Modelo de seguridad orientado a preservar la confidencialidad, integridad y privacidad de los datos, en un sistema para el almacenamiento y compartición de datos multimodales en entornos de investigación, soportado en bases de datos NoSQL.

Irving Lyonel Solsol Vilca

Instituto Tecnológico Metropolitano.
Facultad de Ingenierías, Departamento de Sistemas.
Medellín, Colombia.
2019

Modelo de seguridad orientado a preservar la confidencialidad, integridad y privacidad de los datos, en un sistema para el almacenamiento y compartición de datos multimodales en entornos de investigación, soportado en bases de datos NoSQL.

Irving Lyonel Solsol Vilca

Tesis o trabajo de grado presentada(o) como requisito parcial para optar al título de:
Magíster en Seguridad Informática.

Directores:
Gloria Mercedes Díaz Cabrera PhD.

Héctor Fernando Vargas Montoya MSc.

Línea de Investigación:
Procesamiento de datos de alta dimensión.

Grupo de Investigación:
Máquinas Inteligentes y Reconcomiendo de Patrones.

Instituto Tecnológico Metropolitano - ITM.
Facultad de Ingenierías, Departamento de Sistemas
Medellín, Colombia
2019

Dedicatoria

A mis padres, que siempre han estado presente a lo largo de mi formación profesional.

A mis hermanos, para que tengan referencia de que la perseverancia y la dedicación abre nuevas puertas que nos lleva lejos.

A mi esposa, que gracias a su constante apoyo, me ha permitido superar todos los obstáculos presentados a lo largo del desarrollo de este trabajo.

Agradecimientos

En principio, dar mi agradecimiento al Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior - ICETEX, así como también, al Programa Nacional de Becas y Crédito Educativo - PRONABEC, que a través de la Beca de Reciprocidad Perú - Colombia, me dieron la oportunidad de poder desarrollar la Maestría en Seguridad Informática, de igual manera, dar las gracias al Instituto Tecnológico Metropolitano - ITM, por aceptarme como estudiante y darme todas las facilidades para poder desarrollar exitosamente el programa de Maestría.

Muy especialmente, dar el agradecimiento a la PhD. Gloria Mercedes Días Cabrera, directora principal de este trabajo de grado, que junto a su acompañamiento, orientación y conocimientos compartidos, me ha permitido alcanzar los objetivos y metas trazadas durante el proceso de mi formación profesional; de igual manera, dar el agradecimiento al MSc. Héctor Fernando Vargas Montoya, codirector de este trabajo de grado, que con su conocimiento técnico, ha permitido dar claridad a muchas dudas, así como también darme la orientación para no desviarme del rumbo trazado en el desarrollo de este trabajo.

Finalmente, dar el agradecimiento a todos los docentes del programa de Maestría, que me brindaron su apoyo y me compartieron sus conocimientos, los cuales me permitieron seguir creciendo profesionalmente, así mismo, dar las gracias a los compañeros de estudios Paulo Diaz, Luis Castañeda, Luis Flores y a los compañeros del laboratorio de investigación MIRP Julián Arango, Andrés Pérez, Carlos Duarte, Fredy Torres, Rubén Fonnegra, Andrés Giraldo, entre otros, que me permitieron compartir gratas experiencias académicas, culturales, sociales y de ocio, en esta hermosa tierra colombiana.

Resumen

En los últimos años los entornos de investigación científica han avanzado en el desarrollo de proyectos colaborativos, en los que participan diferentes instituciones, incluso de diferentes organizaciones y países. Un componente importante de los procesos de colaboración en investigación, es la compartición de información, como pueden ser datos para experimentación de diferentes tipos, modelos computacionales, planos electrónicos, entre muchos otros, que pueden ser sensibles porque contienen información altamente relevante para el éxito de los proyectos, o incluso porque contienen información que puede ser sujeto de protección intelectual. Tradicionalmente, los investigadores han optado por compartir sus datos a través de correo electrónico, uso de dispositivos extraíbles y recientemente el uso de servicios de alojamiento de archivos en la nube y en todo caso descuidando los aspectos de seguridad para salvaguardar dicha información. Por lo anterior, este proyecto propone el desarrollo de un modelo de seguridad, orientado a mantener la seguridad de la información de los datos multimodales que se almacenan y comparten en un proyecto de investigación, el cual, a partir de un análisis de riesgos, definirá las políticas, procedimientos y controles que deberán ser implementados para el almacenamiento y compartición de datos de investigación. El proyecto incluye la implementación de mecanismos de seguridad en una base de datos NoSQL, dado su orientación al tratamiento de datos multimodales (característica de los datos generados en este tipo de ambientes). El modelo de seguridad y un prototipo del sistema de almacenamiento y compartición de datos serán implementados en el Laboratorio de Máquinas Inteligentes y Reconocimiento de Patrones del ITM, dado que en él se desarrollan actualmente proyectos en colaboración, en los que se produce información sensible.

Palabras clave: Análisis de riesgos, Modelo de seguridad, NoSQL, Datos no estructurados, Compartición de datos.

Abstract

In recent years, scientific research environments have advanced in the development of collaborative projects, in which different institutions participate, even from various organizations and countries. An essential component of collaborative research processes is information sharing, such as data for experimentation of different types, computational models, electronic designs, among many others. These components may be sensitive because they contain highly relevant information for the success of projects, or even because they contain information that may be subject to intellectual protection. Traditionally, researchers have opted to share their data via email, use of removable devices, and recently the use of cloud file hosting services, and in any case, neglecting the security aspects to safeguard such information. Therefore, this project proposes the development of a security model aimed at maintaining the security of the knowledge of multimodal data that is stored and shared in a research project. Based on risk analysis, it will set policies, procedures, and controls to implementing for the storage and sharing of research data. The project includes the implementation of security mechanisms in a NoSQL database, given its orientation to the treatment of multimodal data (characteristic of data generated in this type of environment). The security model and a prototype of the data storage and sharing system will be implemented in the ITM's Intelligent Machines and Pattern Recognition Laboratory, as it is currently developing collaborative projects in which it produces sensitive information..

Keywords: Risk analysis, Security model, NoSQL, Unstructured data, Data sharing

Contenido

Lista de Figuras

Lista de Tablas

1. Introducción

En los últimos años, se ha notado una tendencia creciente en la compartición de datos en el ámbito científico y académico [7, 39], con la finalidad de permitir que otros investigadores contribuyan a dar continuidad a los resultados de alguna investigación que se haya realizado o que haya quedado inconclusa; así como para poder generar nuevas investigaciones a partir de un resultado obtenido [3, 37]. En una encuesta denominada Open Science Researcher Insights, realizada por Wiley Soons a sus autores entre el 2013 y 2016, se encontró que el 69 % de estos comparten muchos datos a través de repositorios de datos específicos y generales; también por otros medios como conferencias y en algunas circunstancias de manera informal mediante correos electrónicos, contacto directo, etc. Esta creciente tendencia a la compartición demuestra que esta actividad es fundamental para la investigación [7, 39], por lo que en el campo de la seguridad de la información, trae retos importantes, debido a la necesidad de preservar la privacidad, la integridad y la confidencialidad de los datos a compartir [38], además del control adecuado del acceso a estos, según acuerdos establecidos. Lo anterior, dada la sensibilidad de esta información en términos de la protección intelectual y la confidencialidad de la información que cada grupo de trabajo debe tener.

Entre los diferentes aspectos que definen la manera como se aborda la seguridad de la información se encuentra la manera como esta es almacenada y compartida. Recientemente se han orientado esfuerzos para la creación de nuevos mecanismos de compartición de datos, que respondan a las diferentes necesidades de los modelos específicos de investigación [1] [2], entre los que se cuenta el compartir información de múltiples fuentes, y modalidades como son imágenes, señales, videos, correos electrónicos, archivos de procesador de texto, hojas de cálculo, modelos, entre otros[8]. Algunos sistemas de compartición de datos, diferentes a proveer un acceso a un directorio, propusieron que se realizará una extracción de datos estructurados de los contenidos no estructurados, estableciendo atributos bien definidos que se implementaban a través de bases de datos relacionales, que por lo general son de tipo texto [2]. Estos esquemas, limitan el uso de los datos originales, y por tanto el desarrollo de las investigaciones.

Desde hace algunos años se ha visto como una solución la introducción de base de datos no relacionales, también conocidas como bases de datos NoSQL (Not-Only Structured Query Language) [41], que trae importantes aportes para gestionar los grandes volúmenes de datos, como son: permitir el manejo y las eficientes consultas de grandes volúmenes de datos, esca-

[1] http://adni.loni.usc.edu/data-samples/access-data/

[2] https://www.kaggle.com/datasets

lar horizontalmente utilizando servidores básicos y almacenar datos semiestructurados y no estructurados [21]. A pesar de sus ventajas en el manejo eficiente de datos, las bases de datos NoSQL, desde su creación, han mostrado brechas de seguridad que, a pesar de los avances en su mitigación persisten en la actualidad [33], entre las que se encuentran vulnerabilidades de cifrado en los datos en reposo y en movimiento, además de vulnerabilidades en la autenticación, autorización y ser susceptible a los ataques de inyección de código. Estas brechas de seguridad deben ser tomadas en cuenta a la hora de implementar soluciones basadas en estas tecnologías, por lo cual el estudio de estas y cómo mitigarlas, sigue siendo un campo abierto de trabajo en el área de seguridad informática [4].

En el caso del Instituto Tecnológico Metropolitano – ITM, este cuenta con un sistema integrado de laboratorios llamado Parque i, que cuenta con 20 laboratorios que soportan los diferentes grupos de investigación, en el cual se vienen desarrollando investigaciones para diferentes áreas de aplicación, en el marco de las cuales, se realizan actividades de compartición de datos, tanto con investigadores a nivel institucional, como de otras instituciones y de otros países. Esta actividad se realiza de forma manual a través de dispositivos de almacenamiento externos, enlaces a servidores de la institución o a servicios externos como OneDrive, Dropbox, Google Drive, entre otros. Particularmente, en la línea de Investigación de Procesamiento de datos de alta dimensión, se vienen ejecutando proyectos como el "Protocolo abreviado de resonancia magnética asistido por computador para la detección y categorización de lesiones sospechosas de cáncer de mama", el cual se desarrolla en alianza con el Instituto de Alta Tecnología Médica (IATM) con financiación de Colciencias. En el marco de este proyecto, por ejemplo, las partes se comprometen a custodiar los productos tecnológicos resultado del proyecto, entre los cuales se cuenta una base de datos, conformada por un estudio retrospectivo y otro prospectivo; que, de acuerdo al diseño de la investigación, incluirá imágenes de diferentes modalidades (resonancia magnética, ultrasonido, mamografía, entre otras), información clínica, modelos computacionales y resultados del procesamiento de las mismas. Información que al ser accedida inadecuadamente puede poner en riesgo el desarrollo de la investigación.

Por lo anterior, como se ha evidenciado para otros ambientes de investigación a nivel mundial, se requiere proponer soluciones que permitan cumplir con los compromisos de custodiar dicha información y de preservar la seguridad de los datos sensibles que pueden generarse en estos laboratorios, considerando la diversidad de datos de cada proyecto y los compromisos de custodia que se acuerden para cada proyecto, sea propio o con otras entidades o sujetos particulares participantes en ellos.

En ese sentido, este trabajo inició con el desarrollo un análisis de riesgos informáticos que ha buscado identificar los riesgos y amenazas a las que se encuentran expuestos los datos generados, procesados y almacenados en estos tipos de entornos de investigación; para lograr esto, se adopta la metodología MAGERIT, que es una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [24], centrada en la gestión de riesgos de la información. Seguidamente, con los riesgos identificados y teniendo como soporte el modelo

de seguridad establecido por el MINTIC [25], se desarrolla un modelo de seguridad y privacidad de la información, acompañado de controles, políticas y procedimientos, los cuales fueron elaborados con base a la norma ISO/IEC 27001:2013 [18]; estos permitirán dar un tratamiento a las amenazas más críticas identificadas en dicho análisis de riesgos. Así mismo, referenciado en la descripción general del diseño de seguridad de infraestructura de Google [9] y las Consideraciones para un enfoque multidisciplinario en la ingeniería de sistemas seguros fiables, como la norma de referencia NIST SP 800-160 vol-1 [32], se desarrolla, una plataforma prototipo sobre una base de datos NoSQL, para el almacenamiento y compartición de datos de investigación, en ello, se implementan los controles, políticas y procedimientos de seguridad, que son aplicables del Modelo de seguridad. Finalmente, se realiza una verificación de cumplimiento funcional y técnico de los requerimientos de seguridad implementado en el prototipo de almacenamiento.

1.1. Problema a Resolver

El Grupo de Investigación Máquinas inteligentes y Reconocimiento de patrones, participa en el desarrollo de diferentes proyectos, en los que se generan conjuntos de datos que almacenan información de diferentes modalidades. Estas se generan, ya sea a partir de adquisiciones propias, diseñadas desde el comienzo para ser usadas para investigación, o a partir de datos compartidos por Instituciones externas. En los dos casos, el ITM, a través de los investigadores, adquiere el compromiso de preservar la protección de la información que maneja, en especial de preservar la privacidad de los sujetos participantes. Sin embargo, el tratamiento de esta información no se encuentra monitoreada; por lo que cada investigador da tratamiento a ésta de la mejor manera que crea conveniente, intentando preservar los compromisos firmados, ya sea mediante consentimiento informado o a través de convenios interinstitucionales. Sin embargo, la mayoría de estos investigadores no cuentan ni con el conocimiento, ni con las herramientas necesarias para dar un correcto tratamiento a la información para la reducción de los riesgos de exposición.

En la revisión de literatura se identifican trabajos que permiten implementar soluciones al manejo de datos no estructurados, mediante una base de datos NoSQL, sin embargo, también se ha encontrado que estas herramientas presentan vulnerabilidades que se encuentran en los datos en tránsito y en reposo, además de vulnerabilidades en la autenticación, autorización, así como también a los ataques de inyección. Esto se debe a que este tipo de bases de datos se encuentran más enfocados en el rendimiento y manejo de grandes volúmenes de datos que en la seguridad misma [41]. Los trabajos consultados en la revisión de literatura explican con claridad que los mecanismos de seguridad con las que estas bases de datos cuentan, son limitados, es por ello que para alcanzar un nivel aceptable de seguridad, se desarrolla e implementan configuraciones que permitan soportar la integración con algunas herramientas adicionales que permitan reforzar principalmente el cifrado de datos en tránsito y en reposo, además de incrementar la seguridad en la autenticación y autorización de accesos a los

motores y datos almacenados en estos tipos de bases de datos [33, 12, 10]. En todo caso, la definición e implementación de estos mecanismos depende del alcance y los requerimientos específicos del sistema, por lo cual es requerido realizar un análisis de riesgos de seguridad, que permita identificar los activos de información sensibles y sus riesgos asociados, en cada caso.
Por lo anterior, y dada la necesidad del ITM de controlar de manera responsable el tratamiento de la información y la compartición de datos multimodales que se maneja dentro de este entorno de investigación, se requiere responder a la pregunta de ¿Cómo proveer mecanismos para la protección de la seguridad de la información multimodal sensible que se genera, almacena y comparte en proyectos de investigación?,teniendo en cuenta que:

1. Los investigadores no conocen los aspectos exigidos para preservar la protección de los datos.

2. Que la solución debe permitir la protección tanto de datos adquiridos en los laboratorios del Instituto, como de los obtenidos por fuentes externas, con los que se tenga convenio.

3. Que la solución debe permitir compartir los datos multimodales, de manera segura, con investigadores internos y externos a la institución.

Para dar respuesta a este interrogante, este proyecto propone el desarrollo de un modelo de seguridad que integre controles y políticas de seguridad en un prototipo de sistema de información soportado en una base de datos NoSQL, dado que estas facilitan el almacenamiento de información multimodal. Desde el punto de vista de la seguridad de la información, esta solución plantea otros interrogantes que deberán ser abordados en el desarrollo del proyecto como son:

1. ¿Cuáles son los riesgos a la seguridad de la información que se presentan en los procesos de almacenamiento y compartición de datos de proyectos de investigación?

2. ¿Cuáles son las políticas y controles que deben conformar el modelo de seguridad para mitigar los riesgos en un ambiente de proyectos de investigación que maneje información sensible en bases de datos NoSQL?

3. ¿Cómo implementar los mecanismos y controles de seguridad en un sistema basado en bases de datos NoSQL para almacenar y compartir datos multimodales sensibles?

1.2. Hipótesis.

El desarrollo e implementación de un modelo de seguridad, que integre políticas, procesos, procedimientos y herramientas informáticas, apoyado en un sistema sobre bases de datos NoSQL, contribuirá en la protección de la información sensible, de diferentes modalidades, que se almacena y comparte en proyectos de investigación.

1.3. Objetivos.

1.3.1. Objetivo General.

Desarrollar un modelo de seguridad orientado a mantener la seguridad de la información de los datos multimodales que se almacenan y comparten en un proyecto de investigación, en un sistema basado en bases de datos NoSQL.

1.3.2. Objetivos Específicos.

- Realizar un análisis de riesgos para identificar las vulnerabilidades de seguridad de información que pueden afectar el proceso de almacenamiento y compartición de datos multimodales en un ambiente de investigación
- Definir el conjunto de políticas, procedimientos y controles para conformar el modelo de seguridad que permita gestionar los riesgos identificados.
- Desarrollar una plataforma sobre una base de datos NoSQL, que implemente mecanismos de seguridad requeridos para el almacenamiento y compartición de datos en investigación.
- Verificar el cumplimiento funcional y técnico de los requerimientos de seguridad implementados en el sistema de almacenamiento y compartición de datos.

2. Marco Teórico y Antecedentes

2.1. Análisis y gestión de riesgos informáticos

El análisis de riesgos, consiste en desarrollar un conjunto de actividades y procesos, que parte desde la identificación de activos informáticos, las amenazas y salvaguardas existentes, todo esto, junto a una adecuada valoración basado en los criterios establecidos por la metodología aplicada, permite obtener un mapa de riesgos informáticos y según las dimensiones de seguridad (disponibilidad, integridad, confidencialidad, entre otros.), se deberán desarrollar estrategias de seguridad que permitan abordar los riesgos y amenazas de seguridad informáticas de acuerdo a su nivel de impacto [24].

2.1.1. Análisis de riesgos informáticos

Es un proceso ordenado que agrupa un conjunto de actividades busca estimar la magnitud de los riesgos y amenazas a la que se encuentran expuestos los activos de información y está compuesta de los siguientes elementos:

a. Identificación y clasificación de los activos (Hardware, Software, Datos/Información, entre otros.) que requieren ser protegidos.

b. Valoración de los activos de acuerdo a su importancia e impacto que tendría dentro de una organización en caso de sufrir un daño o perdida.

c. Identificación y determinación las amenazas a las que están expuestos los activos anteriormente identificados.

d. Identificación de salvaguardas existentes y evaluar su eficiencia ante los riesgos identificados.

e. Evaluación de los impactos generados de las amenazas materializadas sobre los activos.

f. Evaluación de los riesgos ante la ocurrencia de las amenazas identificadas.

Al finalizar el análisis de riesgos se logrará tener un esquema detallado (mapa de riesgos) de los niveles de riesgos a las que están expuestos los activos de información para dar el tratamiento adecuado y oportuno [24, 11].

2.1.2. Dimensiones y criterios de valoración

Los valores de los activos son asignado cualitativamente con base a las dimensiones con las que se valoraran los activos.

Dimensiones.

Las dimensiones son características que permiten estimar el valor de un activo independientemente de la faceta del análisis de riesgos, por lo que al usarlos permiten estimar el valorar a consecuencias de que una amenaza se materialice y el perjuicio que representa para una organización si un activo se ve afectado en una dimensión determinada. En particular, se utilizarán las dimensiones de disponibilidad, integridad de datos y confidencialidad de la información.

a. **Disponibilidad**: Consiste en la disposición de los servicios a ser usados en el momento que se requiera.

b. **Integridad de datos**: Consiste en preservar la exactitud y estado completo de los datos almacenados en la base de datos.

c. **Confidencialidad de la información**: Consiste en garantizar que los datos estén protegidos y solo puedan ser accedidos por los usuarios que tengan la debida autorización.

Criterios de valoración.

a. **Valoración de activos.**
La valoración de los activos de información, es un procedimiento necesario que permite poder estimar la importancia que tiene cada uno de los activos, el valor se asigna bajo ciertos criterios, como el valor económico o impacto que pueda sufrir un activo según los principios de seguridad en entornos de disponibilidad, integridad y confidencialidad, para ello, la metodología MAGERIT establece una tabla de valoración detallada en la Tabla 2.1, basado en estos, se establecerán los valores.

Valor		Criterio
10	extremo	daño extremadamente grave
9	muy alto	daño muy grave
6 - 8	alto	daño grave
3 - 5	medio	daño importante
1 - 2	bajo	daño menor
0	despreciable	irrelevante a efectos prácticos

Tabla 2.1.: Criterio de valoración de activos [23].

b. **Valoración de amenazas.**
La valoración de las amenazas es de mucha importancia en un análisis de riesgos, debido a que cuando un activo se encuentra expuesto o es víctima de una amenaza, este, no es afectado en todas las dimensiones, ni tampoco de la misma forma, es por ello que la metodología establece criterios y valores de medición según su degradación y probabilidad de ocurrencia (con ello establecer los niveles de riesgos), estos se detallan en las Tablas 2.2 y 2.3 para así evaluar que tan afectado o comprometido se encuentra un activo ante la ocurrencia o materialización de una amenaza.

Valor		**Criterio**	
MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Tabla 2.2.: Criterio de degradación del valor [24].

Valor		**Criterio**	
MA	**100**	muy frecuente	a diario
A	**10**	frecuente	mensualmente
M	**1**	normal	una vez al año
B	**1/10**	poco frecuente	cada varios años
MB	**1/100**	muy poco frecuente	siglos

Tabla 2.3.: Criterio de probabilidad de ocurrencia [24].

c. **Valoración de salvaguardas.**
Valorar estos mecanismos de control identificados, es de mucha importancia, debido a que permite determinar el nivel de eficiencia y eficacia según su grado de madurez frente a un riesgo y la materialización de una amenaza. Para ello, en la Tabla 2.4, se detalla los niveles proporcionados por la metodología, dichos mecanismos de control deben ser evaluados al momento de realizar la calificación del riesgo, dado que estos pueden incidir en el resultado final.

Factor	Nivel	Significado
0 %	L0	inexistente
	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100 %	L5	optimizado

Tabla 2.4.: Criterio de valores de Salvaguardas [24].

d. **Valoración del Impacto y el riesgo.**

Impacto	
Valor	**Criterio**
[10]	**Nivel 10**
[9]	**Nivel 9**
[8]	**Alto (+)**
[7]	**Alto**
[6]	**Alto (-)**
[5]	**Medio (+)**
[4]	**Medio**
[3]	**Medio (-)**
[2]	**Bajo (+)**
[1]	**Bajo**
[0]	**Despreciable**

Riesgo	
Valor	**Criterio**
{9}	**catástrofe**
{8}	**desastre**
{7}	**extremadamente crítico**
{6}	**muy crítico**
{5}	**crítico**
{4}	**muy alto**
{3}	**alto**
{2}	**medio**
{1}	**bajo**
{0}	**despreciable**

Tabla 2.5.: Criterios de valores acumulados y repercutidos del impacto y el riesgo [20].

2.1.3. Gestión de riesgos informático

Es un proceso organizado, que permiten a las organizaciones controlar y gestionar los riesgos informáticos a los cuales se encuentran expuestos los activos de información. Estos procesos junto con la interacción de todas las partes involucradas de una organización, permitirán identificar e implementar las salvaguardas (controles) que permitan poder eliminar, prevenir, mitigar o controlar los riegos identificados [26, 16, 18].

2.2. Gestión de seguridad de la información

Son procesos definidos que busca preservar la protección de la información soportando por controles y políticas de seguridad bien definidas que deben permitir preservar la confidencialidad, integridad y disponibilidad de la información, así como también a los sistemas de

información con que estas interactúan, estos procesos además deben preservar la autenticidad y el no repudio de la información generada [17, 18].

Modelo de gestión de seguridad

Un modelo de gestión de seguridad, conforma parte de un Sistema de gestión de la seguridad de la información (SGSI), está compuesta por un esquema operacional soportado por la ISO 27001:2013 [25], éste permite poder establecer metas para gestionar adecuadamente la seguridad de los activos de información [25].

Metodología de gestión de riesgos

La metodología MAGERIT cuenta con un plan de seguridad [24], que permite poder gestionar adecuadamente la seguridad de los activos de información, esta metodología se encuentra alineada con lo establecido por la ISO/IEC 27001 y 27002, además de contar una herramienta que cuenta con los Código de buenas prácticas para la Gestión de la Seguridad de la Información [20].

Mecanismos de seguridad

Son mecanismos que permiten gestionar adecuadamente los controles de seguridad de la información, algunos de los mecanismos más importantes son [17]:

- **Autenticación.** Es el proceso de validación de la verificación de la identidad de un usuario que requiere acceder a la base de datos.
- **Autorización.** Consiste en establecer los permisos requeridos a un usuario para acceder a los datos almacenados en una base de datos.
- **Auditoría de datos.** Consiste en registrar todas las actividades generadas por los usuarios con la finalidad de poder identificar una acción realiza dentro de las bases de datos.
- **Cifrado de datos.** Es un proceso de codificación de datos que tiene como finalidad salvaguardar la confidencialidad de la información.
- **Cifrado de datos de reposo.** Consiste en cifrar los datos que se encuentran almacenados dentro de un sistema de información.
- **Cifrado de datos en tránsito.** Consiste en cifrar los datos que circulan durante la comunicación entre el usuario y un sistema de información y su propósito es dar confidencialidad y privacidad a esos datos, para ello, se usan protocolos como SSL, TLS, entre otros.

2.3. Almacenamiento y compartición de datos no estructurados

En la actualidad los datos no estructurados se vienen almacenando en bases de datos NoSQL, debido a sus características de flexibilidad, escalabilidad, alto rendimiento y alta funcionalidad. Este tipo de Base de datos ha servido para que hoy en día se desarrollen medios de compartición de datos como lo son Adni[1], que es una base de datos pública de estudio sobre el Alzheimer y Kaggle[2], que es una comunidad que contiene datos científicos, estadísticos e ingeniería para el aprendizaje automático, entre otros. Estos evidencian la actividad de compartir datos científicos en una comunidad de investigación [39].

Bases de datos NoSQL

NoSQL (Not Only SQL) [41], es un término que Carlo Strozzi en 1998 [36], utilizó para describir a un grupo de bases de datos que no son relacionales. Estas bases de datos tienen un esquema libre, por lo que no tiene una estructura definida para el almacenamiento de datos, no usan lenguaje SQL, tampoco permiten consultas joins, no garantizan la propiedad ACID (Atomicidad, Consistencia, Aislamiento, Durabilidad), hacen escalamiento horizontal, hacen uso amplio de la memoria principal del equipo donde opera, es una solución al problema de los altos volúmenes de información y a los grandes volúmenes de consultas y transacciones diarias, estos tipo de bases de datos diseñados para trabajar con datos no estructurados como las imágenes, señales, videos, correos electrónicos, archivos de procesador de texto, hojas de cálculo, etc. Existen cuatro tipos de bases de datos más representativas que usan sus respectivos sistemas de gestión de base de datos (SGBD) NoSQL [22, 41]:

- Orientado a documento: Son aquellas que trabajan con datos semi estructurados, como documentos. Estos datos son almacenados en formatos estándares como: XML, JSON o BSON. Este es el tipo de base de datos más usada, ya que se puede adaptar a gran cantidad de proyectos incluso con sistemas que funciona con una base dato relacional. Aquí se tiene a SGBD NoSQL como: MongoDB y CouchDB.

