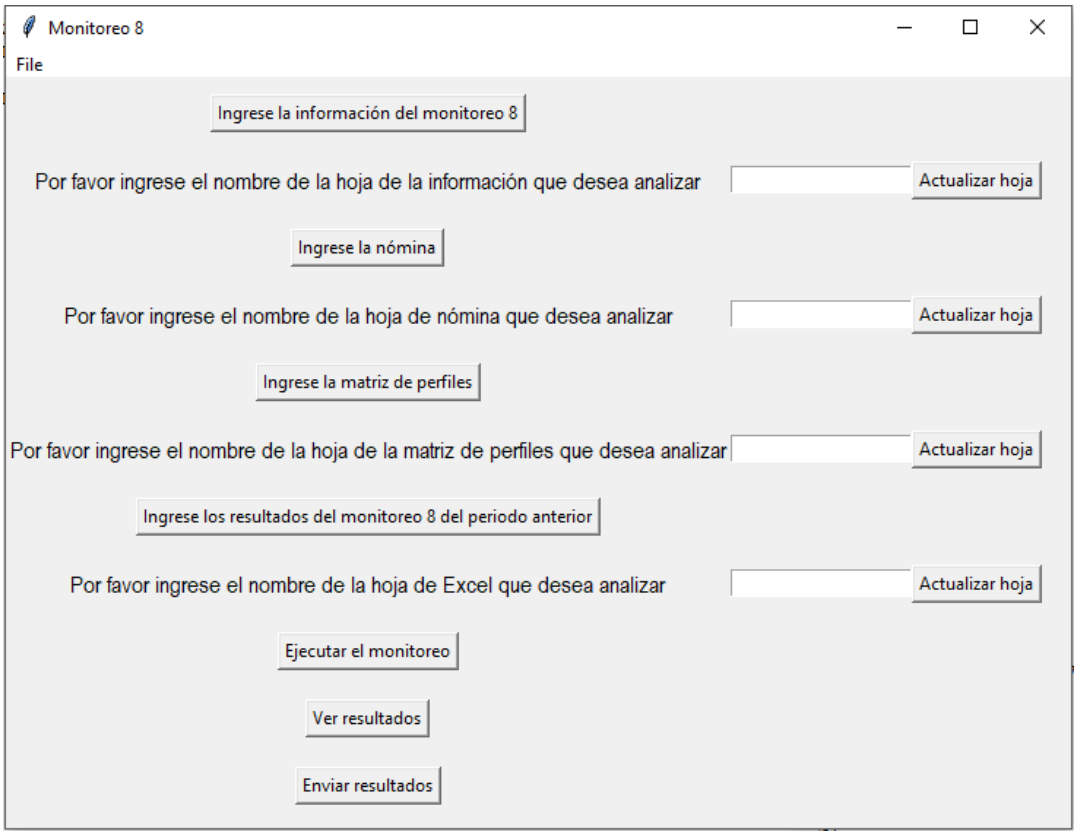

Monitoreo 3
File
Ingrese la información del monitoreo 3
Por favor ingrese el nombre de la hoja de la información que desea analizar
Actualizar hoja
Ingrese la nómina
Por favor ingrese el nombre de la hoja de nómina que desea analizar
Actualizar hoja
Ingrese los usuarios dominio
Por favor ingrese el nombre de la hoja de usuarios dominio que desea analizar
Actualizar hoja
Ingrese los resultados del monitoreo 3 del último año
Por favor ingrese el nombre de la hoja de Excel que desea analizar
Actualizar hoja
Ejecutar el monitoreo
Ver resultados
Enviar resultados