- Orientadas a columnas: Este tipo base de dato está definida para realizar consultas y agregaciones sobre grandes volúmenes de datos. Su desempeño es similar a las bases de datos relacionales, pero su almacenamiento es en columnas de datos en lugar de registros. Aquí se tiene a SGBD NoSQL como: Cassandra y HBase.

- Clave valor: Estas son las más sencillas de usar. Simplemente guardan secuencias de valores que poseen una clave y su valor. Cuando se quiere obtener un dato, solo se busca por su clave y se recupera el valor. Aquí se tiene a SGBD NoSQL como: DynamoDB, Redis.

[1] http://adni.loni.usc.edu/data-samples/access-data/
[2] https://www.kaggle.com/datasets

- Grafo: se encuentran definidas en la teoría de grafos, utilizan nodos y aristas para mostrar los datos almacenados. Son muy útiles para guardar información en diseños que trabajen con muchas relaciones, basadas en redes y conexiones sociales. Aquí se tiene a SGBD NoSQL como: Infinite Graph y Neo4j.

Estos tipos de bases de datos tienen el rendimiento operacional como función principal por lo que la mayoría de estos sistemas implementan mecanismos de seguridad predefinidos y básicos, estudios recientes han mostrado que se mantienen vulnerabilidades importantes que deben ser abordadas desde el diseño de las políticas y controles, según el caso de aplicación [33, 12].

2.4. Antecedentes de la seguridad de la información en Base de Datos NoSQL

Con la aparición y creciente implementación de los sistemas de gestión de bases de datos (SGBD) no relacionales (NoSQL), se han desarrollado investigaciones para abordar la identificación y mitigación de los Riesgos de seguridad en estas bases de datos [1, 6, 12, 33].
Las primeras investigaciones de los diferentes SGBD NoSQL [29], han iniciado con la identificación de las vulnerabilidades que algunos SGBD, ya que estos habían emergido con diversas vulnerabilidades, los cuales en su diseño no fueron considerados, esta investigación fue de gran importancia para poner mostrar los problemas de seguridad existentes en las organizaciones que optaban por esta tecnología, debido a que manejaban información sensible y esto ponía en riesgo la confidencialidad, integridad y privacidad de los mismos. En tal sentido, la seguridad que proporcionan estos sistemas por defecto es una capa muy delgada, comparada con los muchos retos que esta tecnología genera. Estas tecnologías trabajan con código abierto y hace que posean vulnerabilidades como la **autenticación** [34], explican que este mecanismo por lo general se encuentra desactivado y el nivel de seguridad que tiene es muy básico, por lo que permite que un atacante pueda evadir cualquier tipo de control, como consecuencia se genera otra vulnerabilidad, la de **autorización**, en este punto, los mismos autores recalcan que por defecto éste se encuentra desactivado en muchas bases de datos y que la implementación de mecanismos de control basados en roles es indispensable. Es claro que, si se logra obtener el acceso a través de un usuario autenticado, es posible tener control sobre algunos tipos específicos de datos, en la mayoría de los casos, la finalidad sería poder **escalar privilegios** dentro de las bases de datos [29].
En cuanto a las vulnerabilidades de **protocolos de conexión**, una investigación [4], muestra que estas bases de datos tienen dificultades para la comunicación entre nodos y la facilidad con que se logra configurar le hace vulnerable al acceso de los datos en tránsito que podría ser interceptados para insertar algún tipo de código camuflados en los datos y de esa forma le permitan tomar el control de las bases de datos; además de que existen problemas para el **cifrado de datos** [40]. En la vulnerabilidad de **inyección de código**, se han realizado

investigaciones de algunos ataques a través de inyección JavaScript e inyección PHP [30, 31, 1, 6, 14, 33], donde se muestran que muchos atacantes han logrado tener éxito y logran acceder sin autorización, con la finalidad de modificar la información almacenada y hasta apoderarse de la totalidad de la información, estas vulnerabilidades pueden llevar a que se materialice un ataque de **denegación de servicio (DoS)** que consiste específicamente evita el acceso de los usuarios a la base de datos, por lo que un atacante podría asumir el control total de una base de datos, como ha sido mostrado por [29, 4, 6]. Por otro lado la falta de **control de auditorías** [29, 40, 6, 34], en estos tipos de bases de datos dificulta poder supervisar y registrar las acciones individuales y en conjunto, efectuadas por los usuarios de bases de datos, así como también identificar registro de posibles intentos de sustracción de contraseñas, lo cual impide tomar medidas antes de la ocurrencia de posibles ataques.

Además de los trabajos en la identificación de las vulnerabilidades en los SGDB NoSQL, otros investigadores han abordado el trabajo de mitigación a estas vulnerabilidades, sin embargo, solo se han limitado a algunos mecanismos de seguridad en algunos SGBD, entre ellas están MongoDB, Canssandra y Neo4j. Shahriar & Haddad [34], propusieron incorporar políticas de seguridad, con lo cual se pretende tener definidos los requerimientos de seguridad específicos para las bases de datos NoSQL. Para concentrar la mitigación de la mayoría de las vulnerabilidades (autenticación, autorización, cifrado de datos, entre otros), diferentes autores han implementado **controles y filtros de seguridad en un middleware**, que es un software que permite conectar dos aplicaciones para pasar los datos entre ellos [41, 4, 13, 21, 34]. También Aviv Ron et al. [31], resalta la importancia de programar capacitaciones periódicas sobre implementación de mecanismos de seguridad dirigido a los desarrolladores de bases de datos, Por último, también se han definido algunos controles para **defenderse de ataques**, en los trabajo de Chahal et al. [4] y Aviv Ron et al. [31], recomiendan limitar la entrada de los usuarios a la validación en el acceso, también asignar controles a todos los usuarios para evitar la inyección de JavaScript y HTML a través de archivos y por último, verificar y filtrar las variables en las sentencias de consulta, esto con la finalidad de mitigar las vulnerabilidades en la infraestructura de diseño de las bases de datos. Hou et al. [14], menciona que los esfuerzos de mitigación no serán del todo efectivos si no se protege la infraestructura de red interna donde operan estos sistemas, con equipos específicos como los firewalls, implementando las configuraciones correspondientes.

En la reciente investigación de Saxena & Sachdeva [33], muestra que a la fecha algunas de las vulnerabilidades antes mencionadas, todavía representan amenazas a la seguridad de la información almacenada en bases de datos NoSQL, estas vulnerabilidades se muestran en la Tabla 2.6, donde se evidencia que los datos almacenados aun presentan amenazas importantes en la seguridad de los datos.

Categoría	MongoDB	Cassandra	Redis
Datos en Reposo	El cifrado de datos solo se enfoca a nivel de aplicación.	Débil mecanismo de cifrado de datos.	No soporta cifrado de datos y se almacenan como texto plano.
Datos en Movimiento	Débil mecanismo de cifrado de datos.	Los datos en el nodo cliente, y en la comunicación entre nodos no se encuentran cifrados.	La comunicación entre el cliente y el servidor no está cifrada.
Autenticación	No presente por defecto.	Parcialmente presente.	No soporta por defecto.
Autorización	No está presente por defecto y solo es posible por roles a nivel de base de datos.	No está presente como ajuste predeterminado.	No presente.
Ataque de Inyección	Posible, usando JavaScript	Posible, usando Cassandra Query Language (CQL).	No es posible.
Acceso al puerto público	Se ejecuta en el puerto 27017 por defecto y es de acceso público	Se ejecuta en el puerto 8888 por defecto, y puede ser excedido con este puerto.	Siempre escucha el puerto 6379 de forma predeterminada.
Enlace IP	Por defecto abierto al público	Por defecto abierto al público.	Por defecto abierto al público.

Tabla 2.6.: Las vulnerabilidades de seguridad bases de datos NoSQL
Fuente: Adaptada de Saxena & Sachdeva [33]

Es preciso tener en cuenta que las organizaciones que tienen implementado estos tipos de bases de datos han realizado esfuerzos en mitigar sus vulnerabilidades con la implementación de configuraciones de seguridad, sin embargo, estas medidas no son suficientes ya que los atacantes constantemente se encuentran explorando nuevas mecanismos y formas de vulnerar cualquier medida de seguridad implementada. Por otro lado, las vulnerabilidades identificadas y reportadas en el portal Common Vulnerabilities and Exposures (CVE), muestra una lista de vulnerabilidades de algunas bases de datos NoSQL, entre las más recientes que se han publicado se encuentran: CVE-2019-17426, CVE-2019-2390, CVE-2019-16869, CVE-2019-14439, CVE-2018-9327, CVE-2018-8073, encontrados en las bases de datos MongoDB, Cassandra, Redis y CouchDB. Las publicaciones de estas vulnerabilidades detallan técnicamente más a fondo lo descrito con anterioridad.
Con las recomendaciones y los esfuerzos realizados por diferentes investigadores y desarrolladores a través de los trabajos realizados, se evidencia que los SGBD NoSQL, aún no son totalmente seguras, por lo que la implementación de mecanismos de seguridad en estas bases de datos, sigue siendo un tema abierto en investigación [29, 28, 40, 13, 14, 34].

3. Diseño metodológico

El desarrollo de este trabajo, comprendió de 4 fases ilustrada en la Figura 3.1. La **primera etapa**, inició con la realización de un análisis de riesgos informático dentro del entorno de investigación del Laboratorio de Máquinas Inteligentes y Reconocimiento de Patrones - MIRP y los laboratorios del Instituto de Alta Tecnología Médica - IATM, mediante el cual se han identificado los activos de información y los riesgos de seguridad de la información que se presentan en el almacenamiento y compartición de datos en los procesos que comprenden el desarrollo de una investigación, dentro de un ambiente de investigación. La **segunda etapa**, consistió en desarrollar un modelo de seguridad con los respectivos controles, políticas y procedimiento de seguridad, basados en los riesgos con mayor impacto, identificados en el análisis de riesgos, dichos controles fueron soportados por lo establecido en las normas ISO/IEC 27001:2013 [18] y 27002:2014 [19], se usó esta norma dado el amplio repertorio y buenas prácticas a nivel mundial que se tienen para la reducción de riesgos a través de diferentes controles adicionales, ya que la metodología MAGERIT en la gestión de riesgos, tiene un enfoque más técnico y dentro del proceso, se encontraron riesgos de tipo administrativo, por eso la selección de una norma que permita ser más amplia en su contexto. En la **tercera etapa**, se desarrolló un prototipo de sistema que permite el almacenamiento y compartición segura de datos en un entorno de investigación, en ella se incorporó mecanismos de seguridad, que fueron definidos en el modelo de seguridad y han permitido abordar las amenazas con mayor impacto, identificados en el análisis de riesgos. Este prototipo de sistema está soportado por una base de datos NoSQL [41], debido a su orientación al almacenamiento de grandes volúmenes de datos no estructurados. Para el diseño de la arquitectura se referenció en la Descripción general del diseño de seguridad de infraestructura de Google [9] y las Consideraciones para un enfoque multidisciplinario en la ingeniería de sistemas seguros fiables de la NIST SP 800-160 vol-1 [32], Por último, la **cuarta etapa**, se verificó el cumplimiento funcional y técnico de los requerimientos y componentes de seguridad implementados, la evaluación se basó por lo establecido en uno de los controles en la norma ISO/IEC 27001:2013 [18].

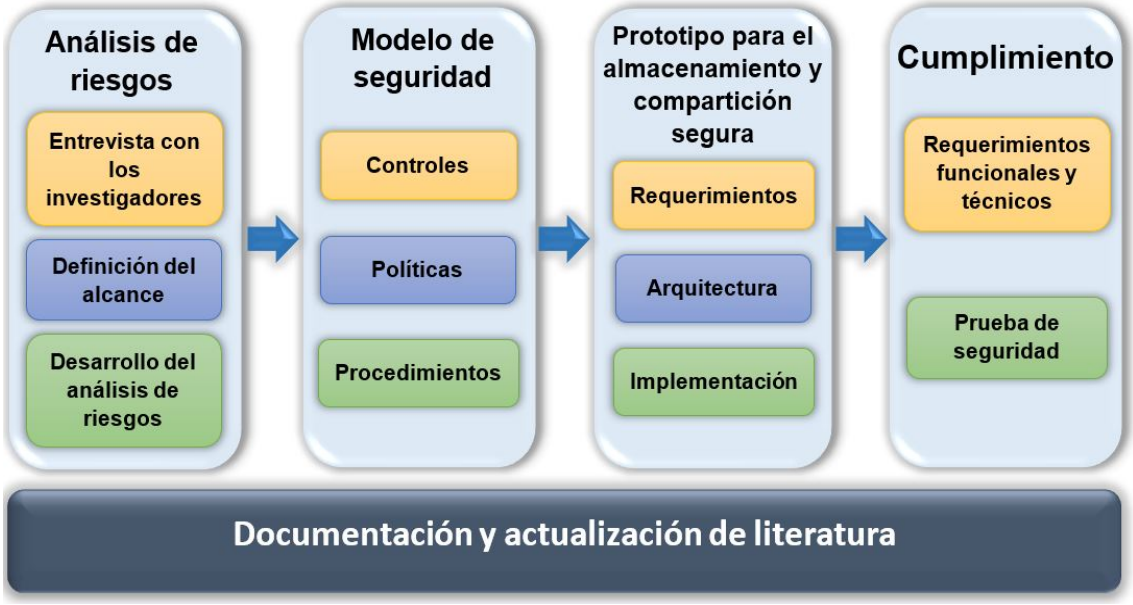


Figura 3.1.: Diseño metodológico del proyecto
Fuente: Elaboración propia.

3.1. Etapas de la Metodología

Primera etapa: Desarrollo de un análisis de riesgos

Para esta etapa, el análisis de riesgos se realizó haciendo uso de la herramienta EAR/PILA para la versión 3 de la metodología MAGERIT (Figura 4.1.), así mismo, se tuvo en cuenta la ISO 27001:2013 como complemento para diferentes riesgos encontrados. Dicha herramienta fue solicitada oficialmente (con su respectiva licencia) al encargado de la administración del software en ar-tool[1], en España. Esta primera etapa se inició desarrollando reuniones con los investigadores que se encuentran dirigiendo proyectos de investigación, estas reuniones permitieron identificar los escenarios de investigación y la forma de cómo aplicar el análisis de riesgos. A partir de las reuniones, se definió el alcance del análisis de riesgos, que ha permitido conocer los límites de esta etapa, junto al tipo de información recolectado y los resultados mostrados.

El análisis de riesgos, estuvo centrado en identificar las amenazas y riesgos en el manejo de los datos en los procesos que comprenden el desarrollo de una investigación, dentro de un ambiente de investigación. Debe aclararse que, aunque esta etapa se realizó en los laboratorios MIRP y IATM, este análisis se orientó a la identificación de amenazas y riesgos en términos generales, para este tipo de procesos y ambientes, por lo que se tomó como caso práctico al proyecto "Protocolo abreviado de resonancia magnética asistido por computador para la detección y categorización de lesiones sospechosas de cáncer de mama", debido a que en este

[1] https://www.ar-tools.com/magerit/index.html

proyecto se maneja información de carácter confidencial que contiene información sensible y presenta aspectos relevantes en cuanto al tipo de información que se almacena y comparte en la colaboración con diferentes instituciones, de forma tal que el modelo a desarrollar pueda implementarse en otros laboratorios. El análisis de riesgo se desarrolló usando la Metodología de Análisis y Gestión de Riesgos – MAGERIT V.3 [24], ya que se centra en la gestión de riesgos de la información y cumple con lo que establece la norma ISO/IEC 27001 en su numeral 8.2 evaluación de los riesgos para la seguridad de la información, donde la norma establece los criterios que hay que tener en cuenta para la evaluación de riesgos. Por otro lado, los resultados obtenidos se muestran en un contexto general debido a que el caso práctico cuenta con acuerdos de confidencialidad acerca de la información y los equipos tecnológicos que se utilizan.

Lo anterior, ha llevado a que el análisis de riesgos se enfoque únicamente en los dominios de seguridad de Disponibilidad, Integridad y Confidencialidad de la información y todos los resultados de cada proceso desarrollado está enfocado en los mismos, es por ello, que la metodología muestra tres mapas de riesgos, donde se evidencia el nivel de riesgos a los que se encuentran expuestos los activos de información. En ese sentido, se ha identificado las amenazas que generan mayor impacto en los activos de información de acuerdo a los dominios de seguridad que se ha definido y el tratamiento que se dará a las mismas a través del modelo de seguridad.

Segunda etapa: Desarrollo del modelo de seguridad

Para esta etapa, el modelo de seguridad se construye a partir de los diferentes riesgos encontrados y con el apoyo de la norma ISO 27001:2013 para la propuesta de los diferentes controles. En ese sentido, el modelo de seguridad contiene el marco legal y normativo, estrategia de cumplimiento, entendimiento de la necesidad, ejecución del PHVA y el modelo de estado de madurez del sistema; así mismo, se definen los mecanismos de seguridad como los roles y perfiles, políticas y controles a los riesgos. El modelo de seguridad de la información para entornos de investigación se ha desarrollado desde un contexto general buscando abordar las amenazas con mayor impacto que fueron identificados en el análisis de riesgos, donde se han considerado los dominios de seguridad de Disponibilidad, Integridad y Confidencialidad de la información, sin embargo, en este modelo se ha considerado los dominios de **Integridad y Confidencialidad**, junto a la **privacidad** como aspecto de seguridad, para el cumplimiento del objetivo y alcance, que busca preservar la seguridad de la información. En ese sentido, su diseño y estructura esta referenciada en el Modelo de Seguridad y Privacidad propuesto por el MINTIC [25] y lo establecido en la norma ISO/IEC 27001:2013 [18]. Este modelo, cuenta con un objetivo general que define su propósito de desarrollo, la misma que ha permitido definir el alcance, estableciendo el límite de este modelo, así mismo, se cuenta con un mapa de procesos que muestra la interrelación de los procesos dentro del entorno de investigación, en ello, se especifica los procesos donde el modelo desarrollado interviene.

Este modelo de seguridad, en su estructura inicialmente cuenta con un ciclo de operación (PHVA), que cuenta con 4 fases y cada una de ellas, tiene definidas unas metas que permitirán obtener un producto específico para abordar la seguridad de la información dentro del entorno de investigación, así mismo, se ha establecido unos criterios que permitirán medir el nivel de madurez del modelo de seguridad, para que de esta manera se pueda identificar el nivel de seguridad de la información existente en el entorno de investigación.

Lo anterior, junto al código de prácticas para los controles de seguridad de la información definidos en la ISO/IEC 27002:2013 [19], se han desarrollado unos mecanismos de seguridad, como son: **1) Roles y responsabilidades**, que contiene algunos de los roles y las responsabilidades que tiene el equipo de trabajo orientado a la seguridad y privacidad de la información, **2) Controles**, para este modelo, se han adoptado los controles de la norma ISO/IEC 27001:2013, dejando de lado los controles de la Metodología MAGERIT, debido a que estos controles tienen un alcance mucho más amplio en términos de protección de la información lo que permite una gestión más amplia y adecuada de las amenazas identificadas, a diferencia de los otros controles, que son más técnicos, **3) Políticas de seguridad y privacidad**, estas fueron estructuradas en referencia de la ISO/27002:2013 y fueron desarrollados con base a los controles previamente seleccionados para preservar confidencialidad, integridad y privacidad de la información y **4) Procedimientos**, que fueron elaborados para mitigar las amenazas con mayor impacto previamente identificadas en el análisis de riesgos.

Todos los mecanismos de seguridad desarrollados están definidos como anexos y soportarán al modelo de seguridad en el cumplimiento de su objetivo y alcance, durante la generación, procesamiento, almacenamiento y compartición de datos de investigación.

Tercera etapa: Desarrollo de un prototipo de sistema para el almacenamiento y compartición seguro de datos

Para esta etapa, el prototipo fue desarrollado en el lenguaje PHP v7.2.18, utilizando la herramienta NetBeans IDE V11.1 como editor de código y una base de datos NoSQL creada en el motor MongoDB Community Server v4.2.1.Para la implementación, se ha utilizado una Workstation dentro de las instalaciones del laboratorio de Máquinas Inteligentes y Reconocimiento de Patrones - MIRP, la máquina cuenta con las siguientes características: sistema operativo Windows 10 pro de 64bits, procesador AMD A10-5800B X64 3.8GHz, memoria RAM de 12 GB y Disco duro SATA de 500 GB. En esta máquina se ha instalado y configurado un Servidor Web gratuito con la herramienta Apache v2.4.39, en donde se ha implementado el prototipo de almacenamiento y compartición de datos de investigación. El proceso de desarrollo del prototipo, fue desarrollado adaptando la metodología en cascada [27], a las necesidades de desarrollo del prototipo, de la cual se ha abordado solo tres de sus cinco fases; la metodología fue abordado inicialmente **definiendo los requisitos**, de los cuales son siete funcionales y dos no funcionales; como segunda fase se ha realizado el **diseño del prototipo**, esta fase parte **A)** Definiendo el diseño de la arquitectura del prototipo de alma-

cenamiento, para lo cual se han tenido en como referencia lo establecido por la norma NIST SP 800-160 vol-1 [32], que proporciona consideraciones de seguridad para el desarrollo de Sistemas Confiables y seguros, además del diseño de seguridad en la infraestructura de Google [9], que proporciona un resumen del diseño de la seguridad de la infraestructura técnica de Google; **B)** Se ha realizado el modelado y desarrollo del prototipo, donde se describe y muestran los diagramas de los principales procesos que el prototipo realiza, en el desarrollo se han tenido en cuenta la guía de desarrollo de seguridad definida por OWASP [35] y **C)** Se describe y muestra los mecanismos de seguridad implementados en el prototipo, con el propósito de abordar las principales amenazas que generan mayor impacto en entornos de investigación, y como última fase, se realizó la **implementación del prototipo**, en donde se ha preparado una maquina workstation que contiene herramientas que permiten que el prototipo funcione y opere a través de una interfaz web, las pruebas del prototipo se han desarrollado en una cuarta etapa.

Cuarta etapa: Evaluación de requerimientos y componentes de seguridad

Para esta etapa, el prototipo fue sometido al escaneo de vulnerabilidades web, utilizando la herramienta Acunetix v11.0.170951158, esta herramienta fue instalada en una segunda máquina y a través de conexión de red se ejecutó los escaneos de vulnerabilidades que ha permitido evidenciar y ajustar las fallas iniciales de desarrollo y de seguridad encontradas, para que de esta manera se haya podido mitigar las amenazas y vulnerabilidades previamente definidas. El desarrollo de ésta última etapa, se ha realizado en dos fases, en la primera fase, se ha realizado una **verificación funcional y técnica** de los requerimientos previamente definidos, esta verificación ha consistido en **A)** una inspección visual de los requisitos implementados, validando que todo lo definido se haya implementado, **B)** una prueba funcional, que ha consistido en interactuar con las funcionalidades implementadas y **C)** una revisión de los mecanismos de cifrado, utilizando un herramienta para a captura de datos en tránsito y revisando los datos almacenados directamente en la base de datos. La segunda fase, ha consistido en realizar una **prueba de seguridad** al prototipo a través de una herramienta de escaneo de vulnerabilidades web, que permite detectar posibles fallos de seguridad de desarrollo de software.
Esta etapa se ha desarrollado siguiendo lo establecido en el Anexo A.14.2.8 (Pruebas de seguridad de sistemas) y A.14.2.9 (Pruebas de aceptación de sistemas), de la ISO/IEC 27001:2013 y la ISO/IEC 27002:2013.

4. Análisis de riesgos

El análisis de riesgos es un procedimiento de seguridad que cuenta con varias etapas a seguir, para su desarrollo se utilizó la metodología MAGERIT V.3 [23], inicialmente se definió el contexto donde se desarrollará cada una de sus etapas. La Figura 4.1 muestra las etapas que se siguieron en el análisis de riesgos, partiendo con la definición del alcance que éste tendrá, con el propósito de establecer límites a las actividades a desarrollar, luego, se procedió a establecer reuniones con los investigadores, con la finalidad de identificar los activos de información dentro de un entorno de investigación, posteriormente, se realizó la valoración correspondiente, junto con la identificación de las amenazas y la identificación de las salvaguardas existentes, también, se evaluó el impacto de la materialización de las amenazas y los riesgos asociados. Durante el desarrollo de las etapas del análisis de riesgos se utilizó la herramienta técnica EAR/PILAR 7.1.10[1], que es muy utilizada en el desarrollo de análisis de riesgos y se encuentra avalada por el Portal de Administración Electrónica (PAe) del gobierno de España, esta herramienta cuenta con todo lo que establece la metodología MAGERIT y como resultado, permitió obtener un mapa de riesgos detallado de los activos de información a las que encuentran expuestos, los resultados obtenidos son tratados adecuadamente con la finalidad de cumplir con los acuerdos de confidencialidad que se adquieren en un entorno de investigación [25].

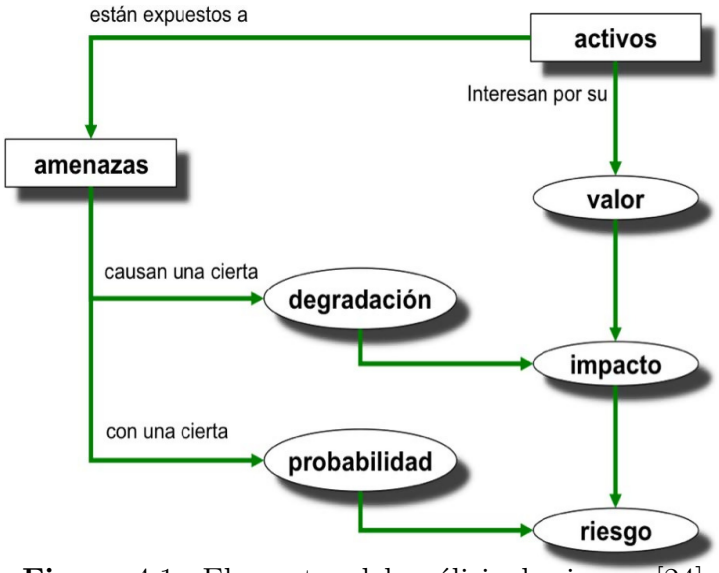


Figura 4.1.: Elementos del análisis de riesgos [24].

[1]https://www.pilar-tools.com/es/index.html

Las definiciones y la secuencia de pasos están dadas por la misma metodología MAGERIT (Figura 4.1), en consideración que la norma establece de igual manera unos pasos secuenciales para determinar los riesgos e impactos, el manual oficial indica que, "Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza"(numeral 3.1.3 Determinación del impacto potencial), así mismo define el riesgo potencial como "la medida del daño probable sobre un sistema"(numeral 3.1.4 Determinación del riesgo potencial); por lo cual, la norma establece que primero se debe abordar el impacto potencial que una amenaza puede ejercer sobre un activo y luego el riesgo que esta puede generar con base en la probabilidad de ocurrencia. En consecuencia, los pasos estipulados y ejecutados para el análisis de riesgos dada por la norma son:

- Paso 1: Activos.
- Paso 2: Amenazas.
  - Determinación del impacto potencial.
  - Determinación del riesgo potencial.
- Paso 3: Salvaguardas.
- Paso 4: Impacto residual.
- Paso 5: Riesgo residual.

Tomado de manual oficial MAGERIT[2]

4.1. Contexto

En general un proyecto de investigación se desarrolla en participación de una o más instituciones públicas o privadas, que cuentan con recursos tecnológicos y personal multidisciplinario conformando un equipo de investigadores. Para ello, se establece un entorno de trabajo donde se definen roles y responsabilidad, a fin de distribuir de forma organizada las actividades a desarrollar durante todo el ciclo del proyecto, éste, toma un liderazgo a través de un investigador principal que cuenta con el soporte administrativo de las instituciones participantes, así como también de todo el equipo de investigadores, cuya función principal es establecer las estrategias y toma de decisiones adecuadas para el cumplimiento de los objetivos planteados, por otro lado, el equipo de investigación cuenta con un coordinador por cada institución, que junto a otros investigadores multidisciplinarios, tienen asignadas actividades específicas. Dentro del equipo de investigadores, un proyecto de investigación cuenta con un equipo de soporte, que cumple con las funciones de brindar apoyo especializado en tecnologías a todos

[2]https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

los investigadores participantes, un ejemplo de una estructura de equipo de investigación se muestra en la Figura 4.2.

Dicho lo anterior, durante el desarrollo de un proyecto de investigación, se generan y comparten información técnica y científica entre los investigadores participantes, esta información, que aún se encuentra en proceso de desarrollo se clasifica como información confidencial ya que de acuerdo a la investigación, contiene información sensible y este por lo general son compartidos a través de dispositivos de almacenamiento externos, intercambios de correos electrónicos y medios de almacenamiento en la nube, entre otros. Estas prácticas en un ambiente de investigación son las más usadas y comunes, sin embargo, las medidas de seguridad para preservar la confidencialidad e integridad de toda la información generada no son las más adecuadas, estas prácticas durante el desarrollo de un proyecto de investigación representan un problema de seguridad a la información, debido a que las instituciones participantes y los responsables de los proyectos, no tienen forma de hacer seguimiento de donde se encuentra almacenada y como se viene usando toda la información que circula en un entorno de investigación.

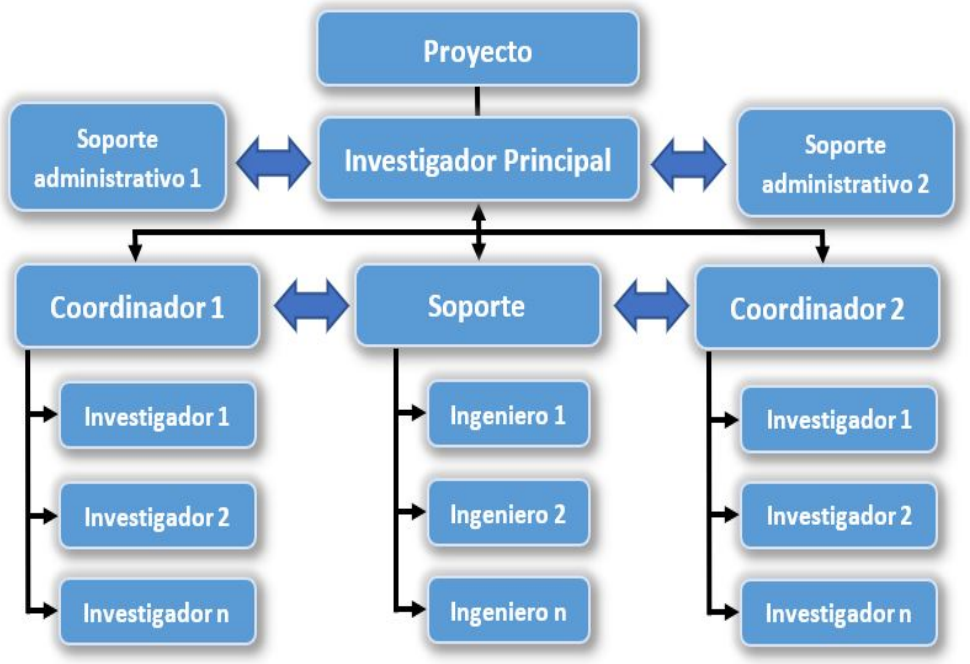


Figura 4.2.: Entorno de un proyecto de investigación multi institucional
Fuente: Elaboración propia.

4.2. Alcance

Desarrollar un análisis de riesgos informáticos a los activos de información involucrados en los procesos operativos para el desarrollo de la investigación, usando la metodología MAGERIT V.3 dentro de un entorno de investigación.

4.3. Identificación de activos de información

Dentro de un entorno de un ambiente de investigación, se cuenta con diferentes activos de información que han sido adquiridos por necesidades específicas, a través de planes de implementación o mediante la adquisición de proyectos de investigación, estos activos, son utilizados en diferentes actividades como recolección y procesamiento de datos, experimentos, entre otros.

En particular, la identificación de los activos de información está basado en un contexto general de un entorno de investigación, donde se encuentran activos de información comúnmente utilizados en este tipo de entornos, inicialmente se han establecido 5 categorías o capas (activos esenciales[B], servicios internos [IS], equipamiento [E], instalaciones [L] y personal [P]), como lo establece la metodología, luego se han identificado los activos de información de acuerdo a su categoría, a los que se le ha asignado un código de identificación, esto consiste en el código de la categoría más un número consecutivo [categoría-número consecutivo]. Con base a lo anterior, los activos de información han sido identificados y clasificados adecuadamente, así mismo se establecen diferentes vulnerabilidades para cada activo, lo que permitirá un correcto desarrollo de los procedimientos posteriores del análisis de riesgos, el resultado de este procedimiento se detalla en la Tabla A.1.

4.4. Valoración de activos de información

La valoración se ha desarrollado bajo las dimensiones de seguridad con respecto a la disponibilidad, la integridad y confidencialidad de los datos. Los valores y criterios empleados se muestran en la Tabla 2.1, estos valores son establecidos por la metodología empleada. La valoración ha permitido obtener datos que se muestran en la Tabla A.2, que son de mucha importancia ya que permiten estimar el valor funcional u operacional que supondría poder recuperar a los activos de información dentro de un entorno de investigación de una posible incidencia que afecte a los mismos.

En la asignación de los valores se han tenido en cuenta factores como el costo de reposición, el valor de la mano de obra para la reparación, el valor de las pérdidas económicas que podría ocasionar, entre otros.

4.5. Identificación de amenazas

La identificación de amenazas, parte inicialmente por identificar los tipos de amenazas existentes, la metodología empleada cuenta con un catálogo de amenazas [23] y estos se clasifican en cinco categorías (Desastres naturales, de origen industrial, errores y fallos no intencionados, ataques deliberados y riesgos sobre la privacidad).
Este procedimiento, ha surgido a partir de la identificación de las actividades funcionales, estos datos se muestran en las Tablas A.3 a A.7, donde las amenazas identificadas se muestran de forma distribuidas por activo de información y ha permitido evidenciar los riesgos a los que se encuentran expuestos y lo que le podría suceder a los activos de información en perjuicio del entorno de investigación.

4.6. Valoración de las amenazas

La valoración de las amenazas, también se ha desarrollado bajo las dimensiones de seguridad con respecto a la disponibilidad, integridad y confidencialidad de los datos. Parte del hecho de que la materialización de una amenaza no afecta a un activo a todas sus dimensiones ni en la misma forma y cuantía, es por ello, que en la valoración se ha tenido en cuenta los criterios de degradación que mide el daño y la probabilidad que estima la posibilidad de que se materialice una amenaza, estos, permiten definir el valor de una amenaza sobre los activos de información, los valores de estos criterios se detallan en las Tablas 2.2 y 2.3.
Lo anterior, ha permitido realizar una valoración de acuerdo al contexto del análisis de riesgos y los datos obtenidos se detallan en las Tablas A.8 a A.12, estos datos muestran los valores de cada amenaza identificada por activo de información y según los criterios de valoración, permite poder mostrar de manera general el riesgo al que se encuentran expuestos.

4.7. Identificación de salvaguardas

El procedimiento de identificación de salvaguardas, parte inicialmente identificando las medidas de seguridad (políticas, procedimientos, controles, etc.), existentes dentro del entorno de investigación, para ello, se ha tenido como referencia el entorno de investigación que previamente se ha definido en la introducción del presente documento. Las salvaguardas en un entorno de investigación, por lo general surgen con la necesidad de implementar recursos tecnológicos para los servicios de comunicaciones y desarrollo de actividades, en ese sentido, siempre se va contar con mecanismos o salvaguardas de seguridad como medida de protección para prever posibles daños o incidencias de seguridad hacia los activos de información.
Por lo anterior, la metodología empleada muestra un catálogo de salvaguardas [23], este documento nos sirve para identificar cual de estas salvaguardas se encuentran implementadas, con base al catálogo, la Tabla A.13, muestra las salvaguardas identificadas.

4.8. Valoración de las salvaguardas

Valorar salvaguardas es un procedimiento diferente a la valoración de activos y amenazas, ya que este, está orientado a medir la eficacia y la eficiencia de las salvaguardas existentes para los activos de información frente a los riesgos expuestos. En ese sentido, la metodología empleada establece unos criterios se muestran en la Tabla 2.4, para medir la eficacia y madurez de las salvaguardas.
Los valores asignados a cada salvaguarda corresponden al nivel de madurez en funcionalidad e implementación dentro del entorno de investigación que se ha tenido como referencia, la Tabla A.14, muestra las salvaguardas agrupadas por tipo con su respectivo valor de madurez, con esta información ya se puede tener una referencia del nivel de seguridad que tienen los activos de información frente a las amenazas existentes.

4.9. Estimación del impacto y riesgos por activo

Esta etapa del análisis de riesgos, muestra los resultados de todo el proceso realizado, producto de la correlación que la herramienta [20] realiza de forma automática, con base a toda la información suministrada. Las Tablas A.15 a A.18, muestran a detalle los valores de los impactos y riesgos acumulados y repercutidos a la que se encuentran expuesto los activos de información mostrados en la Tabla A.1, antes y después de la identificación de las salvaguardas existentes, los criterios de valoración mostrados en la Tabla 2.5 son establecidos por la metodología aplicada. Lo anterior, permite realizar un análisis independiente a través de gráficas del impacto y riesgo acumulado, ya que esta información refleja el nivel del daño y la probabilidad de ocurrencia ante la materialización de las amenazas identificadas.

4.9.1. Impacto acumulados

El impacto acumulado muestra el nivel de daño directo e indirecto que puede tener un activo de información ante la materialización de las amenazas, según las dependencias existentes en cada uno de ello, la Figura 4.3, muestra el impacto potencial acumulado (línea roja), ante la materialización de las amenazas sin ninguna medida de seguridad y el impacto acumulado con salvaguardas (línea azul), ante la materialización de las amenazas con las salvaguardas implementadas.

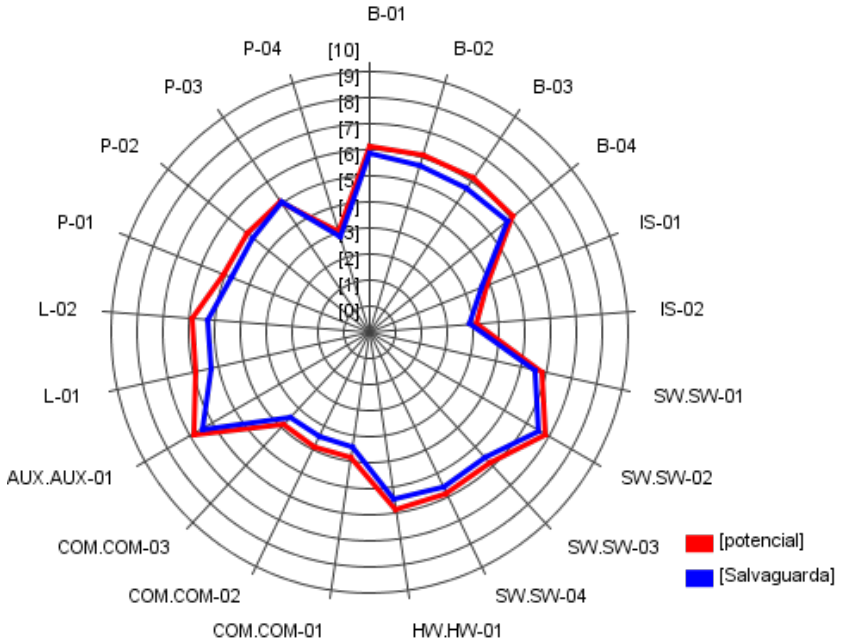


Figura 4.3.: Impacto acumulado por activo
Fuente: EAR/PILAR 7.1.10.

Un análisis general de la Figura 4.3, permite evidenciar que la materialización de las amenazas identificadas sobre los activos de información ya sea por su valor, su degradación o por su dependencia, impactan significativamente en cada uno de ellos, por lo que el daño de acuerdo a sus dominios de seguridad, son considerables, en ese sentido, la implementación de las salvaguardas, reducen mínimamente el impacto. Este margen pequeño podría interpretarse como que las salvaguardas no son del todo eficientes, esto sería debido a que no se encuentran correctamente implementadas o no se estén aplicando según como se haya establecido.

4.9.2. Riesgo acumulado

El riesgo acumulado muestra la probabilidad y el efecto directo que tienen las amenazas hacia los activos de información ante la materialización de las amenazas, los valores obtenidos permiten estimar el daño potencial a la que se encuentra expuesto un entorno de investigación, la Figura 4.4, muestra la probabilidad de riego potencial acumulado (línea roja) que tendrían los activos ante la materialización de las amenazas y el riego acumulado con salvaguardas (línea azul), muestra el nivel del riego que tendrían los activos con las salvaguardas implementadas.

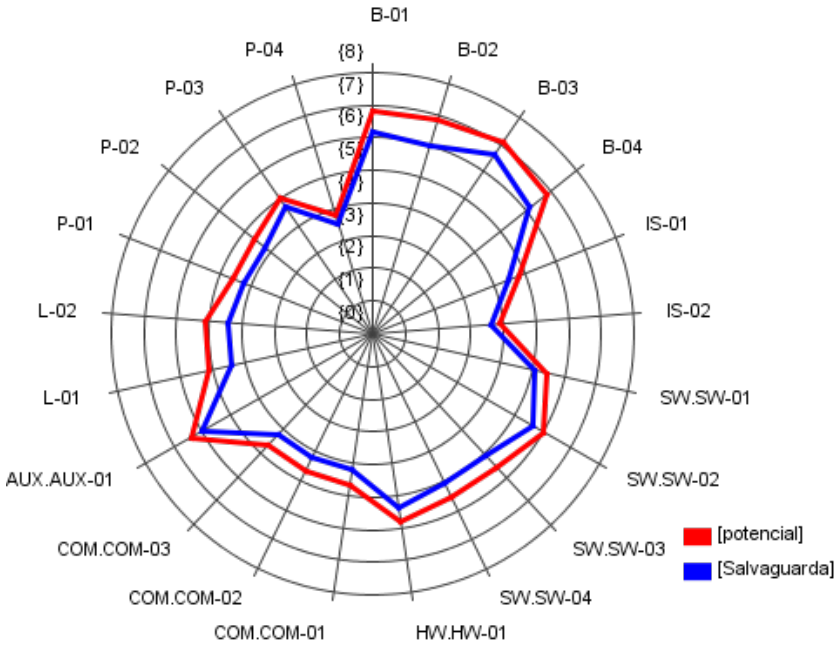


Figura 4.4.: Riesgo acumulado por activo
Fuente: EAR/PILAR 7.1.10.

Un análisis general a la Figura 4.4, permite evidenciar que la materialización de las amenazas produce un daño significativo a los activos de información y las salvaguardas existentes disminuyen mínimamente el riego de daño a la que estos activos se encuentran expuestos. La materialización de las amenazas, al no encontrarse correctamente implementados o no aplicar adecuadamente las salvaguardas de seguridad ocasionarían un daño importante, considerando los tipos de activos con los que se cuentan y las actividades que se desarrollan en estos tipos de ambientes.

4.9.3. Mapa de riesgos por dominio de seguridad.

El mapa de riesgos se encuentra seccionado por dominios de seguridad, por lo que según la escala de valores detallado en la Tabla 2.5, muestran el valor probable del efecto que pueden tener sobre los activos de información mostrados en la Tabla A.1, ante la materialización de las amenazas identificadas. Las Figuras 4.5 a 4.7, que a continuación se muestran son generados automáticamente por la herramienta [20], de acuerdo a la dependencia existente entre activos de información, con base en los resultados de la Tabla A.16.

Disponibilidad.

La figura muestra que todos los activos de información se verían afectados en su disponibilidad por lo que es preciso adoptar estrategias y medidas de control que permitan disminuir el riesgo a los que se encuentran expuestos.

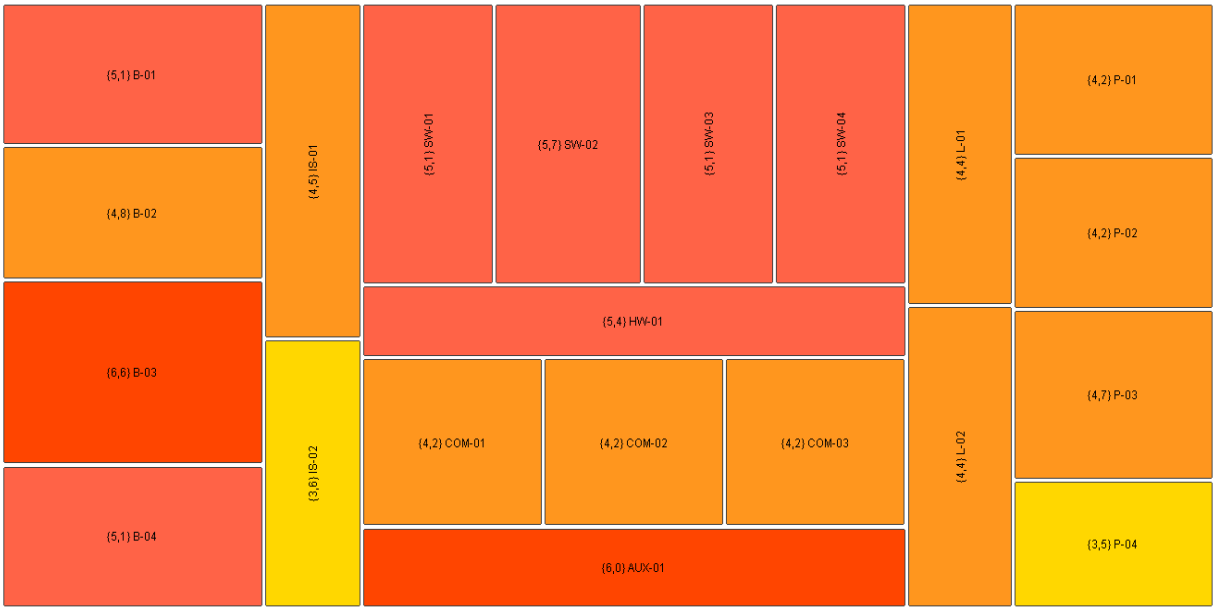


Figura 4.5.: Riesgo acumulado por dominio de Disponibilidad.
Fuente: EAR/PILAR 7.1.10.

Integridad.

La figura muestra que todos los activos de información a excepción de los activos de servicios internos [IS] y equipos de comunicación [COM], podrían verse afectados en su integridad, sin embargo, adoptar estrategias y medidas de control permitirían disminuir el riesgo a los que se encuentran expuestos.

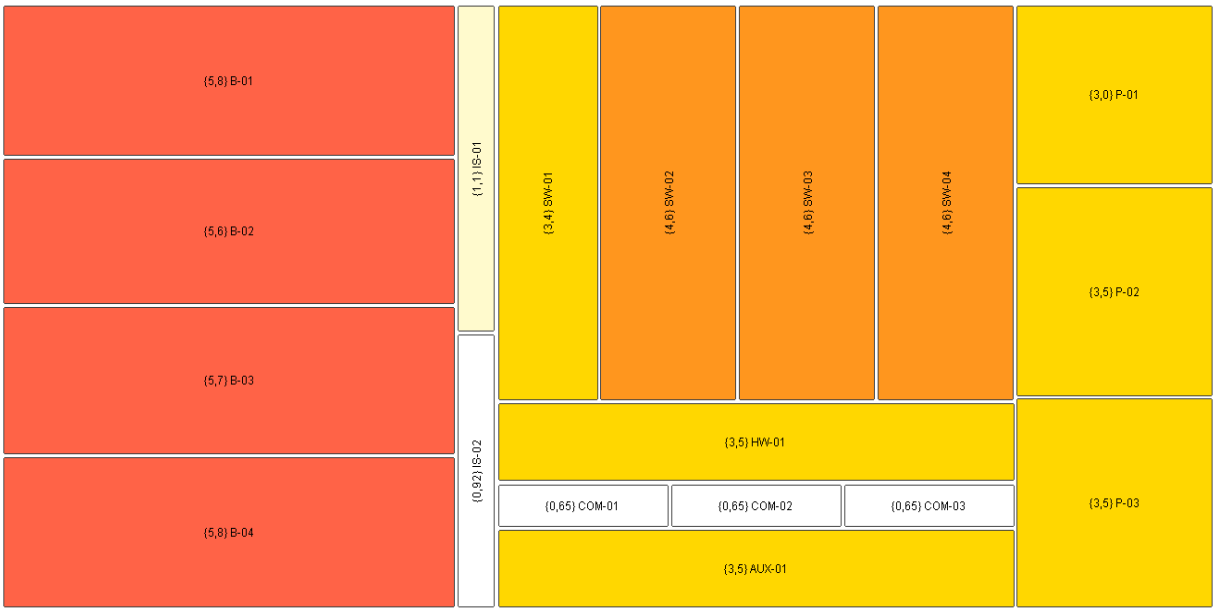


Figura 4.6.: Riesgo acumulado por dominio de Integridad.
Fuente: EAR/PILAR 7.1.10.

Confidencialidad.

La figura muestra que todos los activos de información a excepción de uno de los activos de servicios internos [IS], podrían verse afectados en su Confidencialidad, sin embargo, adoptar estrategias y medidas de control permitirían disminuir el riesgo a los que se encuentran expuestos.

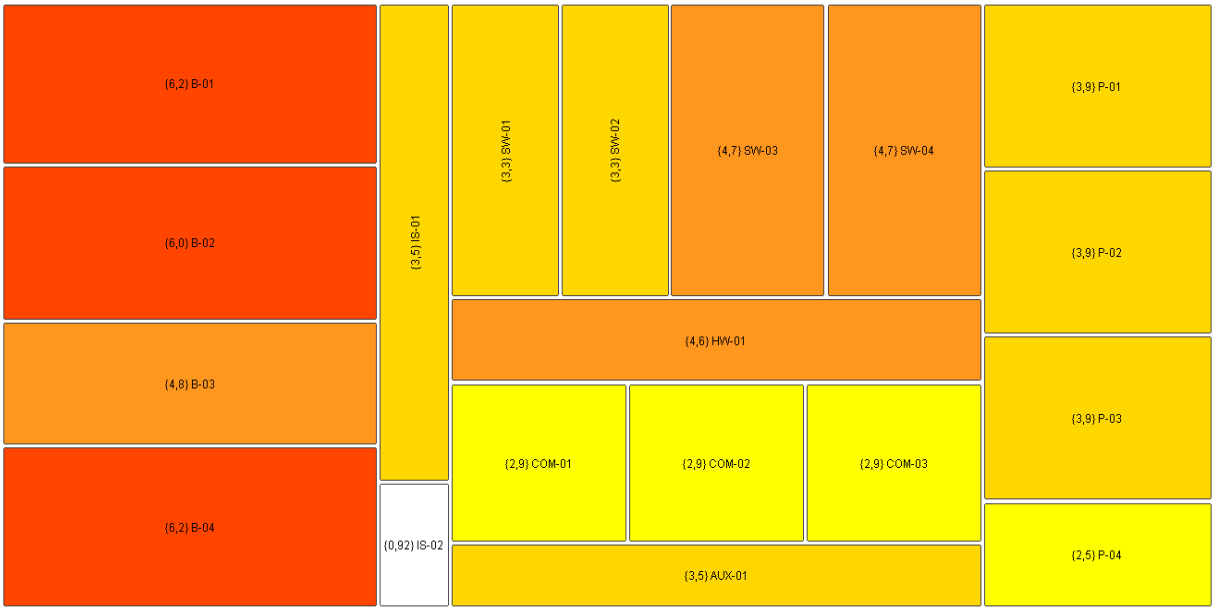


Figura 4.7.: Riesgo acumulado por dominio de Confidencialidad.
Fuente: EAR/PILAR 7.1.10.

A partir de estos resultados, se procederá a realizar una estrategia para el tratamiento de las amenazas con mayores impactos hacia los activos de información dentro de un entorno de investigación.

4.9.4. Tratamiento de amenazas.

El tratamiento al impacto de las amenazas identificadas en el análisis de riesgos, inicialmente ha consistido en identificar todas las amenazas con altos impactos de acuerdo al criterio de valoración mostrados en la Tabla 2.5 y los resultados obtenidos en el **Apartado 4.9**. En particular, se ha establecido por parte de la coordinación del proyecto y del laboratorio ITM, que el tratamiento está asociado a todas las amenazas que tengan un valor superior a 4, esto ha permitido reducir a un total de 21 amenazas potenciales. Posteriormente se ha procedido a la clasificación por tipo de amenazas y definir el tratamiento a realizar a cada una de ellas, la Tabla 4.1, muestra el accionar a cada una de estas amenazas.

Tipo	Amenazas	Tratamiento			
		Aceptar	Mitigar	Eliminar	Transferir
Ataques	[A.5] Suplantación de la identidad		**X**		
	[A.6] Abuso de privilegios de acceso		**X**		
	[A.8] Difusión de software dañino		**X**		
	[A.11] Acceso no autorizado		**X**		
	[A.15] Modificación de la información		**X**		
	[A.22] Manipulación de programas		**X**		
	[A.24] Denegación de servicio				**X**
	[A.25] Robo de equipos				**X**
	[A.29] Extorsión				**X**
Errores y fallos no intencionados	[E.15] Alteración de la información		**X**		
	[E.18] Destrucción de la información		**X**		
	[E.19] Fugas de información				**X**
Desastres industriales	[I.*] Desastres industriales				**X**
	[I.1] Fuego				**X**
	[I.2] Daños por agua				**X**
	[I.5] Avería de origen físico o lógico				**X**
	[I.6] Corte del suministro eléctrico				**X**
	[I.7] Condiciones inadecuadas de temperatura o humedad				**X**
	[I.11] Emanaciones electromagnéticas				**X**
Desastres naturales	[N.1] Fuego				**X**
	[N.2] Daños por agua				**X**

Tabla 4.1.: Tratamiento de las amenazas.

El proceso de análisis de riesgos ha permitido identificar y evaluar el nivel de riesgo a la que un entorno de investigación se encuentra expuesto, incluyendo la eficiencia y eficacia de las salvaguardas identificadas, estos resultados han permitido establecer el tratamiento de amenazas con mayores impactos en lo activos de información.