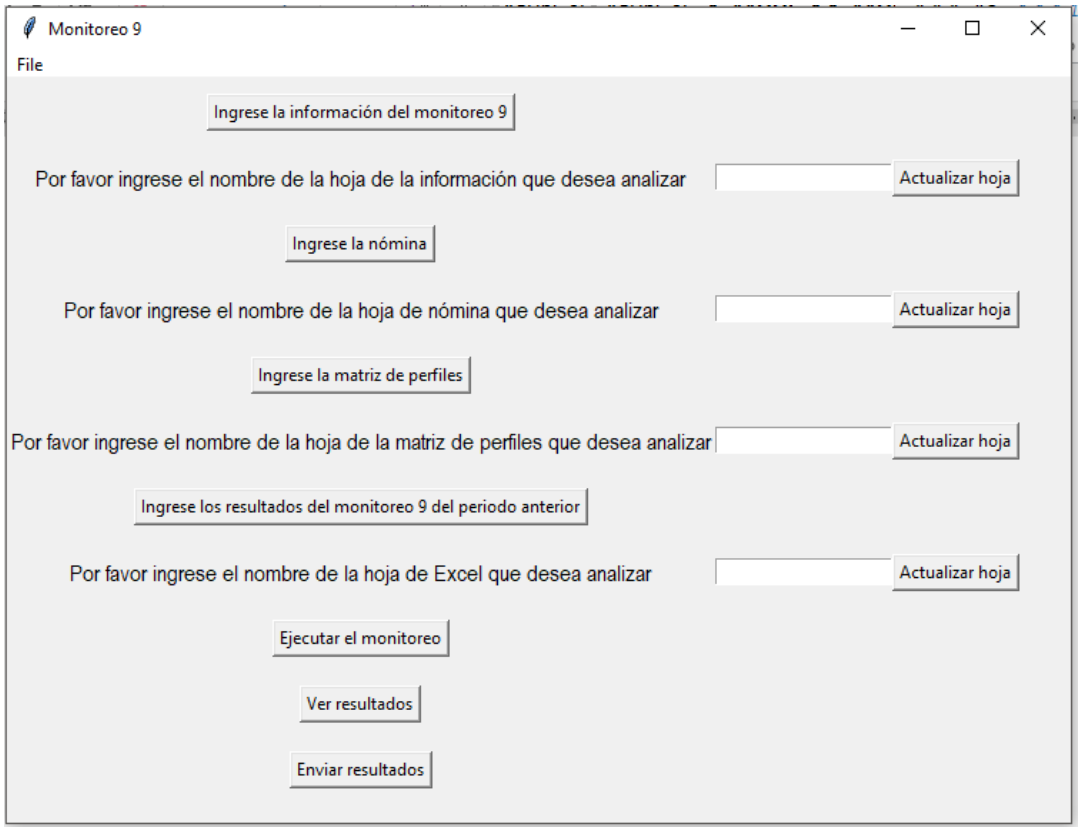

Monitoreo 4
File
Ingrese la nómina actualizada
Por favor ingrese el nombre de la hoja de la nómina que desea analizar
Actualizar hoja
Ingrese la matriz de perfile del monitoreo 4
Por favor ingrese el nombre de la hoja de la matriz de perfile que desea analizar
Actualizar hoja
Ingrese los resultados del monitoreo 4 en el período anterior
Por favor ingrese el nombre de la hoja de Excel que desea analizar
Actualizar hoja
Ejecutar el monitoreo
Ver resultados
Enviar resultados