Toda la información obtenida es fundamental para el desarrollo del siguiente capítulo que consistirá en desarrollar un modelo de seguridad de la información para un entorno de investigación. mediante el desarrollo de políticas, procedimientos y controles de seguridad se espera mitigar el impacto de los riesgos más altos a los que se encuentran expuestos los entornos de investigación y en el mejor de los casos poder eliminar algunos de ellos.

5. Modelo de seguridad de la información para entornos de investigación

En un entorno de investigación se desarrollan múltiples actividades de proyectos de investigación, los mismos que muchas veces adquieren compromisos legales de privacidad y confidencialidad de la información, es por ello, que la seguridad de la información que se genera, procesa o almacena deben estar resguardadas con mecanismos de seguridad que permitan salvaguardar la privacidad, integridad y confidencialidad de la información. En ese sentido, durante el desarrollo de las actividades propias del personal de un entorno de investigación, se generan algunas amenazas que ponen en riesgo la seguridad de la información, esto se reflejan en los resultados del análisis de riesgos mostrados en el **Apartado 4.9**, estas en muchos casos surgen debido a que el personal no siempre es consciente o no tiene la cultura de la seguridad de la información. Lo anterior, ha permitido desarrollar el presente modelo de seguridad de la información, que busca mitigar las principales amenazas de seguridad de acuerdo al tratamiento de amenazas definido en la **Tabla 4.1**, para ello, el modelo cuenta con un conjunto de mecanismos que permitirán preservar la seguridad y privacidad de la información.

5.1. Marco legal

- **Ley Estatutaria 1581 de 2012 Régimen de Protección de Datos Personales:** Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma[1].

- **Ley Estatutaria 1266 de 2008 Habeas Data:** Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás

[1] http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política[2].

- **Constitución Política de Colombia, Artículos 15 y 20:** Art. 15: Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Art. 20: Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación[3].

- **Ley 1273 de 2009**, Ley de delitos informáticos, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones[4].

- **Decreto 1377 de 2013**, Por la cual se reglamenta la Ley 1581 de 2012[5].

- **Decreto 1074 del 26 de mayo de 2015**, "Por medio del cual se expide el Decreto Único Reglamentario Del Sector Comercio, Industria y Turismo"[6].

- **Sentencia C-748/11**, "Por la cual se dictan disposiciones generales para la protección de datos personales"[7].

- **CONPES 3854**, política nacional de seguridad digital, Incluye componentes como la gobernanza, la educación, la regulación, la cooperación internacional y nacional, la investigación y desarrollo, y la innovación[8].

- **CONPES 3701**, lineamientos de política para ciberseguridad y ciberdefensa, para contrarrestar las amenazas cibernéticas en el entorno digital[9].

[2]http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html
[3]http://www.secretariasenado.gov.co/index.php/constitucion-politica
[4]http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html
[5]https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf
[6]https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=76608
[7]http://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm
[8]https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3854.pdf
[9]https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

5.2. Estándares

- **Norma ISO 27001:2013**, Sistemas de gestión de seguridad de la información, esta norma internacional se ha preparado para proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información [18].
- **Norma ISO 27002:2013**, Código de prácticas para los controles de seguridad de la información, esta Norma Internacional está diseñado para que las organizaciones utilizan como referencia para la selección de los controles en el proceso de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO / IEC 27001 [19].
- **MAGERIT v.3:** Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, elaborada por el antiguo Consejo Superior de Administración Electrónica (actualmente Comisión de Estrategia TIC), como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión[10].

5.3. Definiciones

- **Activo de información:** Es el elemento que contiene información física, digital y de conocimiento adquirido necesarios para el cumplimiento de los objetivos planteados por el entorno de investigación [24].
- **Acuerdo de confidencialidad:** Contrato en la cual los investigadores y terceros, se comprometen a no revelar información a la que tengan acceso, fuera del entorno de investigación [15].
- **Amenaza:** Es la materialización del riesgo, mediante una fuente de daño potencial [24].
- **Autenticación:** Procedimiento de comprobación de identidad y credenciales de acceso a un ambiente o sistema de información [17].
- **Impacto:** Efectos ocasionado proveniente de la materialización de una amenaza [24].
- **Probabilidad:** Medida para estimar la materialización de una amenaza [24].
- **Riesgo:** Probabilidad de que se materialice una amenaza pudiendo causar daños o perjuicios a los activos de información [24].

[10] https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.

- **Vulnerabilidad:** Es toda debilidad en la seguridad de la información que potencialmente puede ser aprovechada por una amenaza [24].

- **Terceros.** Persona u organización ajena a los procesos propios de un entorno de investigación, esto incluye sin limitarse, proveedores, clientes, entes de control, entre otros.

5.4. Objetivo general

Desarrollar un Modelo de Seguridad de la Información para entornos de investigación, dirigido a proteger los activos de información, desde un enfoque de la prevención y mitigación del riesgo; en cumplimiento de la legislación colombiana, las políticas y procedimientos establecidos a partir de los resultados obtenidos de un previo análisis de riesgos informáticos.

5.5. Alcance

El modelo de seguridad se encuentra orientado en preservar la confidencialidad, integridad y privacidad de la información en los procesos operativos para el desarrollo de la investigación, basado en las amenazas con mayor impacto identificados en el análisis de riesgos.

5.6. Cumplimiento

Este documento es aplicable para todos los niveles de un entorno de investigación y a sus procesos vinculados. Por tal razón, debe ser conocido, aceptado y cumplido en su totalidad por el personal y terceros que tengan acceso, almacenen, conozcan, procesen o difundan información de propiedad del mismo.

5.7. Mapa de procesos de un entorno de investigación

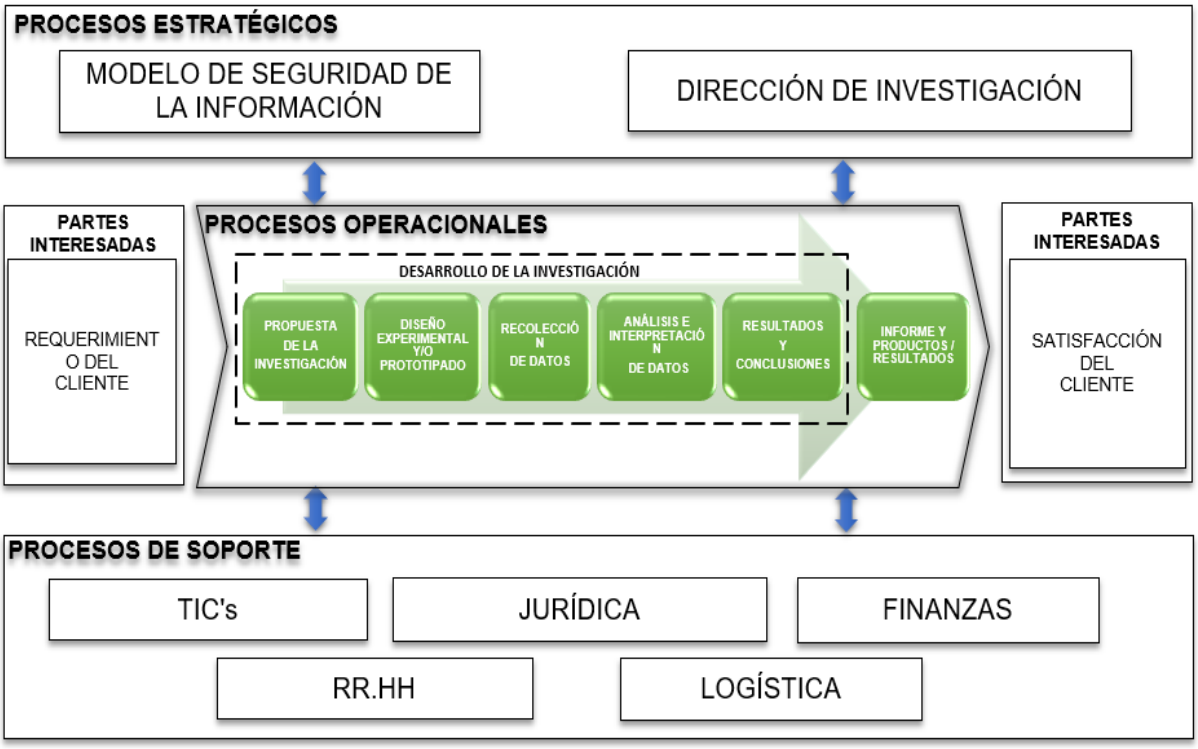


Figura 5.1.: Mapa de procesos de una entorno de investigación.
Fuente: Elaboración propia.

5.8. Ciclo de operación

El modelo de seguridad, se ha diseñado y basado en los riesgos, amenazas e impactos identificados en el análisis de riesgos desarrollado en el **Capítulo 4**, con base a los resultados obtenidos. La Figura 5.2, muestra el ciclo de operaciones que contienen metas que se deben desarrollar para la prevención y mitigación de los riesgos e impactos de las amenazas identificadas dentro de un entorno de investigación.

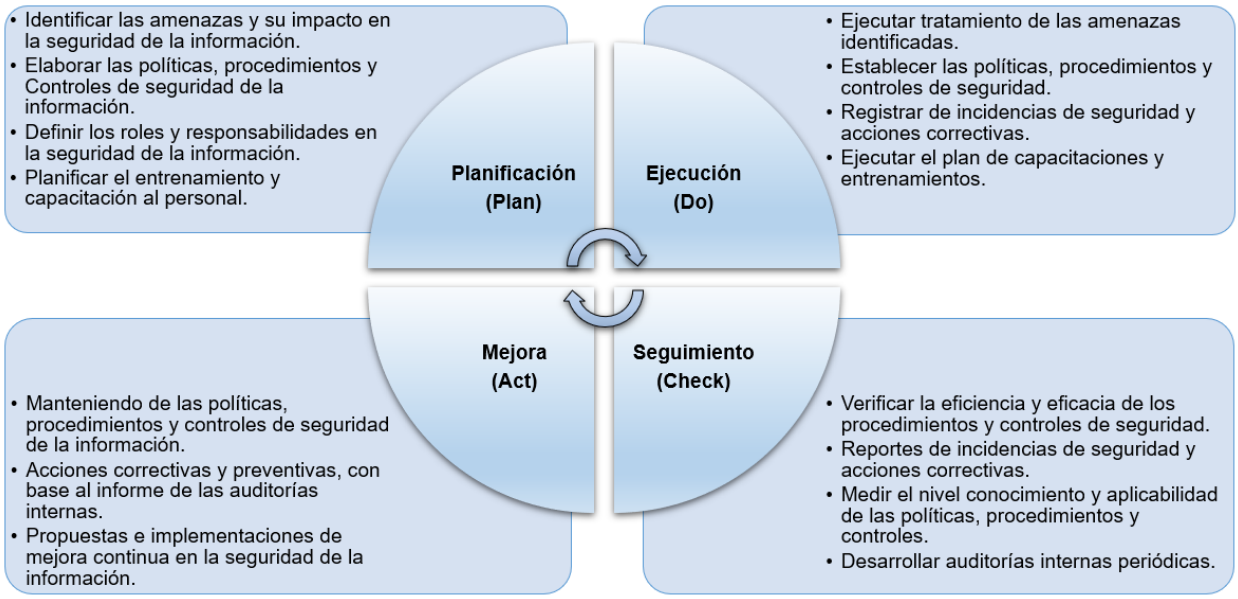


Figura 5.2.: Ciclo de operación.
Fuente: Elaboración propia.

Cada uno de las fases y metas establecidas en este ciclo de operación, son definidas en un contexto general, esto servirá como base para el cumplimiento del objetivo y alcance del modelo de seguridad.

5.8.1. Fase de Planificación (Plan)

Esta fase contiene las metas que deberán diseñarse y servirán como base y soporte en el cumplimiento de la seguridad de la información dentro de un entorno de investigación.

Item	Metas	Producto
1	Identificar las amenazas y su impacto en la seguridad de la información.	Tratamiento del nivel de riesgos acumulados
2	Elaborar las políticas de seguridad y privacidad de la información	Documento de políticas de seguridad y privacidad de la información aprobada por la alta dirección.
3	Elaborar los procedimientos y controles de seguridad de la información	Documento de procedimiento y controles de seguridad de la información aprobada por la alta dirección.
4	Definir roles y responsabilidades en la seguridad de la información	Equipo responsable de la seguridad de la información.
5	Planificar el entrenamiento y capacitación al personal.	Plan de entrenamiento y capacitaciones al personal aprobada por la alta dirección.

Tabla 5.1.: Metas y productos de la fase de planificación.

Identificar las amenazas y su impacto en la seguridad de la información.

La identificación de las amenazas y su impacto deben ser obtenidos a través del desarrollo de un análisis de riesgo, para ello se debe de establecer una metodología que se encuentre alineada a la norma ISO/IEC 27001.
El desarrollo del análisis de riesgos deberá contar con la autorización y respaldo de la alta dirección en brindar todas las facilidades en la recolección de información, ya que esto es esencial para la toma de decisiones en la seguridad y privacidad de la información.
En particular, el análisis de riesgos se ha desarrollado en el **Capítulo 4**, en donde los resultados obtenidos, es esencial para establecer los lineamientos y estructurar el presente modelo de seguridad.

Elaborar las políticas de seguridad y privacidad de la información.

Se debe definir la política de seguridad y privacidad de la información en un documento formal, donde se exprese la intención de la alta dirección en respaldar el modelo de seguridad de la información. El documento deberá contener una política de carácter general y las políticas específicas de seguridad de la información.
Este documento deberá ser revisado, modificado según necesidad, aprobada y respaldada por la alta dirección.

Elaborar los procedimientos y controles de seguridad de la información.

Se deben elaborar los documentos de procedimientos y controles de seguridad, en su contenido deberá especificar las acciones a efectuar y las medidas que se deben tomar para resguardar la seguridad y privacidad de la información. Los documentos deberán tener objetivos, indicadores de medición y plazos definidos que permitan evaluar el grado o nivel de cumplimiento, la eficiencia y la eficacia de las mismas.
Este documento deberá ser revisado, modificado según necesidad y aprobada por la alta dirección.

Planificar el entrenamiento y capacitación al personal.

Se debe desarrollar un plan de trabajo anual basados en los antecedentes de seguridad, problemáticas vigentes y proyecciones en tendencias e innovaciones tecnológicas en la seguridad y privacidad de la información.
Este documento deberá ser revisada, modificada según necesidad, aprobada y respaldada por la alta dirección, mediante la asignación de los recursos e insumos necesarios para la ejecución y cumplimiento del cronograma establecido.

5.8.2. Fase de Ejecución (Do)

Esta fase contiene las metas que permitirá al entorno de investigación poder ejecutar las metas establecidas en la fase de planificación.

Item	Metas	Producto
1	Ejecutar tratamiento de las amenazas identificadas.	Registro de implementación de controles el tratamiento de amenazas identificadas.
2	Establecer las políticas, procedimientos y controles de seguridad.	Ejecución y difusión al personal del entorno de investigación las políticas, procedimientos y controles de seguridad y privacidad de la información.
3	Registro de incidencias de seguridad y acciones correctivas.	Reporte de incidencias de seguridad
4	Ejecutar el plan de capacitaciones y entrenamiento.	Registro de asistencia a los entrenamientos y capacitaciones.

Tabla 5.2.: Metas y productos de la fase de implementación.

Ejecutar tratamiento de las amenazas identificadas.

Se debe de definir que tratamiento se debe realizar sobre las amenazas identificadas, esto quiere decir que se deberá decidir si se debe aceptar, mitigar, eliminar o transferir los riesgos de la posible materialización de cada amenaza identificada, sin embargo, se deberá dar

prioridad el tratamiento de las amenazas que como resultado del análisis de riesgos tengan mayor impacto.
Las acciones a ejecutar en esta meta, deberá estar dirigida por el responsable de la seguridad y privacidad de la información, así mismo deberá tener el respaldo de la alta dirección.

Establecer las políticas, procedimientos y controles de seguridad.

Se debe de ejecutar las políticas, los procedimientos e implementar los controles que permitan mitigar los riesgos e impactos de materialización de las amenazas identificadas en el análisis de riesgos y otros que puedan surgir en el tiempo, así mismo, se deberá hacer la difusión adecuada de la documentación correspondiente sobre las mismas.
Esta meta debe estar dirigida y supervisada por el responsable a cargo de la seguridad y privacidad de la información.

Registro de incidencias de seguridad y acciones correctivas.

Se debe diseñar el formato físico o digital y documentar todas las incidencias de seguridad, así como también las acciones correctivas aplicadas, con el propósito de generar un reporte de incidencias de seguridad.
Esta meta debe ser supervisada por el responsable a cargo de la seguridad y privacidad de la información.

Ejecutar el plan de capacitaciones y entrenamiento.

Para el cumplimiento de esta meta, deberá partir definiendo los perfiles del personal que deberá asistir a las capacitaciones o entrenamientos y luego se deberá definir donde se desarrollará el plan, si es dentro o fuera de las instalaciones. En el caso que:

- Si el plan será ejecutado por el personal del entorno de investigación, se deberán adoptar una metodología, elaborar el material adecuado, se diseñarán las estrategias y se asignarán los recursos necesarios para el desarrollo y cumplimiento del plan.
- Si el plan será desarrollado por personal o entidad externa, se deberán gestionar oportunamente la asignación de los recursos necesarios para el personal designado a asistir obligatoriamente a las capacitaciones y entrenamientos aprobados.

Esta meta deberá ser diseñada y desarrollada por el responsable designado por la alta dirección en coordinación con el responsable a cargo de la seguridad y privacidad de la información.

5.8.3. Fase de Seguimiento (Check)

Esta fase contiene las metas que permitirá a los responsables de la seguridad de la información del entorno de investigación, hacer seguimientos a las metas establecidas en la fase de ejecución.

Item	Metas	Producto
1	Verificar la eficiencia y eficacia de los procedimientos y controles de seguridad.	Informe y registro de eficiencia y eficacia
2	Reportes de incidencias de seguridad y acciones correctivas.	Informes mensuales y registros de incidencias de seguridad y acciones correctivas
3	Medir el nivel de conocimiento y aplicabilidad de las políticas, procedimientos y controles.	Encuestas de conocimiento y aplicabilidad
4	Auditorías internas.	Informe de observaciones y no conformidades.

Tabla 5.3.: Metas y productos de la fase de verificación.

Verificar la eficiencia y eficacia de los procedimientos y controles de seguridad.

Se debe de desarrollar y ejecutar un protocolo de pruebas de eficiencia y eficacia de los procedimientos y controles establecidos para la seguridad y privacidad de la información, estos pueden ser o no ser programados. Los resultados deberán ser revisados con base a lo establecido en la documentación establecida por la alta dirección, de ser necesario los procedimientos y controles deberán ser modificados y ajustados hasta alcanzar el cumplimiento del nivel de seguridad establecido.

Esta meta deberá estar a cargo del responsable de seguridad y privacidad de la información y los ajustes deberán ser revisados y aprobados por la alta dirección.

Reportes de incidencias de seguridad y acciones correctivas.

Se debe de desarrollar reportes periódicos sobre las incidencias de seguridad ocurridas y sobre las acciones correctivas empleadas, que permitan generar un historial y trazabilidad acerca de la seguridad y privacidad de la información del entorno de investigación.

Esta meta deberá estar a cargo del responsable de seguridad y privacidad de la información y deberá ser presentada a la alta dirección.

Medir el nivel conocimiento y aplicabilidad de las políticas, procedimientos y controles.

Se deben de desarrollar entrevistas y encuestas dirigida e inopinadas a todo el personal del entorno de investigación, los resultados deberán manejarse con la adecuada confidencialidad y privacidad evitando cualquier conflicto de intereses.

Esta meta deberá estar a cargo de un responsable establecido por la alta dirección.

Auditorías internas periódicas.

La alta dirección deberá de coordinar con el área especializada o personal competente, la ejecución periódica de auditorías internas a todos los procesos que enmarca la seguridad y privacidad de la información.
Esta meta deberá tener como resultado un informe específico del estado de la seguridad y privacidad de la información junto a las recomendaciones, observaciones e inconformidades que podrían surgir del proceso de auditoría.

5.8.4. Fase de Mejora (Act)

Esta fase contiene las metas que permitirá a los responsables de la seguridad de la información del entorno de investigación, poder tomar medidas que permitan la mejora continua en la seguridad de la información basado en la información obtenida en la fase de verificación.

Item	Metas	Producto
1	Manteniendo de las políticas, procedimientos y controles de seguridad de la información.	Versión actualizada de las políticas, procedimientos y controles de seguridad de la información, aprobada por la alta dirección.
2	Acciones correctivas y preventivas, con base al informe de las auditorías internas.	Informe de acciones correctivas
3	Propuestas e implementación de mejora continua en la seguridad de la información.	Proyectos de mejoras en la seguridad de la información e informes de nuevas implementaciones.

Tabla 5.4.: Metas y productos de la fase de mejora.

Manteniendo de las políticas, procedimientos y controles de seguridad de la información.

Se debe de establecer un proceso de control de documentos, que de acuerdo a la necesidad y con base a los resultados de la fase de seguimiento, permita realizar actualizaciones, modificaciones de los documentos y formatos de las políticas, procedimientos y controles de seguridad de la información.
Esta meta deberá ser desarrollada por el responsable a cargo de la seguridad y privacidad de la información, junto a otros que la alta dirección considere conveniente. Posteriormente todas las modificaciones o actualizaciones, deberán ser revisadas, aprobadas y respaldadas por la alta dirección.

Acciones correctivas y preventivas, con base al informe de las auditorías internas.

Se deberán de aplicar todas las recomendaciones, levantar todas las observaciones y no conformidades, realizadas producto de las auditorías desarrolladas a través del informe de auditoría, para ello se deberá coordinar con el área responsable de la auditoría y definir un tiempo acorde a las necesidades que permita cumplir con lo establecido en el informe de auditoría.
Esta meta deberá ser dirigida por el responsable de la seguridad y privacidad de la información.

Propuestas e implementación de mejora continua en la seguridad de la información.

Como meta final del ciclo de operación del modelo de seguridad, todo el personal involucrado con los procesos de seguridad y privacidad de la información podrán proponer proyectos, mejoras e innovaciones tecnológicas que permitan mejorar la seguridad y privacidad de la información dentro del entorno de investigación.
Esta meta deberá ser revisada por el responsable de la seguridad y privacidad de la información y la alta dirección a fin de evaluar la viabilidad y las necesidades.

5.9. Madurez del modelo de seguridad

Este modelo permitirá al entorno de investigación identificar cual es su nivel de madurez con respecto a la seguridad y privacidad de la información desde un nivel inicial hasta un nivel óptimo, en la Figura 5.3 se detalla en que consiste cada nivel de este modelo de madurez.

Figura 5.3.: Madurez del modelo de seguridad.
Fuente: Adaptada de MINTIC [25].

Cada nivel de madurez, establece unos criterios que ayudaran a determinar el estado de la seguridad y privacidad de la información en la que se encuentra el entorno de investigación:

Nivel 0 / Inexistente

- Existen controles de seguridad físicos y de infraestructuras tecnológicas que no se encuentran alineados al modelo de seguridad.
- No reconocen a la información como un activo esencial para los propósitos del entorno de investigación.
- No existe conciencia de la importancia de la seguridad y privacidad de la información dentro del entorno de investigación.

Nivel 1 / Inicial

- Tienen identificado los problemas de seguridad y privacidad de la información.
- Las incidencias de seguridad y privacidad son tratadas solo cuando se materializan.
- Existe la necesidad de implementar mecanismos de seguridad y privacidad de la información.

Nivel 2 / Repetible

- Pueden identificar y reconocer de forma general los activos de información.
- Los activos de información son clasificados según su tipo.
- Existe conciencia de seguridad sobre la información y servicios abiertos al público.
- Los temas concernientes a la seguridad y privacidad de la información son vistos en las reuniones de la alta dirección.
- El entorno de investigación cuenta con un plan de trabajo para la seguridad y privacidad de la información.

Nivel 3 / Proceso definido

- El entorno de investigación cuenta con un diagnóstico de un análisis de riesgos informáticos.
- Se definen los objetivos y el alcance de la seguridad y privacidad de la información.
- La alta dirección y su equipo de trabajo, definen, aprueban y difunden las políticas de seguridad y privacidad de la información.
- La alta dirección y su equipo de trabajo, definen y aprueban los procedimientos y controles de seguridad y privacidad de la información.

- Se han definido y asignados los roles y responsabilidades en materia de la seguridad y privacidad de la información
- Cuentan con un inventario detallado de los activos de información obtenidos mediante la aplicación de una metodología.
- Adoptan una metodología para el tratamiento de los riesgos de la seguridad y privacidad de la información.
- Tienen establecido un plan de tratamiento de riesgos y amenazas de la seguridad y privacidad de la información.

Nivel 4 / Gestionado

- Se monitoriza periódicamente el uso de los activos de información del entorno de investigación.
- Se establecen indicadores para medir el cumplimiento de las políticas procedimientos y controles de seguridad y privacidad de la información.
- Se evalúa la eficiencia y eficacia de los procedimientos y controles de seguridad y privacidad de la información.
- Se toman las medidas necesarias para prevenir y mitigar las incidencias de seguridad y privacidad de la información.

Nivel 5 / optimizado

- El modelo de seguridad cumple con su objetivo y alcance establecido.
- Las auditorías corroboran la correcta aplicación del modelo de seguridad.
- El modelo de seguridad aporta valor agregado a la misión y visión del entorno de investigación.
- Los indicadores de eficiencia y eficacia son usados para buscar la mejora continua mediante proyectos y mejoras de innovación tecnológica.

5.10. Mecanismos de seguridad

Los mecanismos de seguridad desarrollados, son un soporte importante para el modelo de seguridad, en este, se han definido roles y responsabilidades, controles, políticas y procedimientos de seguridad de la información que permitirán abordar las amenazas con mayor impacto anteriormente identificadas.

Cada uno de estos, han sido elaborados en un contexto general buscando preservar la seguridad de la información y su contenido permitirá a cualquier entorno de investigación poder adoptarlo ya que está soportado por la norma ISO/IEC 27001:2013 y los controles de seguridad de la información establecidos en su Anexo A.

5.10.1. Roles y responsabilidades

El desarrollo y cumplimiento de las metas establecidas en cada una de las fases del modelo de seguridad, depende de que cada una de ellas tenga un responsable que se asegure y responda por el cumplimiento de lo establecido, es por ello, que se han definido algunos roles y responsabilidades como mecanismo para abordar el objetivo del presente modelo de seguridad de la información, la misma que se encuentra detallada en el **Anexo B**.

Este mecanismo, tiene definido los roles principales de seguridad de la información, los mismos que tienen asignados responsabilidades que están definidas en contexto general que permitirán desarrollar y cumplir con las metas establecidas, buscando preservar la confidencialidad, integridad y privacidad de la información que se genera, procese o almacene dentro de cualquier entorno de investigación.

5.10.2. Controles de seguridad de la información

Los controles de seguridad de la información que soportan este modelo de seguridad, han sido seleccionados del Anexo A de la ISO 27001:2013 que cuenta con 14 dominios, 35 objetivos y 114 controles para la seguridad de la información.

En ese sentido, basado en lo establecido en el alcance de este modelo de seguridad, se han abordado **14 dominios, 30 objetivos y 60 controles** para la seguridad de la información en entornos de investigación, los mismos que se muestran en el **Anexo C**, con el propósito de preservar la confidencialidad, integridad y privacidad de la información dentro de los entornos de investigación. Estos controles seleccionados, mitigarán las amenazas detalladas en el **Apartado 4.9.4**, estas son las que tienen mayor impacto dentro de este tipo de entornos, de acuerdo al análisis de riesgos realizado; así mismo, estos controles abordarán otras amenazas existentes en este tipo de entornos que no han sido considerados debido a que su impacto es menor, como se ha podido ver en el **Apartado 4.5**. Es por ello, que los controles establecidos por la ISO 27001 se ajustan a las necesidades de este modelo de seguridad ya que permiten abordar los riesgos de la información de forma más amplia y específica. Cada uno de estos controles, abordan las amenazas desde la parte administrativa como, por ejemplo, los controles de Políticas para la seguridad de la información y Responsabilidades, entre otros, hasta la parte técnica como, por ejemplo, la Gestión de derechos de accesos privilegiados, entre otros, es por ello, que el Anexo en mención, muestra que las amenazas previamente identificadas son abordados por cada uno de los controles seleccionados.

5.10.3. Políticas generales de seguridad y privacidad de la información

Las políticas que se han diseñado, tienen un contexto general para que el entorno de investigación, pueda aplicar los controles de seguridad abordados según necesidad, dentro del desarrollo de sus actividades. Estas políticas se muestran en el **Anexo D**, donde su diseño y estructura esta referenciada a lo establecido en el Anexo A de la ISO/IEC 27001:2013 y en el Código de buenas prácticas para los controles de seguridad de la información de la ISO/IEC 27002:2013.
Estas políticas están definidas de acuerdo a lo establecido en el objetivo y alcance del presente modelo de seguridad, que buscan abordar y dar tratamiento a las amenazas con mayor impacto definidas en el **Apartado 4.9.4**.

5.10.4. Procedimientos para la seguridad de la información

Con el análisis de las amenazas, la identificación de los controles y la definición de las políticas de seguridad, se han diseñado cuatros (04) procedimientos de seguridad:

- Procedimiento para el ingreso seguro a los sistemas de información.
- Procedimiento de protección contra código malicioso
- Procedimiento de transferencia de información.
- Procedimiento de manejo de medios.

Estos procedimientos están detallados en el **Anexo E**, y se ha desarrollado basado en un contexto general para que pueda ser abordado por el entorno de investigación, con base a las amenazas que se han definido en el **Apartado 4.9.4**.
Todo el contenido del modelo se seguridad diseñado, esta orientado a abordar las amenazas existentes dentro de un Entorno de investigación y en particular, los controles, políticas y procedimientos se desarrollaron para mitigar las amenazas que tienen mayor impacto en el desarrollo de actividades de investigación y preservar la privacidad, integridad y confidencialidad de la información.

6. Prototipo de almacenamiento y compartición de datos de investigación

Preservar la confidencialidad y privacidad de los datos que se manejan en un entorno de investigación, es de vital importancia ya que estos en la mayoría de los casos son confidenciales, debido a que están vinculados a proyectos de investigación que han adquirido acuerdos de confidencialidad, por lo tanto, requieren que el almacenamiento de sus datos, se encuentren protegidos. En ese sentido, buscando abordar esas necesidades, se desarrolló un prototipo básico funcional para el almacenamiento seguro y compartición de datos multimodales que permita preservar la confidencialidad e integridad de los datos, con mecanismos que impidan que estos no puedan ser accedidos ni alterados por personas no autorizadas, así como también, preservar la privacidad de los datos, para que la información no se accedida ni divulgada.
El desarrollo de este prototipo, ha sido soportado por el modelo de seguridad definido en el **Capítulo 5**, ya que su contenido está dirigido a mitigar las principales amenazas existentes en un entorno de investigación y en particular, se han aplicados los controles de seguridad para el acceso seguro, certificados digitales y algoritmos para el cifrado de datos, así como también el registro y protección de eventos realizados, todos estos han permitido mitigar las amenazas definidas en la Apartado 4.9.4, que son las amenazas identificadas con mayor impacto en este tipo de entornos. Por otro lado, para el diseño de la arquitectura del prototipo de almacenamiento se ha tenido como referencia, el estándar NIST SP 800-160 vol. 1, el diseño general de seguridad de infraestructura de Google y la selección de la base de datos, se ha basado en la revisión de los mecanismos funcionales y de seguridad existentes en las principales bases de datos NoSQL.

6.1. Referencias de seguridad

En el desarrollo de un prototipo seguro, el diseño de una arquitectura que tenga definida los componentes de seguridad es de vital importancia para preservar la privacidad y confidencialidad de la información, es por ello, que es importante tener referencias de cómo se deben abordar los retos de seguridad, en ese sentido, en el desarrollo del prototipo de

almacenamiento y compartición de datos de investigación, se ha tenido en cuenta el diseño de una infraestructura segura propuesto por Google y las consideraciones en el desarrollo de sistemas seguros establecidos en el estándar NIST SP 800-160 Vol. 1

Descripción general del diseño de seguridad de la infraestructura de Google

Google muestra un diseño general de cómo han tienen implementado la seguridad de su infraestructura, su diseño se encuentra preparado para brindar seguridad durante la operación del ciclo de vida del procesamiento de su información, esto les ha permitido que sus servicios puedan ser implementados de forma segura y que el almacenamiento de datos sea seguro, implementando mecanismos de seguridad que le permiten resguardar la privacidad de sus clientes. Es por ello, que este diseño se tendrá como referencia para definir una arquitectura segura con funciones básicas.

NIST SP 800-160 Vol. 1

Es un estándar desarrollado por la National Institute of Standards and Technology (NIST), desde el punto de vista de la ingeniería, aborda acciones necesarias para desarrollar sistemas más defendibles recomendando métodos, prácticas y técnicas de ingeniería de seguridad en sistemas e ingeniería de software, con esto, busca abordar interrogantes en los problemas de seguridad desde la perspectiva de los requisitos y las necesidades de protección de los interesados, por lo que, estas recomendaciones se utilizan con la finalidad de que dichos requisitos y necesidades se aborden con el rigor adecuado a lo largo de todo el ciclo de vida de un sistema

6.2. Selección de base de datos

La selección de la base de datos, ha iniciado con una revisión del estado de arte, donde se identificó las brechas y retos de seguridad más relevantes, esto se puede ver más a detalle en el **Apartado 2.4**. Lo anterior, ha permitido identificar las categorías y seleccionar algunas de las bases de datos NoSQL más populares de acuerdo al ranking del portal DB-Engines [1], como son: Orientado a Documento (MongoDB, CouchDB), Orientadas a columnas (Hbase, Cassandra), clave-valor (BigTable, DynamoDB) y grafo (Neo4j, GraphDB), con esta selección, se ha realizado una revisión de la documentación técnica de cada una de ellas para la identificación de los mecanismos de seguridad con las que cuentan. La identificación de mecanismos de seguridad, se ha centrado en la Autenticación, Autorización, cifrado de datos en tránsito y en reposo, que son algunos de los mecanismos de seguridad más importantes a considerar en una base de datos.

[1] https://db-engines.com/en/ranking

Los resultados de todo el proceso de revisión e identificación, se muestra en la **Tabla F.1**, en donde se puede encontrar los diferentes mecanismos de seguridad con las que cuentan cada una de las bases de datos seleccionadas, sin embargo, muchas de estas bases de datos requieren realizar configuraciones e integrar con herramientas adicionales para alcanzar un nivel de seguridad aceptable, esto, pueden llegar a ser muy complejos y en algunos casos pueden ser muy costosos.
En ese sentido, para el desarrollo del prototipo de seguridad, se ha seleccionado la base de datos **MongoDB**, debido a que cuenta con una versión gratuita y su motor puede trabajar localmente, el mismo que tiene integrado los mecanismos de seguridad mostrados en la Tabla F.1, los cuales se adaptan a las necesidades y requerimientos del prototipo, así mismo, debido a sus características, puede integrarse con casi cualquier lenguaje de desarrollo.

6.3. Metodología de desarrollo

El proceso de desarrollo ha consistido en adoptar una metodología de desarrollo de software y con base a las necesidades de desarrollo, se ha adoptado y abordado tres procesos del **modelo en cascada**, como se muestra en la Figura 6.1, ya que se busca obtener un prototipo funcional, con un diseño específico de acuerdo al propósito, al alcance y a los requisitos definidos, en ese sentido, esta metodología al tener un modelo de desarrollo lineal, cumple con las necesidades para el desarrollo del prototipo, partiendo desde la definición básica de los requisitos, luego ejecutar el proceso de desarrollo y por último, hacer una implementación con sus respectivas pruebas de funcionamiento.

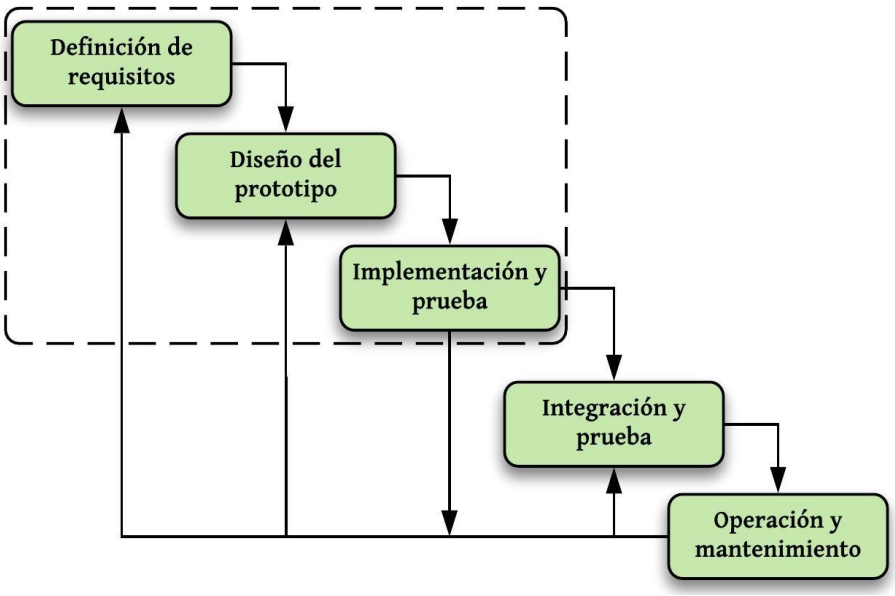


Figura 6.1.: Ciclo de vida del modelo en cascada
Fuente: Adaptada de Méndez, Gonzalo [27].

Propósito

Desarrollar un sistema prototipo para el almacenamiento y compartición segura de datos multimodales (imágenes médicas, señales, audio, video, correos electrónicos, archivos de procesador de texto, hojas de cálculo, entre otros.), que se manejan en ambientes de investigación, sobre una base de datos MongoDB, incorporando mecanismos de seguridad que permitan preservar la confidencialidad, privacidad e integridad de la información almacenada.

Alcance

Desarrollar un prototipo básico de software funcional que incorpore mecanismo de seguridad que protejan la confidencialidad, privacidad e integridad de los datos multimodales almacenados, soportado en una Base de datos de MongoDB.

6.3.1. Definición de requisitos

El desarrollo del prototipo, esta soportado, por los requisitos funcionales y no funcionales, estos, detallan todos los requisitos implementados y desarrollados. Los detalles de estos requisitos funcionales se muestran en las Tablas 6.1 a 6.7 y los no funcionales se muestran en las Tablas 6.8 y 6.9.

Requisitos funcionales

Identificación del requerimiento:	RQF-01
Nombre del requerimiento:	Arquitectura del prototipo.
Características:	El prototipo deberá de operar en un servidor local mediante una arquitectura web
Descripción del requerimiento:	El prototipo debe permitir el acceso de un usuario, desde cualquier navegador instalado en su computador
Prioridad del requerimiento:	Alta

Tabla 6.1.: Requisito funcional - 01

Identificación del requerimiento:	RQF-02
Nombre del requerimiento:	Autenticación de Usuario.
Características:	Todos los usuarios deben autenticarse y validar su identidad para el acceso al prototipo según su rol a través de una interfaz web.
Descripción del requerimiento:	1) El prototipo debe validar las credenciales ingresadas por el usuario. 2) El prototipo debe de generar un código de 2FA para validar la identidad del usuario. 3) El prototipo, debe mostrar la interfaz de acuerdo a su rol (administrador o usuario).
Prioridad del requerimiento:	Alta

Tabla 6.2.: Requisito funcional - 02

Identificación del requerimiento:	RQF-03
Nombre del Requerimiento:	Gestión de Usuarios.
Características:	Se debe gestionar las cuentas de usuarios para dar acceso según su rol y los permisos para interactuar desde la interfaz web de usuario (Frond-end).
Descripción del requerimiento:	1) El administrador debe crear una cuenta y asignar el perfil (usuario o administrador) 2) El administrador, deberá registrar los datos de la cuenta (Documento, Nombres, email, password, estado de la cuenta y su rol). 3) El administrador debe asignar los permisos a la cuenta de usuario (carga, descarga, compartir, eliminar)
Prioridad del requerimiento:	Alta

Tabla 6.3.: Requisito funcional - 03

Identificación del requerimiento:	RQF-04
Nombre del requerimiento:	Gestión de archivos.
Características:	Se debe poder cargar, descargar, eliminar o compartir un archivo con usuario interno del prototipo
Descripción del requerimiento:	1) El prototipo, debe permitir listar los archivos almacenados de un usuario. 2) El prototipo, debe permitir cargar un archivo de cualquier formato, sin alterar su integridad. 3) El prototipo, debe permitir descargar un archivo almacenado sin alterar su integridad. 4) El prototipo, debe permitir compartir un archivo y el usuario solo debe poder descargar. 5) El prototipo, debe permitir eliminar una archivo almacenado y asociado a la cuenta de un usuario
Prioridad del requerimiento:	Alta

Tabla 6.4.: Requisito funcional - 04

Identificación del requerimiento:	RQF-05
Nombre del requerimiento:	Auditoría
Características:	Se debe de registrar todas las acciones realizadas por las cuentas de usuarios.
Descripción del requerimiento:	1) El prototipo, debe de registrar todos las acciones realizadas por los usuarios. 2) El prototipo, debe permitir listar todos los registros desde la interfaz del administrador.
Prioridad del requerimiento:	Alta

Tabla 6.5.: Requisito funcional - 05

Identificación del requerimiento:	RQ-06
Nombre del requerimiento:	Cifrado de datos
Características:	Se debe cifrar los datos almacenados a almacenar, así mismo deber de cifrar los datos generados entre la interfaz web del usuario y el prototipo.
Descripción del requerimiento:	1) El prototipo, debe de realizar un cifrado de los datos en reposo mediante AES256-CBC. 2) El prototipo, debe cifrar los datos en tránsito generados entre la interfaz web del usuario y el prototipo mediante un certificado digital TSL 1.3
Prioridad del requerimiento:	Alta

Tabla 6.6.: Requisito funcional - 06

Identificación del requerimiento:	RQF-07
Nombre del requerimiento:	Base de datos MongoDB
Características:	Se debe de usar la base de datos NoSQL MongoDB, para asegurar que se pueda almacenar cualquier tipo de dato multimodal.
Descripción del requerimiento:	1) El prototipo, debe de estar conectado a la base de datos NoSQL MongoDB para que se pueda almacenar cualquier tipo de dato multimodal 2) Todos los datos almacenados, deberán estar cifrados.
Prioridad del requerimiento:	Alta

Tabla 6.7.: Requisito funcional - 07

Requisitos no funcionales

Identificación del requerimiento:	RQNF-01
Nombre del requerimiento:	Interfaz del prototipo.
Características:	El prototipo, debe de tener una interfaz de usuario sencilla para que el usuario pueda interactuar con facilidad.
Descripción del requerimiento:	El prototipo deber tener una interfaz de uso intuitivo.
Prioridad del requerimiento:	Alta

Tabla 6.8.: Requisito no funcional - 01

Identificación del requerimiento:	RQNF-02
Nombre del Requerimiento:	Mitigación de amenazas.
Características:	El prototipo, deberá preservar la confidencialidad, integridad y privacidad de los datos almacenados.
Descripción del requerimiento:	Deberá asegurarse de mitigar las amenazas previamente identificadas con los mecanismos de seguridad implementados.
Prioridad del requerimiento:	Alta

Tabla 6.9.: Requisito no funcional - 02

6.4. Diseño del prototipo

El prototipo de almacenamiento, tiene como propósito preservar la seguridad de los datos en tránsito y en reposo que se van a gestionar y almacenar dentro de este. En ese sentido, se ha diseñado una arquitectura web detallada en la Figura 6.2, donde se muestra que su diseño se encuentra dividida por módulos; inicialmente se tiene al **Browser (1)**, que es el navegador por donde el usuario previamente registrado podrá acceder e interactuar con las funcionalidades del prototipo, luego se tiene un **Web Service (2)**, que soporta y gestiona los requisitos funcionales y mecanismos de seguridad implementados, entre ellos están el control de accesos, para una autenticación y autorización segura, el cifrado y descifrado de archivos en tránsito en reposo, para que los datos no puedan ser leídos fuera del prototipo, la carga o descarga de archivos, que permite poder gestionar dicha funcionalidad de cualquier dato multimodal y luego está la auditoría, que registra todas las actividades realizadas por los usuarios, también se tiene el **Fron-end (3)**, que es la interfaz donde un usuario previamente registrado y autenticado podrá interactuar con las funcionalidades del prototipo según su rol de usuario (administrador o usuario) y por último, está la **Base de datos MongoDB (4)**, que alojará todos los datos multimodales, las cuentas de usuarios y sus perfiles, previamente cifrados por el Web Service.

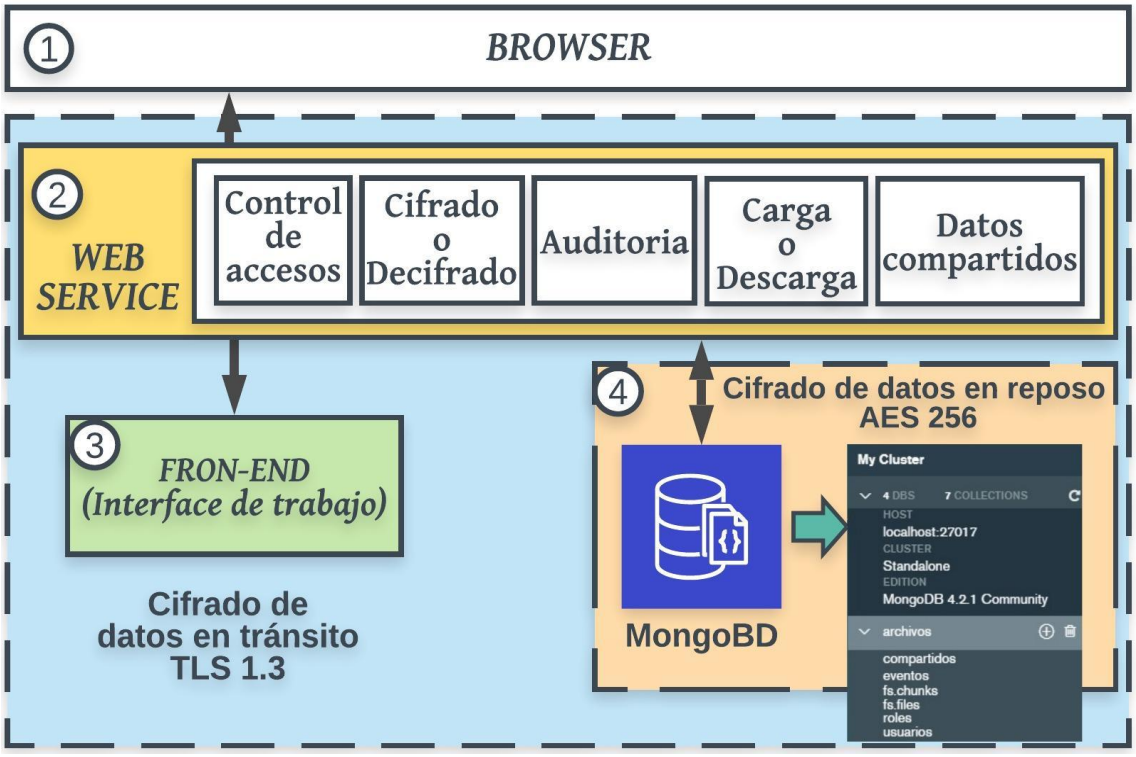


Figura 6.2.: Arquitectura del prototipo de almacenamiento seguro
Fuente: Elaboración propia

6.4.1. Modelado del prototipo

Los diagramas que se muestran en este apartado, ayudan a interpretar la operación del web service y los principales procesos del prototipo como son: el control de acceso, la carga, descarga y compartición de archivos. Estos diagramas, han servido para poder realizar el desarrollo y funcionamiento eficiente del prototipo, con base a los requisitos definidos.

Diagrama de clase: Web Service

La Figura 6.3, muestra la secuencia del proceso que el web service realiza, este es quien tiene implementado los controles de seguridad que permiten mitigar las amenazas con mayor impacto previamente definidos. La seguridad inicia desde el control de acceso donde se valida las credenciales y la autenticación del inicio de sesión, los datos en este proceso se encuentran cifrados y una vez que se haya hecho la validación, el usuario puede interactuar y hacer la gestión de archivos (carga, descarga, compartir o eliminar un dato), así como también la gestión de usuarios (crear, modificar o eliminar un usuario), según su perfil y los permisos asignados.

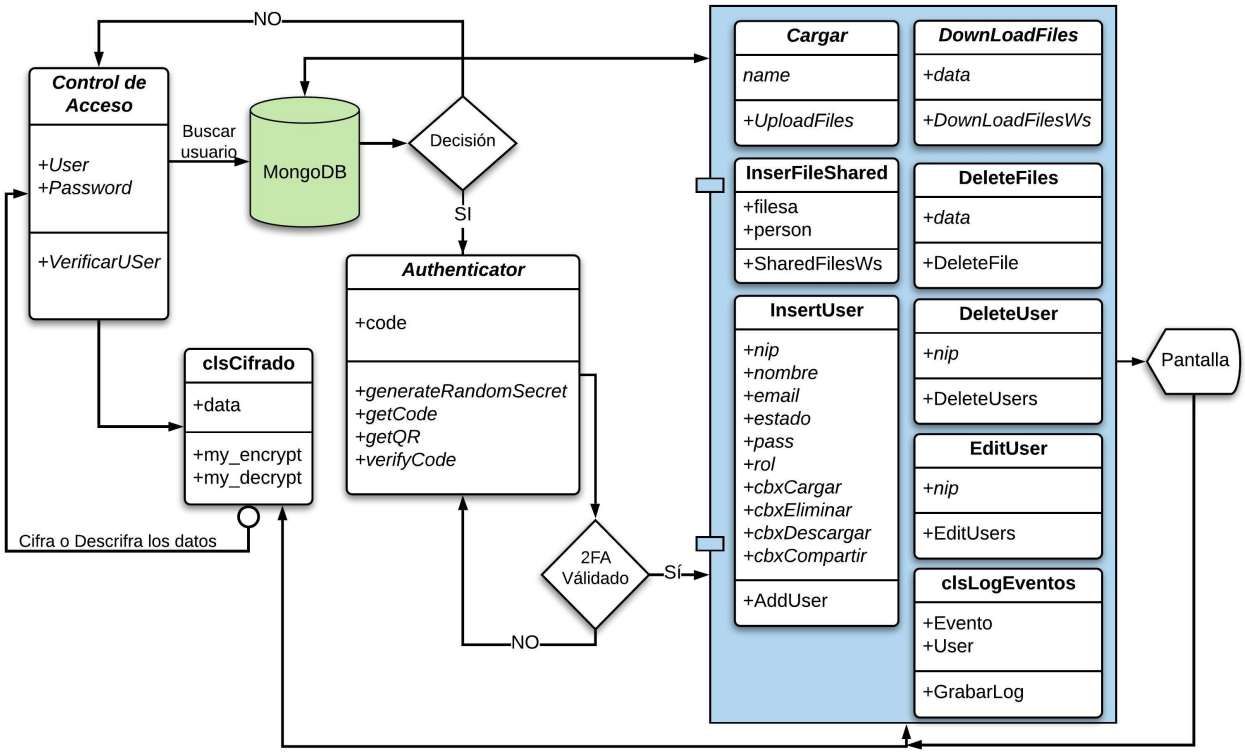


Figura 6.3.: Diagrama de clase Web Service
Fuente: Elaboración propia

Diagrama de secuencia: Control de accesos

La Figura 6.4, muestra la secuencia realizada por el prototipo para ejecutar el proceso de control de accesos, desde el momento que un usuario previamente registrado accede al dominio y carga el formulario de acceso, hasta la validación de las credenciales y el doble factor de autenticación-2FA, realizada por el web service.

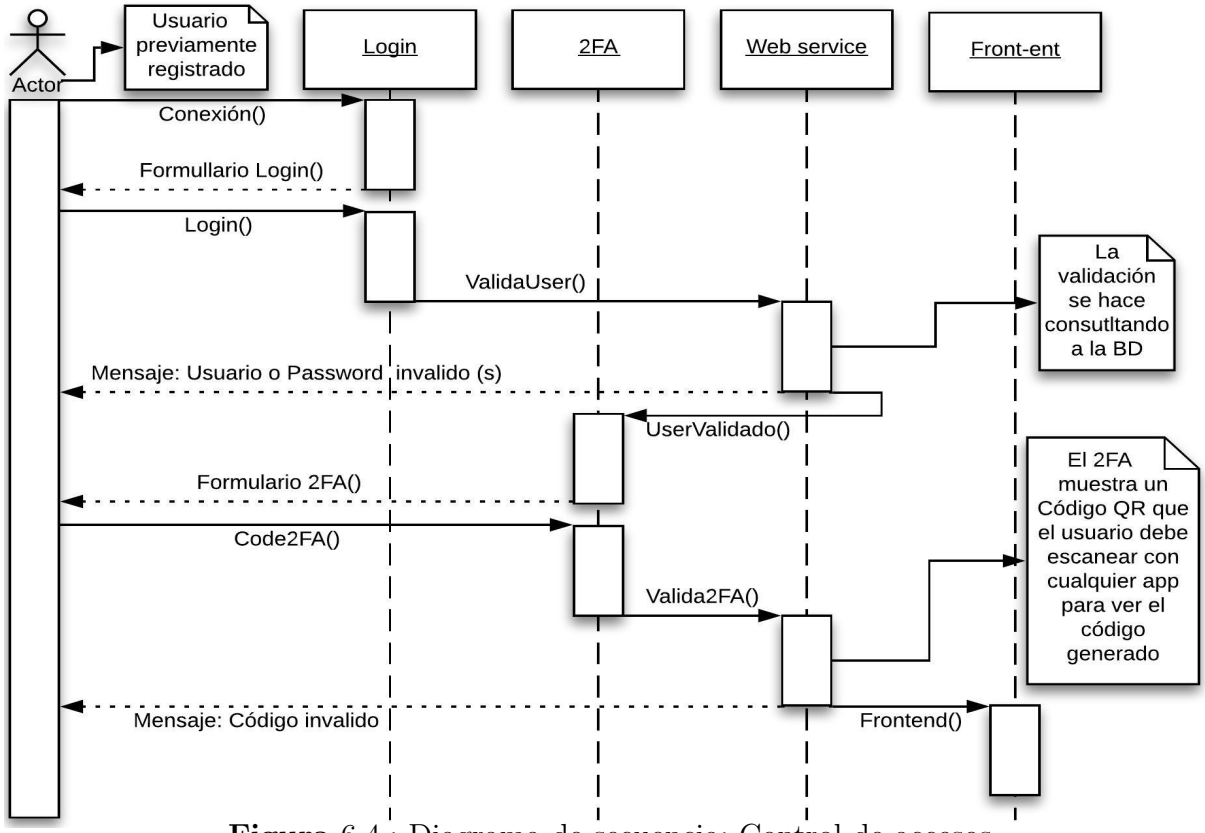


Figura 6.4.: Diagrama de secuencia: Control de accesos.
Fuente: Elaboración propia

Diagrama de secuencia: Carga de datos

La Figura 6.5, muestra la secuencia realizada por el prototipo para ejecutar el proceso de carga de datos, este proceso se puede ejecutar desde una de las opciones de la interfaz de usuario y el web service, es quien ejecuta el todo el proceso del cifrado, almacenamiento y listado de los mismo.