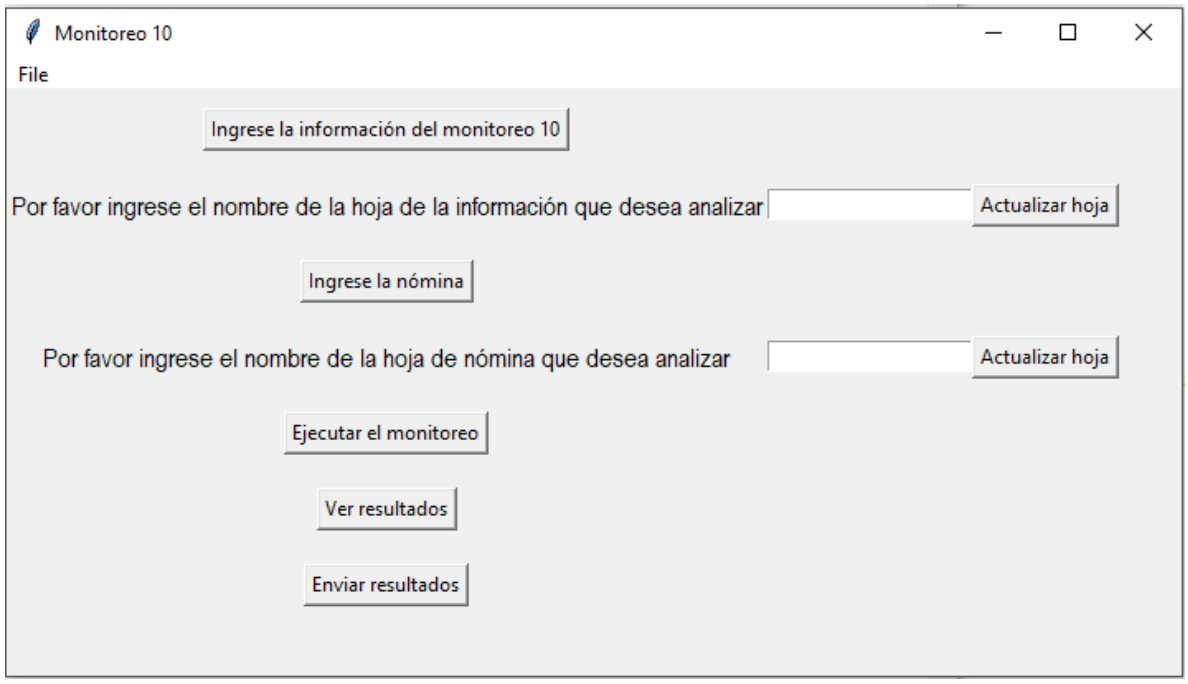

Monitoreo 5
File
Ingrese la información del monitoreo 5
Por favor ingrese el nombre de la hoja de la información que desea analizar
Actualizar hoja
Ingrese los autorizados
Por favor ingrese el nombre de autorizados que desea analizar
Actualizar hoja
Ingrese los resultados del monitoreo 5 en el período anterior
Por favor ingrese el nombre de la hoja de Excel que desea analizar
Actualizar hoja
Ejecutar el monitoreo
Ver resultados
Enviar resultados


Monitoreo 6
File
Ingrese la nómina actualizada
Por favor ingrese el nombre de la hoja de la nómina que desea analizar
Actualizar hoja
Ingrese el Log del monitoreo 6
Por favor ingrese el nombre de la hoja del Log que desea analizar
Actualizar hoja
Ingrese el documento Operación del monitoreo 6
Por favor ingrese el nombre de la hoja de Excel que desea analizar
Actualizar hoja
Ingrese el documento Modulo del monitoreo 6
Por favor ingrese el nombre de la hoja de Excel que desea analizar
Actualizar hoja
Ingrese los resultados del monitoreo 6 en el período anterior
Por favor ingrese el nombre de la hoja de Excel que desea analizar
Actualizar hoja
Ejecutar el monitoreo
Ver resultados
Enviar resultados


Monitoreo 7
File
Ingrese la información del monitoreo 7
Por favor ingrese el nombre de la hoja de la información que desea analizar
Actualizar hoja
Ingrese la nómina
Por favor ingrese el nombre de la hoja de nómina que desea analizar
Actualizar hoja
Ingrese los resultados del monitoreo 7 del periodo anterior
Por favor ingrese el nombre de la hoja de Excel que desea analizar
Actualizar hoja
Ejecutar el monitoreo
Ver resultados
Enviar resultados


Monitoreo 8
File
Ingrese la información del monitoreo 8
Por favor ingrese el nombre de la hoja de la información que desea analizar
Actualizar hoja
Ingrese la nómina
Por favor ingrese el nombre de la hoja de nómina que desea analizar
Actualizar hoja
Ingrese la matriz de perfiles
Por favor ingrese el nombre de la hoja de la matriz de perfiles que desea analizar
Actualizar hoja
Ingrese los resultados del monitoreo 8 del periodo anterior
Por favor ingrese el nombre de la hoja de Excel que desea analizar
Actualizar hoja
Ejecutar el monitoreo
Ver resultados
Enviar resultados