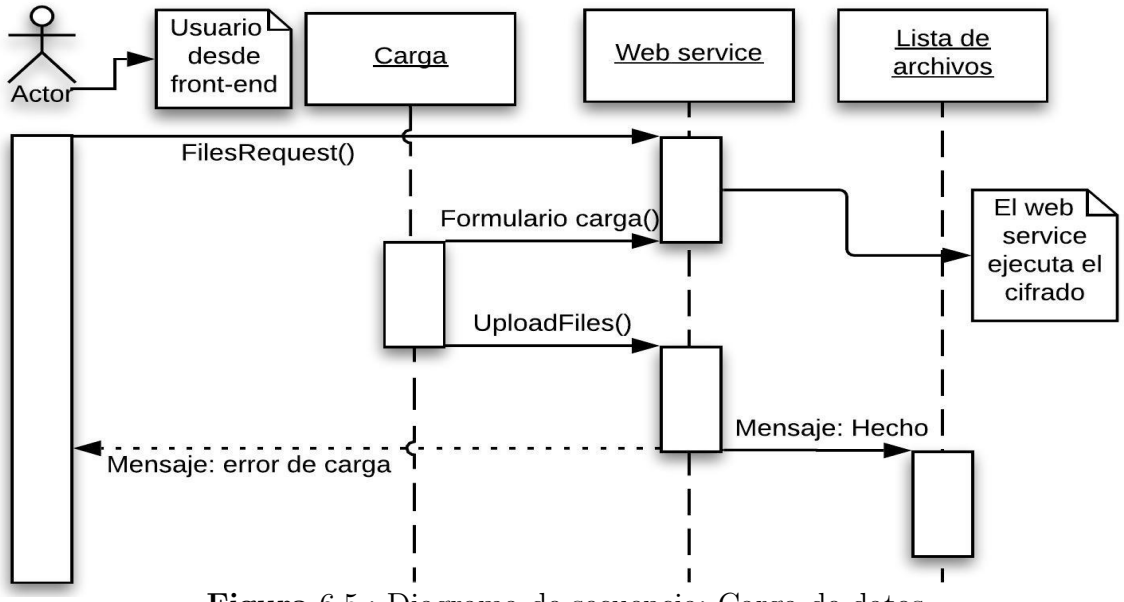


Figura 6.5.: Diagrama de secuencia: Carga de datos.
Fuente: Elaboración propia

Diagrama de secuencia: Descarga de datos

La Figura 6.6, muestra la secuencia realizada por el prototipo para ejecutar el proceso de descarga, este proceso se puede ejecutar una vez que el usuario haya seleccionado el archivo que desea descargar desde la lista de los mismos y luego de ejecutado la descarga, el web service, se encarga de realizar el proceso de descifrado y descarga del archivo seleccionado.

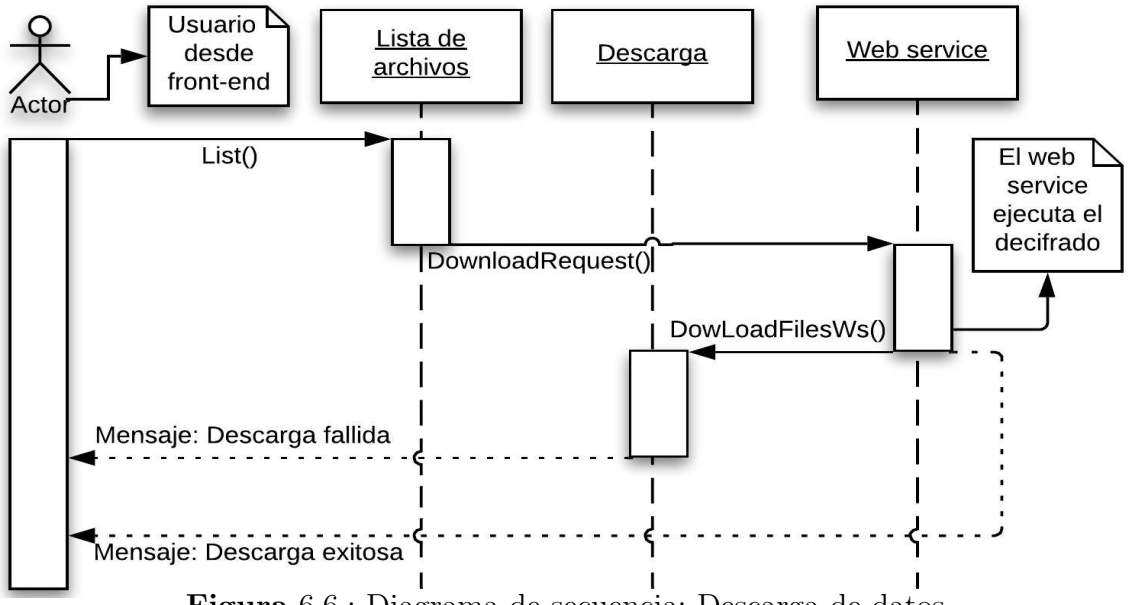


Figura 6.6.: Diagrama de secuencia: Descarga de datos.
Fuente: Elaboración propia

Diagrama de secuencia: Compartir datos

La Figura 6.7, muestra la secuencia realizada por el prototipo para ejecutar el proceso de compartición de datos, este proceso se puede ejecutar una vez que el usuario haya seleccionado el archivo que desea compartir y luego de ejecutado el proceso, el web service muestra un formulario donde se seleccionan los archivos y los usuarios con quien se desea compartir, una vez finalizado el proceso de compartición de datos, los archivos se listan en la opción de archivos compartidos.

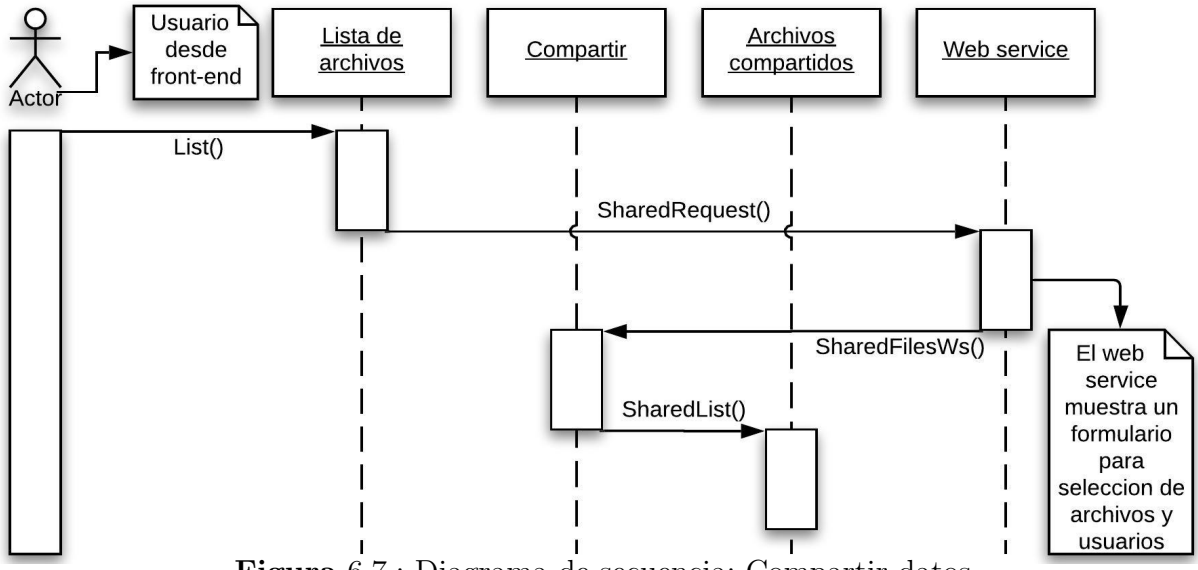


Figura 6.7.: Diagrama de secuencia: Compartir datos.
Fuente: Elaboración propia

6.4.2. Metamodelo lógico del esquema de Base de datos NoSQL

Las Bases de datos NoSQL, por sus características, dificulta poder expresar documentalmente su esquema, sin embargo, el trabajo de Chillón, Alberto H. [5], ha servido como referencia para elaborar y documentar el metamodelo lógico de la base de datos desarrollada en MongoDB como se muestra en la Figura 6.8. La base de datos, está compuesta por 6 colecciones, estas colecciones (son el equivalente a una tabla en BD relacionales), almacenan documentos con la estructura de conjunto de valor de objetos JSON (JavaScript Object Notation), cada una de las colecciones se relacionan a través del *_id*, la misma que también se puede utilizar para realizar consultas según necesidad. La colección **usuarios** contiene datos de cada uno de los usuarios, así como también los permisos, esta colección interactúa con la colección **roles** que identifica el perfil del usuario y la colección "eventos"que registra todas las actividades de cada usuario. Para el caso del almacenamiento de datos en el prototipo, se utilizó la especificación de almacenamiento GridFS de MongoDB, que sirve para almacenar datos que superan el límite de tamaño de documentos BSON de 16 MB, esta especificación utilizada, almacena un archivo usando dos colecciones, la primera es el **fs.files** que almacena el

metadato de un archivo y el otro es **fs.chunks** que almacena el archivo previamente cifrado por el web service en "n" cantidad de fragmentos binarios que varían de acuerdo al tamaño del archivo a almacenar, lo que desde el punto de vista de seguridad, lo hace difícil poder leer el contenido de la base de datos fuera del prototipo; en el caso de compartir un archivo, solo se toma el metadato de la colección **fs.files** y se almacena en la colección **compartidos** junto al *_id* del usuario(s) con quien se va a compartir.

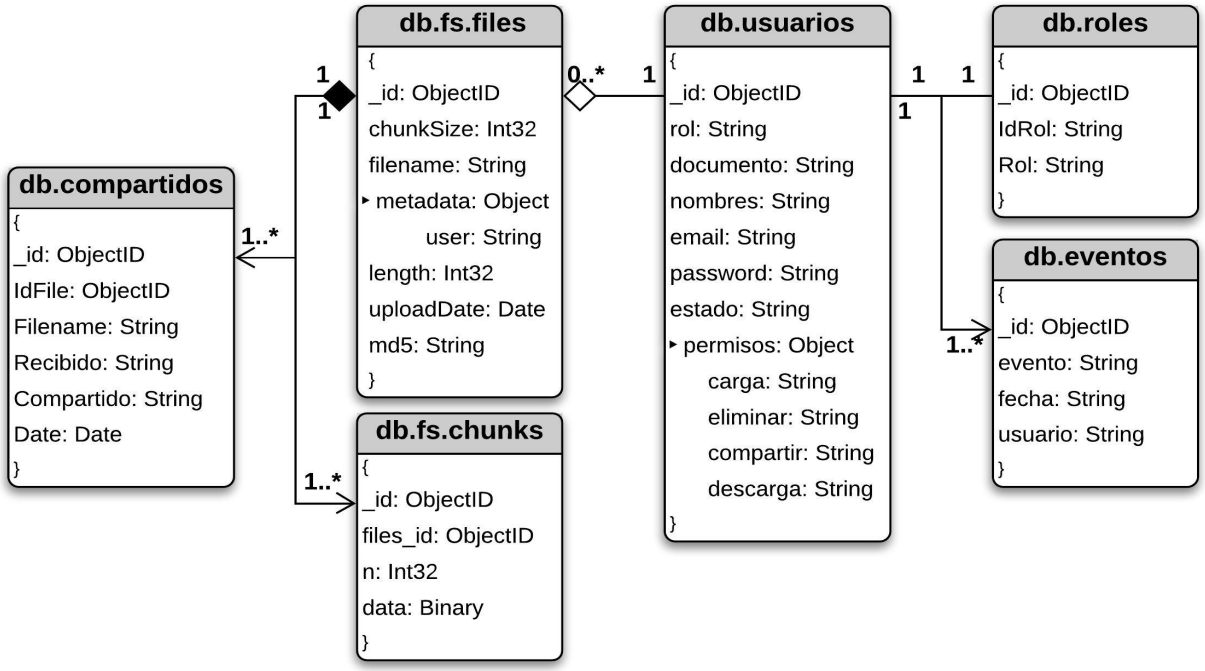


Figura 6.8.: Metamodelo lógico de la Base de datos en MongoDB.
Fuente: Elaboración propia

6.4.3. Implementación de mecanismos de seguridad

El prototipo cuenta con cuatro controles de seguridad muy importantes como mecanismos de seguridad, estos han sido implementados para cumplir con lo establecido en los requisitos funcionales y no funcionales, así como también, brindar seguridad al usuario al momento de interactuar con las funcionalidades del prototipo; estos controles son: El control de acceso, el cifrado de datos en tránsito, el cifrado de datos en reposo y la auditoría de acciones del prototipo.

Control de acceso

El mecanismos de control de accesos está compuesta por tres fases, la primera es el ingreso de las credenciales mostrada en la Figura 6.9, donde una vez que se haya enviado las credenciales, se genera una Id de sesión que junto con la segunda fase de autenticación mostrada en la Figura 6.10, se valida el inicio de sesión, si los datos ingresados son correctos, esta fase genera

una validación de doble factor de autenticación a través de un código oculto en una imagen de código QR, que una vez ingresada el código, en la última fase de verificación de 2FA mostrada en la Figura 6.11, se valida que el código ingresado coincida con las credenciales de usuario y el ID de sesión. Este código de 2FA, no puede ser vuelto a usar para otro intento de inicio de sesión, de esta manera, se asegura que no se cree una sesión en paralelo con la misma ID de sesión.

```php
<?php
session_start();
require 'vendor/autoload.php';
require 'clsCifrado.php';
require 'clsLogEventos.php';
if ( $_SERVER['REQUEST_METHOD']=="POST"){
    VerificarUser();
}
function VerificarUSer(){
    $token = $_POST['itoke'];
        if($_SESSION['Idtoken'] == $token){
            if (isset($_POST['signupInputPassword'])&& !empty($_POST['signupInputPassword']) ){
            $clsCifrado = new clsCifrado();
            $clsLog = new clsLogEventos();
            $manager = new MongoDB\Driver\Manager("mongodb://localhost:27017");
            $collection = (new MongoDB\Client)->archivos->usuarios;
            $pass =$clsCifrado-> my_encrypt((string) $_POST['signupInputPassword']);//Cifrar la passw
            $query = array('email' => (string) $_POST['signupInputEmaill'],'password' =>(string)  $pass );
            $user = $collection ->findOne($query);
        if($user){
            //logeado Exitosamente
                        $_SESSION['email']  =  $_POST['signupInputEmaill'];
                        $clsLog->GrabarLog("Logeo exitoso" ,$_SESSION['email']);
                        header('Location:autenticar.php');
        }else{
            //No logeado
                    $contador=$contador+1;
                    if ($contador>3){
                        echo'<script type="text/javascript"> swal({ title: "Usuario Bloqueado",
                        text: "Contacte a Soporte",   type: "error",   showCancelButton: false,
                        confirmButtonColor: "#DD6B55",   confirmButtonText: "Aceptar",
                        closeOnConfirm: false }, function(){   swal("Volviendo al login!", "",
                        "success"); window.location="index.php";});
                    </script>';
                        }else{
                        echo'<script type="text/javascript"> swal({   title: "Usuario o Password",
                        text: "Invalido(s)",   type: "error",   showCancelButton: false,
                        confirmButtonColor: "#DD6B55",   confirmButtonText: "Aceptar",
                        closeOnConfirm: false }, function(){   swal("Volviendo al login!", "",
                        "success"); window.location="index.php";});
                    </script>';
                        }
        }
    }
}else{
    session_destroy();
    echo'<script type="text/javascript">
       swal({   title: "La Sesión no existe",   text: "",   type: "error",   showCancelButton: false,
       confirmButtonColor: "#DD6B55",   confirmButtonText: "Aceptar",   closeOnConfirm: false },
       function(){   swal("Volviendo al login!", "", "success"); window.location="index.php";});
            </script>';
}
}
?>
```

Figura 6.9.: Ingreso de credenciales.
Fuente: Elaboración propia

```php
<?php
session_start();
require "Authenticator.php";
$Authenticator = new Authenticator();
if (!isset($_SESSION['auth_secret'])) {
    $secret = $Authenticator->generateRandomSecret();
    $_SESSION['auth_secret'] = $secret;
}
    $user   =  $_SESSION['email'] ;
    $qrCodeUrl = $Authenticator->getQR($user, $_SESSION['auth_secret']);
if (!isset($_SESSION['failed'])) {
    $_SESSION['failed'] = false;
}
?>
```

Figura 6.10.: Valida credenciales.
Fuente: Elaboración propia

```php
<?php
session_start();
require 'vendor/autoload.php';
require "Authenticator.php";
require 'clsLogEventos.php';
if ($_SERVER['REQUEST_METHOD'] != "POST") {
    header("location: index.php");
    die();
}else{
    $Authenticator = new Authenticator();
$clsLog = new clsLogEventos();
$checkResult = $Authenticator->verifyCode($_SESSION['auth_secret'],
$_POST['code'], 2);// 2 = 2*30sec clock tolerance
if (!$checkResult) {
    $_SESSION['failed'] = true;
    $clsLog->GrabarLog("Autenticación 2FA NO exitosa" ,$_SESSION['email']);
    header("location: autenticar.php");
    die();
} else{
    $collection = (new MongoDB\Client)->archivos->usuarios;
    $cursorp = $collection->find([ 'email' =>$_SESSION['email']]);
    foreach ($cursorp as $key => $value) {
        $rol=   $value["rol"];
    }
    switch ($rol) {
        case "1":
            $clsLog->GrabarLog("Autenticación 2FA exitosa--> ".$rol ,$_SESSION['email']);
            header("location:Admin.php");
            break;
        case "2":
            $clsLog->GrabarLog("Autenticación 2FA exitosa--> ".$rol ,$_SESSION['email']);
            header("location:Files.php");
            break;
        default:
            break;
    }
}
}
?>
```

Figura 6.11.: Validar 2FA.
Fuente: Elaboración propia

Cifrado de datos en tránsito

El mecanismo de cifrado en tránsito, ha sido implementado a través de la adquisición y configuración de certificado digital TLS 1.3 firmado por una autoridad certificadora, este se ha incorporado al prototipo previa configuración del servidor web, en donde se ha creado un VirtualHost como se muestra en la Figura 6.12 para que el certificado pueda operar adecuadamente.

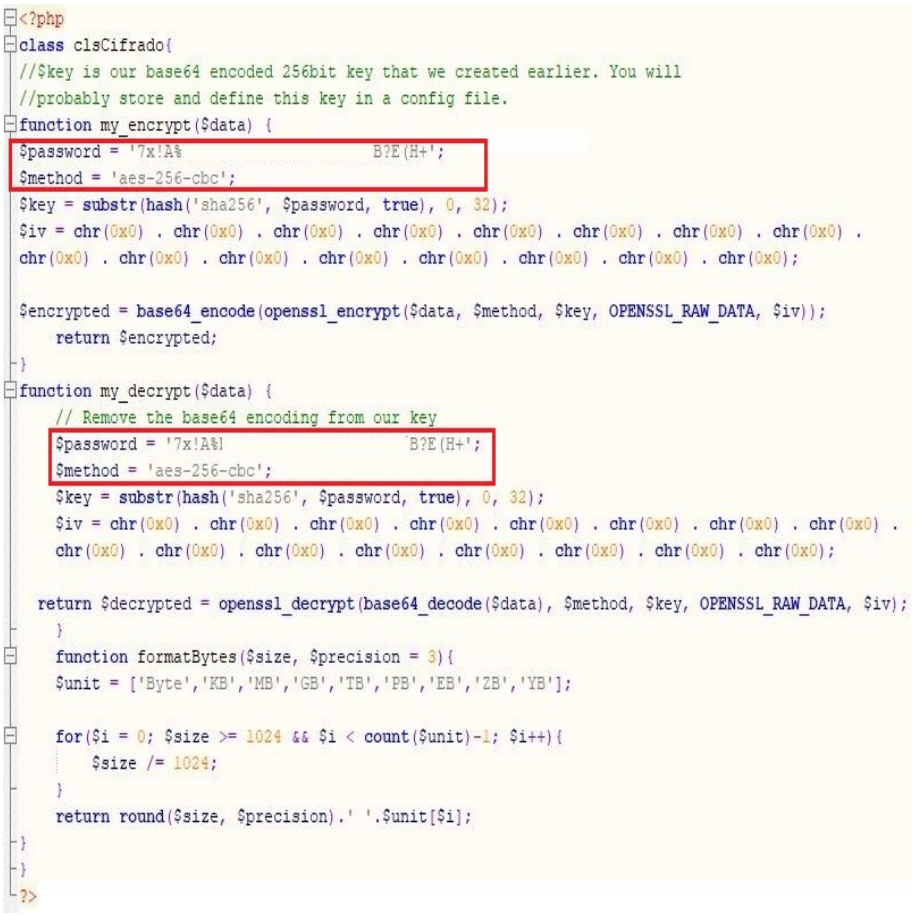
```
#
<VirtualHost *:80>
    ServerName repositorio-itm.info
    DocumentRoot "${INSTALL_DIR}/www/filescloud"
    <Directory  "${INSTALL_DIR}/www/filescloud/">
        options -Indexes -Includes -FollowSymLinks -MultiViews
        Require local
    </Directory>
</VirtualHost>


## repositorio-itm.info
 <VirtualHost *:443>
    DocumentRoot "${INSTALL_DIR}/www/filescloud"
    ServerName repositorio-itm.info
    #ServerAlias *.repositorio-itm.info
    SSLEngine on
    SSLCertificateFile "${INSTALL_DIR}\bin\apache\apache2.4.39\conf\key\298e3171lde7ba47.crt"
    SSLCertificateKeyFile "${INSTALL_DIR}\bin\apache\apache2.4.39\conf\key\repositorio-itm_info.key"
    SSLCertificateChainFile "${INSTALL_DIR}\bin\apache\apache2.4.39\conf\key\gd_bundle-g2-g1.crt"
    <Directory  "${INSTALL_DIR}/www/filescloud/">
        options -Indexes -Includes -FollowSymLinks -MultiViews
        Require all granted
    </Directory>
 </VirtualHost>
```

Figura 6.12.: Configuración de implementación de certificado digital.
Fuente: Elaboración propia

Cifrado y descifrado de datos en reposo

El mecanismo de cifrado y descifrado de datos mostrado en la Figura 6.13, funciona usando una llave privada segura, junto al algoritmo de cifrado de AES 256-CBC. Este proceso funciona bajo el parámetro de cifrado: **encrypted = base64_encode(openssl_encrypt($data, $method, $key, $OPENSSL_RAW_DATA, $iv))**, que consiste en el archivo a cifrar, el método de cifrado, la llave privada, el formato de cifrado de datos y los valores del Vector de inicialización de cifrado, el dato cifrado a través de este parámetro de valores lo devuelve codificado en Base64; de la misma manera, se realiza el descifrado de los datos, con la diferencia de que varía el orden de los datos dentro del parámetro inicialmente definido, quedando de la siguiente forma: **decrypted = openssl_decrypt(base64_dencode($data), $method, $key, $OPENSSL_RAW_DATA, $iv)**. EL proceso de cifrado y descifrado de datos, no altera la integridad inicial de un archivo almacenado, para ello, se ha realizado una verificación de integridad de un archivo previo a la cargar y posterior a la descarga de un archivo desde el prototipo, el resultado de esta verificación se muestra en la Figura G.28.



```php
<?php
class clsCifrado{
//$key is our base64 encoded 256bit key that we created earlier. You will
//probably store and define this key in a config file.
function my_encrypt($data) {
$password = '7x!A%                    B?E(H+';
$method = 'aes-256-cbc';
$key = substr(hash('sha256', $password, true), 0, 32);
$iv = chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) .
chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0);

$encrypted = base64_encode(openssl_encrypt($data, $method, $key, OPENSSL_RAW_DATA, $iv));
    return $encrypted;
}
function my_decrypt($data) {
    // Remove the base64 encoding from our key
    $password = '7x!A%l                    B?E(H+';
    $method = 'aes-256-cbc';
    $key = substr(hash('sha256', $password, true), 0, 32);
    $iv = chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) .
    chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0) . chr(0x0);

  return $decrypted = openssl_decrypt(base64_decode($data), $method, $key, OPENSSL_RAW_DATA, $iv);
    }
    function formatBytes($size, $precision = 3){
    $unit = ['Byte','KB','MB','GB','TB','PB','EB','ZB','YB'];

    for($i = 0; $size >= 1024 && $i < count($unit)-1; $i++){
        $size /= 1024;
    }
    return round($size, $precision).' '.$unit[$i];
}
}
?>
```

Figura 6.13.: Proceso de cifrado y descifrado de datos.
Fuente: Elaboración propia

Auditoría

El mecanismo de auditoría mostrado en la Figura 6.14, consiste en generar un ID de cualquier acción o evento realizado por un usuario y este proceso se lista en la interfaz del administrador en donde se muestra el ID, la acción realizada, la fecha e ID del usuario.

```php
<?php
class clsLogEventos{
    function GrabarLog($Evento,$User) {
    $manager = new MongoDB\Driver\Manager("mongodb://localhost:27017");
    $ColEventos = (new MongoDB\Client)->archivos->eventos;
        $tz = new DateTimeZone('America/Bogota'); //Change your timezone
        $date = date("Y-m-d h:i:sa"); //Current Date
        $a = new MongoDB\BSON\UTCDateTime(strtotime($date)*1000);
        $datetime = $a->toDateTime();
        $datetime->setTimezone($tz); //Set timezone
        $time=$datetime->format(DATE_ATOM);  //(example: 2005-08-15T15:52:01+00:00)
        $insertOneResult = $ColEventos->insertOne(['evento' => $Evento,
        'fecha' => $time,'usuario' => $User,]);
    }
    function GetDateTimeZone(){
        $tz = new DateTimeZone('America/Bogota'); //Change your timezone
        $date = date("Y-m-d h:i:sa"); //Current Date
        $a = new MongoDB\BSON\UTCDateTime(strtotime($date)*1000);
        $datetime = $a->toDateTime();
        $datetime->setTimezone($tz); //Set timezone
        $time=$datetime->format(DATE_ATOM);  //(example: 2005-08-15T15:52:01+00:00)
         return $time;
    }
    function getnextid($database,$collections){
        $m = new MongoClient();
        $db = $m->selectDB($database);
        $cursor = $collection->find()->sort(array("_id" => -1))->limit(1);
        $array = iterator_to_array($cursor);
    foreach($array as $value){

        return $value["_id"] + 1;
    }
 }
}
?>
```

Figura 6.14.: Registro de eventos.
Fuente: Elaboración propia

6.5. Implementación del prototipo

EL prototipo de seguridad se ha implementado en una workstation dentro de las instalaciones del laboratorio de Máquinas Inteligentes y Reconocimiento de Patrones - MIRP. En esta máquina, se ha instalado y configurado el Servidor Web gratuito Apache v2.4.39 y el motor MongoDB Community Server v4.2.1 para que el prototipo de almacenamiento y compartición segura de datos, pueda funcionar adecuadamente y posteriormente se realice las pruebas de cumplimiento funcional y técnico, en el proceso de implementación se ha creado el dominio repositorio-itm.info, a través del VirtualHost del servidor web, la misma a la que se le incorporó un certificado digital TLS 1.3 firmado, en la Figura 6.15, se muestra la interfaz de logueo del prototipo ya implementado listo para realizar pruebas de funcionamiento.

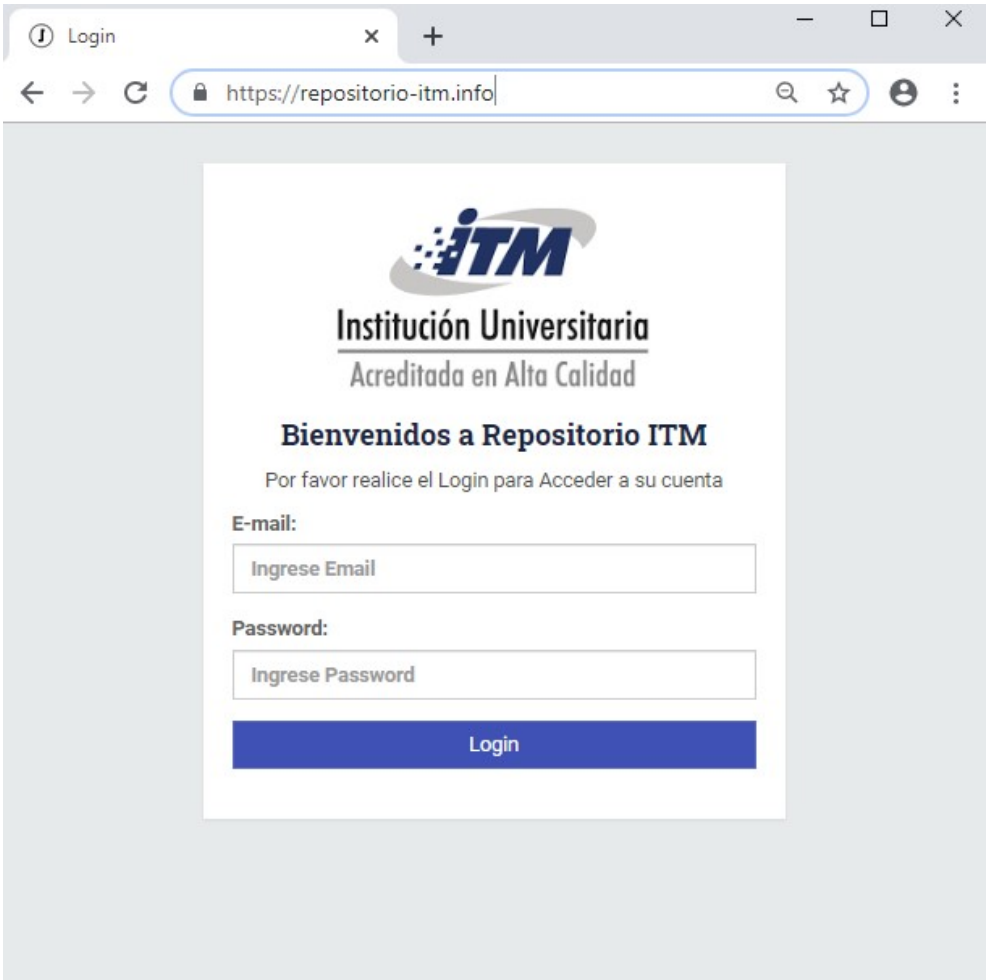


Figura 6.15.: Interfaz de autenticación prototipo.
Fuente: Prototipo desarrollado

6.5.1. Configuraciones básicas de seguridad del Servidor web

Durante el proceso de implementación del prototipo, en el servidor web apache v2.4.39, se tuvo que hacer configuraciones de seguridad básica en el archivo httpd.conf, con el propósito de cubrir vulnerabilidades propias del servidor web, teniendo en cuenta que el prototipo fue desarrollado en el lenguaje de programación PHP (Hypertext Preprocessor), adicionalmente, se ha realizado las configuraciones que implementa el funcionamiento de un certificado digital firmado por una autoridad certificadora mostrada en la Figura 6.12 y cuyo funcionamiento se muestra en el Anexo G.5, este con la finalidad de proteger las conexiones y los datos generados entre el usuario y el prototipo; la configuraciones realizadas en el servidor web, se detallan a continuación:

OCULTAR VERSIÓN DE APACHE

ServerSignature Off

ServerTokens Prod

EJECUTAR APACHE BAJO SU PROPIA CUENTA Y GRUPO

User apache

Group apache

CONTROL EN EL MODULO DE CABECERA

Protección X-XSS

Header set X-XSS-Protection "1; mode=block"

Opciones de X-Frame

Header always append X-Frame-Options DENY

Opciones de tipo de contenido X

Header set X-Content-Type-Options nosniff

Política de seguridad de contenido

Header set Content-Security-Policy "base-uri 'none'; form-action 'self '; frame-ancestors 'none'; upgrade-insecure-requests" "expr =% {CONTENT_TYPE} =∼ m#text \ /(html| javascript)| application\ /pdf| xml#i"

Política de referencia

Header set Referrer-Policy "no-referrer"

Seguridad de transporte estricta de HTTP

Header set Strict-Transport-Security "max-age=31536000; includeSubDomains"

Cookies

```
Header edit Set-Cookie ^(.*)$    $1;HttpOnly;Secure;SameSite=Strict
Header always edit Set-Cookie ^(.*)$    $1;HttpOnly;secure
```

PROTEGIENDO VULNERABILIDADES TRACE

```
TraceEnable Off
```

El prototipo de almacenamiento y compartición de datos de investigación, principalmente se ha soportado por las referencias de seguridad definidas en el Apartado 6.1, y para su diseño y desarrollo se ha seguido, lo establecido en el modelo de seguridad previamente desarrollado en el Capítulo 5, además de la metodología de desarrollo en cascada que se ha adaptado a las necesidades del diseño y desarrollo del prototipo, lo que ha permitido definir los requisitos de diseño e implementación de mecanismos de seguridad; al finalizar todo los procesos, se ha obtenido una solución tecnológica como prototipo de software, que ha sido sometida a pruebas de funcionamiento y operatividad, los resultados de estos se muestran en el Anexo G, a través de imágenes, donde se puede ver el cumplimiento y funcionamiento de todos los requisitos definidos.

7. Cumplimiento funcional y técnico de los requerimientos de seguridad

El cumplimiento de los requisitos funcionales y técnicos de seguridad, es de mucha importancia, en un desarrollo de software ya que de esta manera se puede comprobar que se ha cubierto las necesidades del cliente con respecto a la solución tecnológica, este cumplimiento va de la mano con las pruebas de seguridad que se deben realizar a los desarrollos, antes de ser puestos a producción. en particular, el prototipo, ha sido sometido a una verificación del cumplimiento de los requisitos funcionales y no funcionales, así como también a una prueba de seguridad a través de una herramienta de escaneo de vulnerabilidades.

7.1. Verificación funcional y técnico de los requerimientos de seguridad

La verificación del cumplimiento de requisitos funcionales y técnico de seguridad, se ha desarrollado inicialmente haciendo una **inspección visual** del cumplimiento de los requisitos funcionales establecidos en el **Apartado 6.3.1**, posteriormente, se ha realizado unas **pruebas de funcionamiento**, que ha consistido en interactuar con las funcionalidades establecidas en el prototipo de acuerdo a los roles asignados (administrador o usuario) y por último se ha realizado una **revisión de los mecanismos de cifrado**, ingresando directamente a la base de datos y haciendo capturas de tráfico de datos con la herramienta Wireshark v3.0.6, que es un sniffer muy utilizada para el análisis de protocolos de red.
Las verificaciones de los requisitos se muestran en el **Anexo G**, que de acuerdo a los requerimientos definidos, se muestran capturas de las ventanas de cada uno de los requerimientos funcionalidades y técnicos verificadas, con base a las verificaciones realizadas, en la Tabla 7.1, se muestra en resumen el resultado de la verificación.

Check List de pruebas de requisitos funcionales y de seguridad del prototipo			
Requisitos funcionales	**Cumple**	**No cumple**	**observaciones**
Prototipo con arquitectura web	**X**		Arquitectura web en PHP y servidor Apache v2.4.39
Autenticación de Usuario			
Email y password	**X**		
2FA	**X**		Escaneo código QR.
Gestión de Usuarios			
Agregar	**X**		ID de usuario es email
Modificar	**X**		
Eliminar	**X**		
Gestión de archivos			
Carga	**X**		Carga cualquier dato multimodal
Descarga	**X**		Descarga de dato no afecta integridad
Compartir	**X**		Usuario solo pueden descargar
Eliminar	**X**		Solo lo hace el propietario del archivo
Auditoría	**X**		Registra las actividades de los usuarios
Cifrado de datos			
Tránsito	**X**		Usa certificado digital TLS 1.3 firmado
Reposo	**X**		Datos cifrado en AES256-CBC
Base de datos MongoDB	**X**		MongoDB Community Server v4.2.1
Interfaz intuitivo del prototipo	**X**		Interfaz de fácil acceso y operación
Mitigación de amenazas	**X**		Pruebas de cumplimiento funcional de los requisitos y mecanismos de seguridad

Tabla 7.1.: Check List de pruebas de requisitos funcionales y de seguridad del prototipo
Fuente: Elaboración propia.

7.2. Pruebas de seguridad del prototipo

Las pruebas de seguridad del prototipo, fueron realizadas mediante un escaneo automático, utilizando la herramienta Acunetix[1], que es un escáner de seguridad para aplicaciones web, para este caso en particular, se ha adquirido la versión 11.0.170951158 que contiene herramientas y funcionalidades que permiten detectar posibles fallos de seguridad que comprometan la confidencialidad, integridad y privacidad del prototipo de almacenamiento y compartición de datos. En la Figura 7.1, se muestra el resumen del proceso completo del escaneo de vulnerabilidades realizada con la herramienta antes mencionada, este proceso, ha consistido en ejecutar el escaneo dentro de la misma red con la herramienta instalada en otra PC, este último, con el propósito de que la herramienta pueda interactuar con todos los mecanismos de seguridad con los que cuenta el prototipo, así como también, comprobar las configuraciones de seguridad que se ha implementado al servidor web Apache v2.4.39 mostradas en el Apartado 6.5.1.

[1]https://www.acunetix.com/

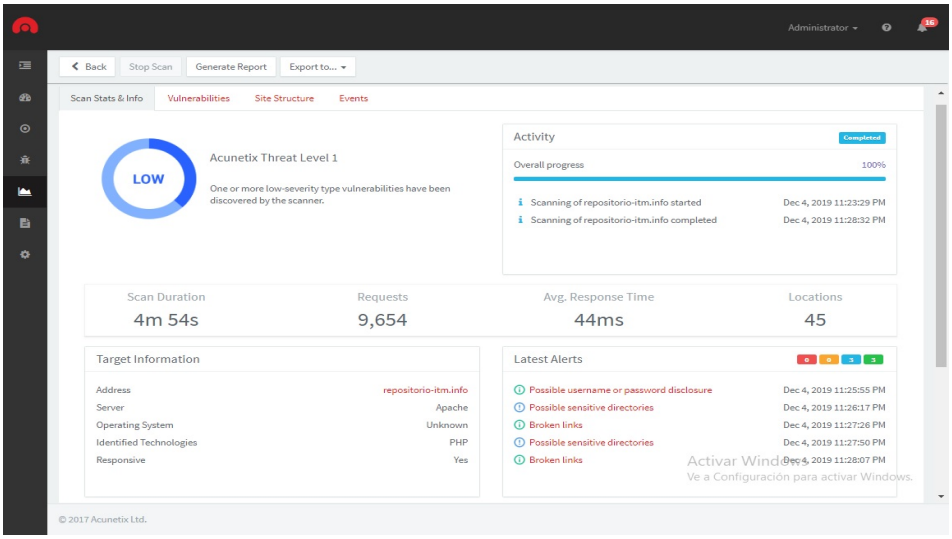


Figura 7.1.: Proceso finalizado del escaneo de vulnerabilidades.

Como resultado del proceso de escaneo de vulnerabilidades, en la Figura 7.2, se muestra las vulnerabilidades encontradas, las mismas que no representan un peligro para el prototipo, el reporte completo de este proceso se encuentra detallado en el Anexo H. En particular, no se profundizó en abordar las vulnerabilidades mostradas por la herramienta, debido a que estos no son parte del mapa de riesgos ni de los controles objetos de este proyecto por lo que se encuentran fuera del alcance de mitigación de las amenazas definidas en el Apartado 4.9.4, sin embargo, estas vulnerabilidades se podrían cubrir implementado políticas de redireccionamiento en el servidor web, control en los números de intentos de inicio de sesión para evitar denegación de servicio o ataques de fuerza bruta y en el caso que el prototipo sea llevado a un entorno de producción, pueden ser cubiertas con controles adicionales e infraestructura tecnológica de seguridad.

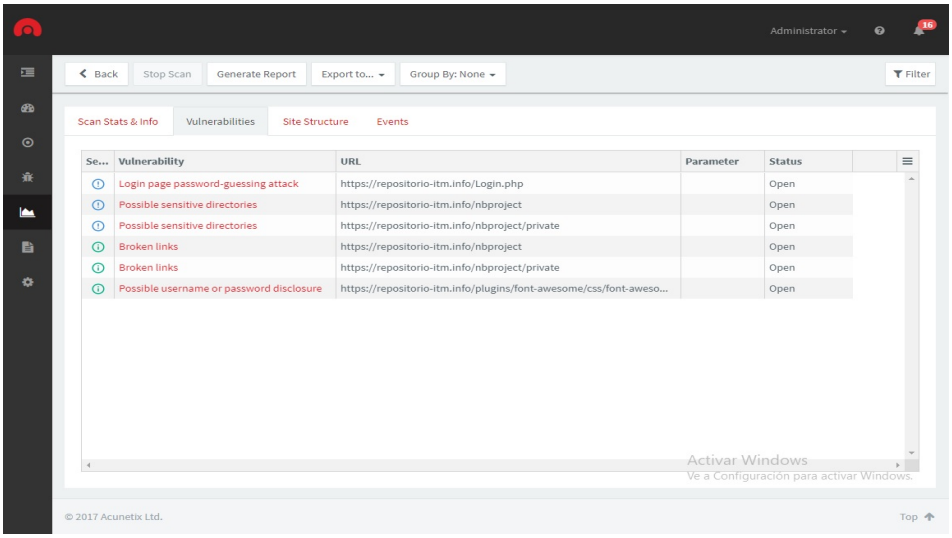


Figura 7.2.: Reporte de vulnerabilidades.

La verificación del cumplimiento de los requisitos funcionales, ha consistido en desarrollar pruebas de operación del prototipo, que durante la misma, se han ido ajustando todas las fallas de desarrollo y de seguridad encontradas, buscando así tener un prototipo que cumpla con la mitigación de las amenazas y vulnerabilidades previamente definidos; al finalizar todo este proceso, se ha desarrollado el escaneo de vulnerabilidades con la herramienta Acunetix que es especializada en detectar vulnerabilidades web. Los resultados de las pruebas de operación y escaneo de vulnerabilidades, permiten corroborar que el prototipo desarrollado cumple con los controles y mecanismos de seguridad apropiados para brindar confidencialidad, integridad y privacidad de los datos generados y almacenados en este.

8. Conclusiones, recomendaciones y trabajos futuros

El presente trabajo contiene un Modelo de seguridad orientado a preservar la confidencialidad, integridad y privacidad de los datos, en un sistema para el almacenamiento y compartición de datos multimodales en entornos de investigación, soportado en bases de datos NoSQL. Este trabajo ha iniciado con una amplia revisión del estado del arte sobre la seguridad en las bases de datos no relacionales (NoSQL), sus retos de seguridad, las vulnerabilidades a las que se encuentran expuestas y como las organizaciones que han adoptado esta tecnología de bases datos, han abordado las seguridad en cuanto a la protección de los datos personales, operacionales y transaccionales acordes a sus necesidades; lo anterior, ha sido fundamental para poder hacer una revisión e identificación de las bases de datos NoSQL más utilizadas en la actualidad y los mecanismos de seguridad existentes en cuanto autorización, autenticación, cifrado de datos en tránsito y en reposo, logrando así poder identificar que la seguridad en estos tipos de bases de datos depende de la gestión y administración de los desarrolladores que integran estas bases de datos con sus aplicaciones (web, móviles, etc.), así mismo, esta revisión ha permitido poder seleccionar a MongoDB como base de datos, debido a sus características funcionales y sus mecanismos de seguridad integrados en su motor, lo que se ajusta a uno de los objetivos desarrollados en este trabajo.

Con base a lo anterior, para este trabajo se ha propuesto una metodología que cuenta con cuatro fases, las mimas que cada una de ellas representa a los objetivos planteados dentro de este trabajo, iniciando con un análisis de riesgos informáticos, siguiendo con el desarrollo de un modelo de seguridad de la información que permita poder mitigar las amenazas con mayor impacto previamente identificados, luego desarrollar un prototipo de software que incorporen mecanismos y controles de seguridad definidos en el modelo de seguridad, que permitan mitigar las amenazas antes mencionadas y por último, realizar una verificación del cumplimiento de las funcionalidades y de mecanismos de seguridad implementados en el prototipo.

El análisis de riesgos informáticos, ha sido desarrollado en los ambientes del laboratorio de Máquinas Inteligentes y Reconocimiento de Patrones - MIRP que es un entorno de investigación real, en donde se ha tenido como referencia uno de los proyectos de investigación que se viene desarrollando dentro de este ambiente; el proceso del análisis de riesgos, ha permitido identificar los activos de información existentes y las múltiples amenazas a los que estos activos se encuentran expuestos, los activos de información en estos tipos de entornos,

así como también las salvaguardas existentes y como las amenazas identificadas impactan en los diversos activos de información, con toda la información obtenida, se ha identificado las amenazas que tienen mayor impacto en los activos de información y para ello se ha definido el tratamiento a realizar. **El modelo de seguridad de la información**, ha sido desarrollado con base a algunos marcos legales y normativos actualmente utilizados en Colombia, este modelo tiene un contexto de aplicación definido y busca abordar las amenazas con mayor impacto previamente identificadas en entornos de investigación, para ello, se ha establecido un ciclo de operación que cuenta con cuatro fases donde cada uno de ellos cuenta con metas que permiten abordar los problemas de seguridad a través de los productos generados por cada una de las metas, así mismo, tiene definido un modelo de madurez que permite identificar el estado de aplicación del modelo de seguridad y para ellos se han definido algunos mecanismos de seguridad que ayudan a abordar y mitigar no solo las amenazas con mayor impacto previamente identificadas, sino que también otras amenazas que posteriormente puedan tomar relevancia de acuerdo a su impacto. Con lo establecido en el modelo y junto a algunos de sus mecanismos de seguridad, se ha **desarrollado un prototipo de software para el almacenamiento y compartición de datos de investigación**, para la cual se han tenido referencias de seguridad que junto a una metodología de desarrollo de software, han permitido definir los requisitos para el diseño y desarrollo del prototipo, en el proceso de desarrollo, se estableció una base de datos no relacional en MongoDB, que previamente había sido seleccionada con base a la revisión del estado del arte, luego se ha realizado el diseño de arquitectura de seguridad del prototipo que junto con el modelado del web service que es quien controla todo el mecanismos de seguridad y algunos de los procesos más importantes, esto ha permitido realizar el desarrollo eficiente del prototipo que tiene incorporado los requisitos funcionales y de seguridad que abordan la mitigación de las amenazas con mayor impacto antes mencionadas, por último, el prototipo ha sido sometido a pruebas de **cumplimiento de funcionalidades técnicas y de requerimientos de seguridad**, estas pruebas han sido desarrolladas en dos etapas, la primera ha consistido en interactuar con cada una de las funcionalidades del prototipo y con la revisión técnica de los mecanismos de seguridad, en la segunda etapa se ha realizado un escaneo de vulnerabilidades web con la herramienta Acunetix que es especializada en la detección de posibles fallos de seguridad que comprometan la confidencialidad, integridad y privacidad de los datos generados y almacenados dentro del prototipo.

La aplicación del modelo de seguridad ha permitido abordar las amenazas de seguridad existentes en entornos de investigación, en particular, el resultado obtenido en el desarrollo de las pruebas realizadas al prototipo de software, evidencian que la aplicación del modelo junto a los mecanismos de seguridad aplicados, han mitigado la materialización de las amenazas con mayor impacto que previamente han sido identificadas; así mismo, el uso de la base de datos MongoDB ha sido importante para demostrar que estas base de datos de acuerdo a sus características, también pueden llegar a ser muy seguras si es que durante el procesos de desarrollo e integración con cualquier solución tecnológica, se tienen en cuenta lo mecanismos

de seguridad apropiados a implementar. Por otro lado, se tiene que tener en cuenta que tipo de mecanismos de seguridad se van a implementar a estas bases de datos ya que es posible que su rendimiento durante el procesamiento de datos pueda verse afectados debido a las características propias de este tipo de base de datos, es importante mencionar que en este trabajo el rendimiento no ha sido un criterio a considerar.

Finalmente, como trabajo futuro el modelo de seguridad puede ser mejorado y ajustado para poder ampliar el alcance de intervención y mitigación de nuevas amenazas, así mismo, el prototipo de almacenamiento seguro, puede ser mejorado para poder ser llevado a un entorno de producción, operando bajo su propia infraestructura, esto debido a que al estar desarrollado con una interfaz web y a la característica de alto rendimiento de la base de datos, este puede soportar múltiples conexiones con operaciones en simultáneo, así mismo, según las necesidades de implementación, también se podría aumentar o mejorar los mecanismos de seguridad ya implementados.

Bibliografía

[1] Algarni, A ; Alsolami, F ; Eassa, F ; Alsubhi, K ; Jambi, K ; Khemakhem, M: An Open Tool Architecture for Security Testing of NoSQL-Based Applications. En: *2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)* (2017), p. 220–225

[2] Baars, Henning ; Kemper, Hans-George: Management Support with Structured and Unstructured Data—An Integrated Business Intelligence Framework. En: *Information Systems Management* 25 (2008), Nr. 2, p. 132–148

[3] Borgman, Christine L.: The conundrum of sharing research data. En: *Journal of the American Society for Information Science and Technology* 63 (2012), jun, Nr. 6, p. 1059–1078. – ISSN 15322882

[4] Chahal, Deepak ; Kharb, Latika ; Gupta, Manhar: Challenges and Security Issues of NOsql Databases. En: *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 2 (2017), Nr. 5, p. 976–982

[5] Chillón, Alberto H. ; Morales, Severino F. ; Molina, Jesús G. ; Ruiz, Diego S.: Visualización de Esquemas en Bases de Datos NoSQL basadas en documentos.

[6] Cuzzocrea, Alfredo ; Shahriar, Hossain: Data masking techniques for NoSQL database security: A systematic review. En: *2017 IEEE International Conference on Big Data (Big Data)*, IEEE, dec 2017. – ISBN 978–1–5386–2715–0, p. 4467–4473

[7] Dai, Sheng-Qi ; Li, Hong ; Xiong, Jun ; Ma, Jun ; Guo, Hai-Qiang ; Xiao, Xiangming ; Zhao, Bin: Assessing the extent and impact of online data sharing in eddy covariance flux research. En: *Journal of Geophysical Research: Biogeosciences* (2018), p. 1–9

[8] Ferreira Junior, José R. ; Oliveira, Marcelo C. ; de Azevedo-Marques, Paulo M.: Cloud-Based NoSQL Open Database of Pulmonary Nodules for Computer-Aided Lung Cancer Diagnosis and Reproducible Research. En: *Journal of Digital Imaging* 29 (2016), Nr. 6, p. 716–729

[9] Google Cloud: Google Infrastructure Security Design Overview — Google Cloud Platform. En: *Whitepaper* (2016), p. 1–14

[10] Govindarajan, M: Challenges for Big Data Security and Privacy. En: *Advanced Methodologies and Technologies in Network Architecture, Mobile Computing, and Data Analytics*. IGI Global, 2019, p. 57–66

[11] Gritzalis, Dimitris ; Iseppi, Giulia ; Mylonas, Alexios ; Stavrou, Vasilis: Exiting the Risk Assessment Maze. En: *ACM Computing Surveys* 51 (2018), Nr. 1, p. 1–30. – ISSN 03600300

[12] Gupta, Neha ; Agrawal, Rashmi: NoSQL Security. En: Raj, Pethuru (Ed.) ; Deka, Ganesh C. (Ed.): *Advances in Computers* Vol. 109. Elsevier, 2018, p. 101–132

[13] Holik, F. ; Neradova, S.: Vulnerabilities of modern web applications. En: *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings* (2017), p. 1256–1261

[14] Hou, Boyu ; Shi, Yong ; Qian, Kai ; Tao, Lixin: Towards Analyzing MongoDB NoSQL Security and Designing Injection Defense Solution. En: *2017 IEEE 3rd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS)*, IEEE, may 2017. – ISBN 978–1–5090–6296–6, p. 90–95

[15] ICETEX, INSTITUTO COLOMBIANO DE CRÉDITO EDUCATIVO Y ESTUDIOS TÉCNICOS EN EL E.: MANUAL DE POLÍTICAS DE SEGURIDAD DIGITAL. 2018. – Informe de Investigación. – 63 p.