Monitoreo 9
File
Ingrese la información del monitoreo 9
Por favor ingrese el nombre de la hoja de la información que desea analizar
Actualizar hoja
Ingrese la nómina
Por favor ingrese el nombre de la hoja de nómina que desea analizar
Actualizar hoja
Ingrese la matriz de perfiles
Por favor ingrese el nombre de la hoja de la matriz de perfiles que desea analizar
Actualizar hoja
Ingrese los resultados del monitoreo 9 del periodo anterior
Por favor ingrese el nombre de la hoja de Excel que desea analizar
Actualizar hoja
Ejecutar el monitoreo
Ver resultados
Enviar resultados


Monitoreo 10
File
Ingrese la información del monitoreo 10
Por favor ingrese el nombre de la hoja de la información que desea analizar
Actualizar hoja
Ingrese la nómina
Por favor ingrese el nombre de la hoja de nómina que desea analizar
Actualizar hoja
Ejecutar el monitoreo
Ver resultados
Enviar resultados

## REFERENCIAS


[1] Ecuesta BID y Finnovista 2018.

[2] ISO/IEC 27001:2013

[3] W. M. R. Reales, «Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013,» Catalunya, 2016.

[4] ISO/IEC 27002:2013

[5] J. C. O. Gonzalez, «Diseño De Un Sistema De Gestion De Seguridad De La Informacion-Sgsi Bajo La Norma Iso/Iec 27001:2013 Para La Empresa "En Linea Financiera" De La Ciudad De Cali-Colombia,» Cali, 2016.

[6] L. B. Arfa, M. Jouini, A. B. Aissa y A. Mili, «A cibersecurity model in Cloud Computing Enviroments,» *Journal of King Saud University – Computer and Information Sciences,* 2012.

[7] Deloitte, «La Evolución de la Gestión de Cyber Riesgos y Seguridad de la Información,» Latinoamerica, 2016.

[8] A. M. Delgado, «Lineamientos, tendencias y estrategias sobre Ciberseguridad y Ciberdefensa en Colombia,» Bogotá, 2014.

[9] Superintendencia Financiera de Colombia, «Superintendencia Financiera de Colombia,» [En línea]. Available: https://www.superfinanciera.gov.co/jsp/index.jsf. [Último acceso: 29 11 2018].

[10] Circular Externa 029 (Circular Básica Jurídica), Superintendencia Financiera de Colombia.

[11] Circular Externa 042, Superintendencia Financiera de Colombia.

[12] Circular Externa 052, Superintendencia Financiera de Colombia.

[13] Circular Externa 007, Superintendencia Financiera de Colombia.

[14] J. W.-B. Lin, «Why Python Is the Next Wave in Earth Sciences Computing,» *Bulletin of the American Meteorological Society,* vol. 93, nº 12, 2012.

[15] J. C. K. S. Emmanuel Paradis, «Ape: Analyses Of Phylogenetics And Evolution In R Language,» *Bioinformatics Applications Note ,* Vol. 20, nº 2, pp. 289-290, 2004.

[16] R Core Team, «R Language Definition,» 2018, p. 55.

[17] A. E. Y. SK Ahammad Fahad, «Big Data Visualization: Allotting by R and Python with GUI Tools,» *IEEE ,* p. 8, 2018.

[18] J. S. F. B. M. N. Laurel Lord, «Survival analysis within Stack Overflow: Python and R,» *IEEE,* p. 9, 2018.

[19] C. P. I. C. B. S.-D. A. Ionuț-Daniel BARBU, «Intruder Monitoring System for Local Networks Using Python,» *Electronics, Computers and Artificial Intelligence ,* 2017.

[20] D. M. V. D. Ankur Gupta, «Web-Log Trend Pattern Analysis with Temporal Approach,» *IEEE.*

## LISTA DE FIGURAS

## LISTA DE TABLAS