[16] International Organization for Standardization: NORMA INTERNACIONAL ISO 31000:2018. 2 (2018), p. 26

[17] International Organization for Standardization / International Electrotechnical Commission - ISO/IEC 27000:2014: Information technology — Security techniques — Information security management systems — Overview and vocabulary. 3 (2014), p. 38

[18] International Organization for Standardization / International Electrotechnical Commission - ISO/IEC 27001:2013: Information technology — Security techniques — Information security management systems — Requirements. 2013 (2013)

[19] International Organization for Standardization / International Electrotechnical Commission - ISO/IEC 27002:2013: Information technology — Security techniques — Code of practice for information security controls. En: *IEC* 2 (2014), Nr. 27002, p. 88

[20] Javier Candau, Centro Criptológico Nacional, Ministerio de la P. *EAR - Herramientas para el Análisis de Riesgos*

[21] Kaur, Amandeep ; Dhindsa, Kanwalvir S.: Analysis of NoSQL Databases : A Comparative Study. 1 (2017), Nr. 1, p. 1–4

[22] Lith, Adam ; Mattsson, Jakob: Investigating storage solutions for large data. (2010), p. 70

[23] Miguel Angel Amutio Gómez, Ministerio de Hacienda y Administraciones P. ; Javier Candau, Centro Criptológico Nacional, Ministerio de la P.: MAGERIT-versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos. (2012), p. 75

[24] Miguel Angel Amutio Gómez, Ministerio de Hacienda y Administraciones P. ; Javier Candau, Centro Criptológico Nacional, Ministerio de la P.: MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. (2012), p. 127

[25] MinTIC: Modelo de Seguridad y Privacidad de la Información. (2015), p. 1–32

[26] MINTIC: Guía de gestión de riesgos. En: *MINTIC* (2016), Nr. 7, p. 39

[27] Méndez, Gonzalo: Proceso Software y Ciclo de Vida. En: *Dpto. de ingeniería de software e inteligencia artificial, facultad de informática de la universidad Complutense de la universidad de Madrid* (2008)

[28] Obay, Mohamed A M. ; Altrafi, G ; Ismail, Mohammed O.: Relational vs . NoSQL Databases : A Survey. En: *International Journal of Computer and Information Technology* 03 (2014), Nr. 03, p. 2279–764. – ISSN 2279–0764

[29] Okman, Lior ; Gal-Oz, Nurit ; Gonen, Yaron ; Gudes, Ehud ; Abramov, Jenny: Security issues in NoSQL databases. En: *Proc. 10th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications, TrustCom 2011, 8th IEEE Int. Conf. on Embedded Software and Systems, ICESS 2011, 6th Int. Conf. on FCST 2011* (2011), p. 541–547

[30] Ron, Aviv ; Shulman-Peleg, Alexandra ; Bronshtein, Emanuel: No sql, no injection? examining nosql security. En: *arXiv preprint arXiv:1506.04082* (2015)

[31] Ron, Aviv ; Shulman-Peleg, Alexandra ; Puzanov, Anton: Analysis and mitigation of NoSQL injections. En: *IEEE Security & Privacy* 14 (2016), Nr. 2, p. 30–39

[32] Ross, Ronald S. ; McEvilley, Michael ; Oren, Janet C.: Systems security engineering: Considerations for a multidisciplinary approach in the engineering of trustworthy secure systems [including updates as of 1-03-2018]. 2018. – Informe de Investigación

[33] Saxena, Upaang ; Sachdeva, Shelly: An insightful view on security and performance of NoSQL databases. 799 (2018), p. 643–653

[34] Shahriar, Hossain ; Haddad, Hisham M.: Security Vulnerabilities of NoSQL and SQL Databases for MOOC Applications Department of Information Technology Department of Computer Science. 8 (2017), Nr. 1, p. 1244–1250

[35] van der Stock, A. *Una Guía para Construir Aplicaciones y Servicios Web Seguros*. 2005

[36] Strozzi Carlo. *NoSQL Relational Database Management System: Home Page*. 2010

[37] Torres-Salinas, Daniel ; Robinson-García, Nicolás ; Cabezas-Clavijo, Álvaro: Compartir los datos de investigación en Ciencia: introducción al data sharing. En: *El profesional de la información* 21 (2012), Nr. 2, p. 16–12

[38] Walport, Mark ; Brest, Paul: Sharing research data to improve public health. En: *The Lancet* 377 (2011), Nr. 9765, p. 537–539

[39] Wiley: Global Data Sharing Trends. 2016. – Informe de Investigación. – 1 p.

[40] Zahid, Anam ; Masood, Rahat ; Shibli, Muhammad A.: Security of sharded NoSQL databases: A comparative analysis. En: *Conference Proceedings - 2014 Conference on Information Assurance and Cyber Security, CIACS 2014* (2014), p. 1–8

[41] Zaki, Asadulla K.: NoSQL Databases: New Millennium Database for Big Data, Big Users, Cloud Computing and its Security Challenges. En: *IJRET: International Journal of Research in Engineering and Technology* (2014), p. 403–409

A. Anexo: Resultados del Análisis de riesgos

A.1. Identificación de activos de información

Activos	Posibles Vulnerabilidades
[B] Activos esenciales	
[B-01] Base de datos	Falta de parches o proceso de actualización, falencia en control de acceso, falta de monitoreo, falta o falencia de configuración de roles y perfiles, falta de políticas de respaldo, ausencia de control de datos de entrada o salida.
[B-02] Productos Tecnológicos en producción	Falta de control de cambios, Falta de parches o proceso de actualización o soporte, accesos directos en producción, falta de políticas de respaldo.
[B-03] Productos Tecnológicos desarrollados	
[B-04] Informes documentales	Falta de integridad o autenticidad, falencia en el proceso de seguimiento o control de versiones.
[IS] Servicios internos	
[IS-01] Servicio de internet	Falta de canal alterno de internet (ISP), falta de protección ante ataques DoS, contrato vencido, mala definición en los ANS.
[IS-02] Almacenamiento en la nube	Falta de canal alterno de internet (ISP), falta de protección ante ataques DoS, contrato vencido o no prorrogado.
[E] Equipamiento	
[SW] Aplicaciones	
[SW-01] Ofimática	No resguardo adecuado de licencias, licencias obsoletas, no actualización de aplicaciones y programas, descarga y uso no controlado de software, ausencia de copias de respaldo.

SW-02] Herram. desarrollo / programación	No resguardo adecuado de licencias, licencias obsoletas, no actualización de aplicaciones y programas, falencias en el control de acceso al código fuente, Ausencia de copias de respaldo, ausencia de control de datos de entrada o salida.
[SW-03] Herram. adquisición y procesamiento de datos de investigación	No resguardo adecuado de licencias, licencias obsoletas, no actualización de aplicaciones y programas, falencias en el control de acceso al código fuente, Ausencia de copias de respaldo.
[SW-04] Sistema operativo	No resguardo adecuado de licencias, licencias obsoletas, no actualización de aplicaciones y programas, falta de parches de seguridad, falencias en el control de acceso, Ausencia de copias de respaldo.
[HW] Equipos	
[HW-01] PC Workstation	Falencia o falta de anti-virus, no control de parches, falencia en el control de acceso, ausencia de políticas de seguridad lógica.
[COM] Comunicaciones	
[COM-01] Router	Falla en el proceso de parches, no actualización de equipos, falencia en la configuración de protocolos y servicios, ausencia de control físico.
[COM-02] Switch	
[COM-03] Access point	
[AUX] Elementos auxiliares	
[AUX-01] Dispositivo almacenamiento externo	Ausencia de copias de seguridad, ausencia de control físico.
[L] Instalaciones	
[L-01] Laboratorio investigación I	Ausencia de control físico, falencia en los utilitarios (aire, humedad, potencia).
[L-02] Laboratorio investigación II	
[P] Personal	
[P-01] Investigadores	Falta de conciencia acerca de la seguridad, Ausencia de mecanismos de monitoreo, falencia o ausencia de capacitación en seguridad o niveles de clasificación, ausencia de conocimiento en gestión de riesgos y el manejo de incidentes de seguridad.
[P-02] Aux. investigación	
[P-03] Ingenieros de soporte	
[P-04] Estudiantes vinculados	

Tabla A.1.: Activos y posibles vulnerabilidades identificadas
Fuente: EAR/PILAR 7.1.10.

A.2. Valoración de activos de información

Activos	D	I	C
[B] Activos esenciales			
[B-01] Base de datos	[8]	[8]	[5]
[B-02] Productos Tecnológicos en producción	[8]	[7]	[5]
[B-03] Productos Tecnológicos desarrollados	[8]	[7]	[5]
[B-04] Informes documentales	[4]	[7]	[5]
[IS] Servicios internos			
[IS-01] Servicio de internet	[3]	[2]	[7]
[IS-02] Almacenamiento en la nube	[5]	[3]	[3]
[E] Equipamiento			
[SW] Aplicaciones			
[SW-01] Ofimática	[1]	[3]	[4]
[SW-02] Herram. desarrollo / programación	[8]	[5]	[3]
[SW-03] Herram. adquisición y procesamiento de datos de inves.	[4]	[4]	[5]
[SW-04] Sistema operativo	[1]	[4]	[4]
[HW] Equipos			
[HW-01] PC Workstation	[7]	[3]	[3]
[COM] Comunicaciones			
[COM-01] Router	[3]	[1]	[2]
[COM-02] Swirch	[3]	[1]	[2]
[COM-03] Access point	[2]	[1]	[2]
[AUX] Elementos auxiliares			
[AUX-01] Dispositivo almacenamiento externo	[8]	[7]	[7]
[L] Instalaciones			
[L-01] Laboratorio investigación I	[4]	[3]	[3]
[L-02] Laboratorio investigación II	[4]	[3]	[3]
[P] Personal			
[P-01] Investigadores	[7]	[7]	[5]
[P-02] Aux. investigación	[7]	[5]	[3]
[P-03] Ingenieros de soporte	[6]	[5]	[3]
[P-04] Estudiantes vinculados	[3]	[5]	[3]

Tabla A.2.: Valoración de activos
Fuente: EAR/PILAR 7.1.10.

A.3. Identificación de amenazas

[B] Activos esenciales
Base de datos
[E.15]Alteración de la información
[E.18]Destrucción de la información
[E.19]Fuga de la información
[A.5]Suplantación de identidad
[A.6]Abuso de privilegios de acceso
[A.11]Acceso no autorizado
[A.15]Modificación de la información
[A.19]Revelación de información
Productos tecnológicos en producción
[E.15]Alteración de la información
[E.18]Destrucción de la información
[E.19]Fuga de la información
[A.5]Suplantación de identidad
[A.6]Abuso de privilegios de acceso
[A.11]Acceso no autorizado
[A.15]Modificación de la información
[A.19]Revelación de información
Productos tecnológicos desarrollados
[E.15]Alteración de la información
[E.18]Destrucción de la información
[E.19]Fuga de la información
[A.5]Suplantación de identidad
[A.6]Abuso de privilegios de acceso
[A.11]Acceso no autorizado
[A.15]Modificación de la información
[A.19]Revelación de información
Informes documentales
[E.15]Alteración de la información
[E.18]Destrucción de la información
[E.19]Fuga de la información
[A.5]Suplantación de identidad
[A.6]Abuso de privilegios de acceso
[A.11]Acceso no autorizado
[A.15]Modificación de la información
[A.19]Revelación de información

Tabla A.3.: Amenazas identificadas - Servicios esenciales
Fuente: EAR/PILAR 7.1.10.

[ES]Servicios externos
Servicio de internet
[I.8] Fallo de servicios de comunicaciones
[E.2] Errores del administrador del sistema / de la seguridad
[E.9] Errores de [re-]encaminamiento
[E.10] Errores de secuencia
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.24] Caída del sistema por agotamiento de recursos
[A.5] Suplantación de la identidad
[A.9] [Re-]encaminamiento de mensajes
[A.11] Acceso no autorizado
[A.14] Interceptación de información(escucha)
[A.15] Modificación de la información
[A.19] Revelación de información
[A.24] Denegación de servicio
Almacenamiento en la nube
[I.5] Avería de origen físico o lógico
[I.9] Interrupción de otros servicios o suministros esenciales
[E.1] Errores de los usuarios
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.15] Modificación de la información
[A.19] Revelación de información
[A.24] Denegación de servicio

Tabla A.4.: Amenazas identificadas - Servicios externos
Fuente: EAR/PILAR 7.1.10.

[E]Equipamiento
[SW]Aplicaciones
Ofimática
[E.8]Difusión de software dañino
[E.18]Destrucción de la información
[E.20]Vulnerabilidades de los programas(software)
[E.21]Errores de mantenimiento/actualización de programas(software)
[A.8]Difusión de software dañino
Herram. desarrollo/programación
[E.1]Errores de los usuarios
[E.4]Errores de configuración
[E.8]Difusión de software dañino
[E.15]Alteración de la información
[E.18]Destrucción de la información
[E.20]Vulnerabilidades de los programas(software)
[E.21]Errores de mantenimiento/actualización de programas(software)
[A.5]Suplantación de la identidad
[A.8]Difusión de software dañino
[A.11]Acceso no autorizado
[A.19]Revelación de información
[A.22]Manipulación de programas
Herram. adquisición y procesamiento de datos de investigación
[E.1]Errores de los usuarios
[E.4]Errores de configuración
[E.8]Difusión de software dañino
[E.15]Alteración de la información
[E.18]Destrucción de la información
[E.20]Vulnerabilidades de los programas(software)
[E.21]Errores de mantenimiento/actualización de programas(software)
[E.24]Caída del sistema por agotamiento de recursos
[A.5]Suplantación de la identidad
[A.6]Abuso de privilegios de acceso
[A.8]Difusión de software dañino
[A.11]Acceso no autorizado
[A.19]Revelación de información
[A.22]Manipulación de programas
Sistema operativo
[E.1]Errores de los usuarios
[E.8]Difusión de software dañino

[E.18]Destrucción de la información
[E.20]Vulnerabilidades de los programas(software)
[E.21]Errores de mantenimiento/actualización de programas(software)
[E.24]Caída del sistema por agotamiento de recursos
[A.4]Manipulación de los ficheros de configuración
[A.5]Suplantación de la identidad
[A.6]Abuso de privilegios de acceso
[A.8]Difusión de software dañino
[A.11]Acceso no autorizado
[A.19]Revelación de información
[A.22]Manipulación de programas
[SW] Equipos
Computadora workstation
[I.1]Fuego
[I.2]Daños por agua
[I.*]Desastres industriales
[I.3]Contaminación medioambiental
[I.5]Avería de origen físico o lógico
[I.6]Corte del suministro eléctrico
[I.7]Condiciones inadecuadas de temperatura o humedad
[E.1]Errores de los usuarios
[E.8]Difusión de software dañino
[A.6]Abuso de privilegios de acceso
[A.8]Difusión de software dañino
[A.11]Acceso no autorizado
[A.24]Denegación de servicio
[A.25]Robo de equipos
[COM] Comunicaciones
Router
[I.3]Contaminación medioambiental
[I.5]Avería de origen físico o lógico
[I.6]Corte del suministro eléctrico
[I.7]Condiciones inadecuadas de temperatura o humedad
[E.1]Errores de los usuarios
[E.4]Errores de configuración
[E.23]Errores de mantenimiento/actualización de equipos(hardware)
[E.24]Caída del sistema por agotamiento de recursos
[A.5]Suplantación de la identidad

[A.6]Abuso de privilegios de acceso
[A.11]Acceso no autorizado
[A.24]Denegación de servicio
[A.25]Robo de equipos
Switch
[I.3]Contaminación medioambiental
[I.5]Avería de origen físico o lógico
[I.6]Corte del suministro eléctrico
[I.7]Condiciones inadecuadas de temperatura o humedad
[E.1]Errores de los usuarios
[E.4]Errores de configuración
[E.23]Errores de mantenimiento/actualización de equipos(hardware)
[E.24]Caída del sistema por agotamiento de recursos
[A.5]Suplantación de la identidad
[A.6]Abuso de privilegios de acceso
[A.11]Acceso no autorizado
[A.24]Denegación de servicio
[A.25]Robo de equipos
Access point
[N.*.11]Calor extremo
[I.3]Contaminación medioambiental
[I.4]Contaminación electromagnética
[I.5]Avería de origen físico o lógico
[I.6]Corte del suministro eléctrico
[I.7]Condiciones inadecuadas de temperatura o humedad
[I.11]Emanaciones electromagnéticas
[E.1]Errores de los usuarios
[E.4]Errores de configuración
[E.23]Errores de mantenimiento/actualización de equipos(hardware)
[E.24]Caída del sistema por agotamiento de recursos
[A.5]Suplantación de la identidad
[A.6]Abuso de privilegios de acceso
[A.11]Acceso no autorizado
[A.24]Denegación de servicio
[A.25]Robo de equipos
[AUX]Elementos auxiliares
Dispositivo de almacenamiento externo
[N.2]Daños por agua

[I.1]Fuego
[I.*]Desastres industriales
[I.3]Contaminación medioambiental
[I.4]Contaminación electromagnética
[I.5]Avería de origen físico o lógico
[I.6]Corte del suministro eléctrico
[I.7]Condiciones inadecuadas de temperatura o humedad
[I.11]Emanaciones electromagnéticas
[E.8]Difusión de software dañino
[E.23]Errores de mantenimiento/actualización de equipos(hardware)
[A.6]Abuso de privilegios de acceso
[A.11]Acceso no autorizado
[A.24]Denegación de servicio
[A.25]Robo de equipos

Tabla A.5.: Amenazas identificadas - Equipamiento
Fuente: EAR/PILAR 7.1.10.

[L] Instalaciones
Laboratorio de investigación I
N.1] Fuego
[N.2] Daños por agua
[N.*.1] Tormentas
[N.*.2] Tormentas eléctricas
[N.*.4] Terremotos
[N.*.7] Deslizamientos del terreno
[N.*.11] Calor extremo
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación medioambiental
[I.4] Contaminación electromagnética
[I.8] Fallo de servicios de comunicaciones
A.6] Abuso de privilegios de acceso
Laboratorio de investigación II
[N.1] Fuego
[N.2] Daños por agua
[N.*.1] Tormentas

[N.*.2] Tormentas eléctricas
[N.*.4] Terremotos
[N.*.11] Calor extremo
[I.1] Fuego
[I.2] Daños por agua
[I.*] Desastres industriales
[I.3] Contaminación medioambiental
[I.4] Contaminación electromagnética
[I.8] Fallo de servicios de comunicaciones
[A.6] Abuso de privilegios de acceso

Tabla A.6.: Amenazas identificadas - Instalaciones
Fuente: EAR/PILAR 7.1.10.

[P] Personal
Investigadores
[E.8] Difusión de software dañino
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.28] Indisponibilidad del personal
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[A.19] Revelación de información
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)
Aux. Investigación
[E.8] Difusión de software dañino
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.28] Indisponibilidad del personal
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado

[A.15] Modificación de la información
[A.19] Revelación de información
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)
Ingenieros de soporte
[E.8] Difusión de software dañino
[E.15] Alteración de la información
[E.18] Destrucción de la información
[E.19] Fugas de información
[E.28] Indisponibilidad del personal
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.15] Modificación de la información
[A.19] Revelación de información
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social (picaresca)
Estudiantes vinculados
[E.8] Difusión de software dañino
[E.19] Fugas de información
[A.5] Suplantación de la identidad
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado

Tabla A.7.: Amenazas identificadas - Personal
Fuente: EAR/PILAR 7.1.10.

A.4. Valoración de las amenazas

[B] Activos esenciales	D	I	C
Base de datos	**A**	**A**	**A**
[E.15]Alteración de la información		A	
[E.18]Destrucción de la información	A		
[E.19]Fuga de la información			A
[A.5]Suplantación de identidad		M	A

[A.6]Abuso de privilegios de acceso	B	M	A
[A.11]Acceso no autorizado		B	A
[A.15]Modificación de la información		A	
[A.19]Revelación de información	B		M
Productos tecnológicos en producción	**A**	**A**	**A**
[E.15]Alteración de la información		A	
[E.18]Destrucción de la información	A		
[E.19]Fuga de la información		M	A
[A.5]Suplantación de identidad		B	M
[A.6]Abuso de privilegios de acceso	B	M	A
[A.11]Acceso no autorizado		B	A
[A.15]Modificación de la información		A	
[A.19]Revelación de información			B
Productos tecnológicos desarrollados	**A**	**A**	**A**
[E.15]Alteración de la información		A	
[E.18]Destrucción de la información	A		
[E.19]Fuga de la información		M	A
[A.5]Suplantación de identidad		B	M
[A.6]Abuso de privilegios de acceso	B	M	A
[A.11]Acceso no autorizado		B	A
[A.15]Modificación de la información		A	
[A.19]Revelación de información			M
Informes documentales	**A**	**A**	**A**
[E.15]Alteración de la información		A	
[E.18]Destrucción de la información	A		
[E.19]Fuga de la información		M	A
[A.5]Suplantación de identidad		B	M
[A.6]Abuso de privilegios de acceso	B	M	A
[A.11]Acceso no autorizado		B	A
[A.15]Modificación de la información		A	
[A.19]Revelación de información	B		M

Tabla A.8.: Amenazas valoradas - Servicios esenciales
Fuente: EAR/PILAR 7.1.10.

[ES] Servicios externos	D	I	C
Servicio de internet	**MA**	**M**	**M**
[I.8] Fallo de servicios de comunicaciones	MA		
[E.2] Errores del administrador del sistema / de la seguridad	M	M	B
[E.9] Errores de [re-]encaminamiento			B
[E.10] Errores de secuencia		B	
[E.15] Alteración de la información		B	
[E.18] Destrucción de la información	M	M	
[E.19] Fugas de información		B	M
[E.24] Caída del sistema por agotamiento de recursos	A		
[A.5] Suplantación de la identidad		M	M
[A.9] [Re-]encaminamiento de mensajes			B
[A.11] Acceso no autorizado		B	M
[A.14] Interceptación de información(escucha)			B
[A.15] Modificación de la información		M	
[A.19] Revelación de información			M
[A.24] Denegación de servicio	A		
Almacenamiento en la nube	**A**	**M**	**M**
[I.5] Avería de origen físico o lógico	B	B	
[I.9] Interrupción de otros servicios o suministros esenciales	A		
[E.1] Errores de los usuarios	M		
[E.15] Alteración de la información		B	
[E.18] Destrucción de la información	M		
[E.19] Fugas de información			B
[A.5] Suplantación de la identidad		M	M
[A.6] Abuso de privilegios de acceso			B
[A.15] Modificación de la información		M	
[A.19] Revelación de información			M
[A.24] Denegación de servicio	A		

Tabla A.9.: Amenazas valoradas - Servicios externos
Fuente: EAR/PILAR 7.1.10.

[E] Equipamiento	D	I	C
[SW] Aplicaciones			
Ofimática	**MA**	**M**	**M**
[E.8] Difusión de software dañino	M	M	M
[E.18] Destrucción de la información	M		
[E.20] Vulnera. de los programas(software)	B	B	M

[E.21] Errores de manten./actualización de programas(SW)	M	B	
[A.8] Difusión de software dañino	MA	M	M
Herram. desarrollo/programación	**MA**	**A**	**M**
[E.1] Errores de los usuarios	B	B	
[E.4] Errores de configuración	B		
[E.8] Difusión de software dañino	M	B	B
[E.15] Alteración de la información		B	
[E.18] Destrucción de la información		B	
[E.20] Vulnera. de los programas(SW)	B	B	B
[E.21] Errores de manten./actualización de programas(SW)	B		
[A.5] Suplantación de la identidad			B
[A.8] Difusión de software dañino	MA	A	M
[A.11] Acceso no autorizado			B
[A.19] Revelación de información			B
[A.22] Manipulación de programas	A	M	M
Herram. adquisición y procesamiento de datos de inves.	**MA**	**A**	**M**
[E.1] Errores de los usuarios	B		
[E.4] Errores de configuración	M	B	B
[E.8] Difusión de software dañino	M	M	B
[E.15] Alteración de la información		M	
[E.18] Destrucción de la información	B		
[E.20] Vulnera. de los programas(SW)	B	M	B
[E.21] Errores de manten./actualización de programas(SW)	B		
[E.24] Caída del sistema por agotamiento de recursos	B		
[A.5] Suplantación de la identidad			M
[A.6] Abuso de privilegios de acceso			M
[A.8] Difusión de software dañino	MA	A	M
[A.11] Acceso no autorizado			M
[A.19] Revelación de información			M
[A.22] Manipulación de programas	A	M	M
Sistema operativo	**MA**	**A**	**M**
[E.1] Errores de los usuarios	B		
[E.8] Difusión de software dañino	M	M	M
[E.18] Destrucción de la información	M		
[E.20] Vulnera. de los programas(SW)	B	B	B
[E.21] Errores de manten./actualización de programas(SW)	B		
[E.24] Caída del sistema por agotamiento de recursos	M		
[A.4] Manipulación de los ficheros de configuración	B		

[A.5] Suplantación de la identidad		B	M
[A.6] Abuso de privilegios de acceso		B	M
[A.8] Difusión de software dañino	MA	A	M
[A.11] Acceso no autorizado			M
[A.19] Revelación de información			M
[A.22] Manipulación de programas	A	M	M
[SW] Equipos			
Computadora workstation	**MA**	**M**	**A**
[I.1] Fuego	MA		
[I.2] Daños por agua	A		
[I.*] Desastres industriales	MA		
[I.3] Contaminación medioambiental	A		
[I.5] Avería de origen físico o lógico	A		
[I.6] Corte del suministro eléctrico	MA		
[I.7] Condiciones inadecuadas de temperatura o humedad	MA		
[E.1] Errores de los usuarios	B	B	
[E.8] Difusión de software dañino	B	B	
[A.6] Abuso de privilegios de acceso	M	M	M
[A.8] Difusión de software dañino	M	M	M
[A.11] Acceso no autorizado	M	M	M
[A.24] Denegación de servicio	MA		
[A.25] Robo de equipos	MA		A
[COM] Comunicaciones			
Router	**MA**	**B**	**M**
[I.3] Contaminación medioambiental	A		
[I.5] Avería de origen físico o lógico	A		
[I.6] Corte del suministro eléctrico	MA		
[I.7] Condiciones inadecuadas de temperatura o humedad	MA		
[E.1] Errores de los usuarios		B	
[E.4] Errores de configuración		B	
[E.23] Errores de manten./actualización de equipos(HW)	M		
[E.24] Caída del sistema por agotamiento de recursos	A		
[A.5] Suplantación de la identidad			B
[A.6] Abuso de privilegios de acceso		B	B
[A.11] Acceso no autorizado	M	B	M
[A.24] Denegación de servicio	MA		
[A.25] Robo de equipos	M		M
Switch	**MA**	**B**	**M**

[I.3] Contaminación medioambiental	A		
[I.5] Avería de origen físico o lógico	A		
[I.6] Corte del suministro eléctrico	MA		
[I.7] Condiciones inadecuadas de temperatura o humedad	MA		
[E.1] Errores de los usuarios		B	
[E.4] Errores de configuración		B	
[E.23] Errores de manten./actualización de equipos(HW)	M		
[E.24] Caída del sistema por agotamiento de recursos	A		
[A.5] Suplantación de la identidad			B
[A.6] Abuso de privilegios de acceso		B	B
[A.11] Acceso no autorizado	M	B	M
[A.24] Denegación de servicio	MA		
[A.25] Robo de equipos	M		M
Access point	**MA**	**B**	**M**
[N.*.11] Calor extremo	B		
[I.3] Contaminación medioambiental	A		
[I.4] Contaminación electromagnética	M		
[I.5] Avería de origen físico o lógico	A		
[I.6] Corte del suministro eléctrico	MA		
[I.7] Condiciones inadecuadas de temperatura o humedad	B		
[I.11] Emanaciones electromagnéticas	B		
[E.1] Errores de los usuarios		B	
[E.4] Errores de configuración		B	
[E.23] Errores de manten./actualización de equipos(HW)	M		
[E.24] Caída del sistema por agotamiento de recursos	A		
[A.5] Suplantación de la identidad			B
[A.6] Abuso de privilegios de acceso		B	B
[A.11] Acceso no autorizado	M	B	M
[A.24] Denegación de servicio	MA		
[A.25] Robo de equipos	M		M
[AUX] Elementos auxiliares			
Dispositivo de almacenamiento externo	**MA**	**M**	**M**
[N.2] Daños por agua	A		
[I.1] Fuego	MA		
[I.*] Desastres industriales	MA		
[I.3] Contaminación medioambiental	A		
[I.4] Contaminación electromagnética	M		
[I.5] Avería de origen físico o lógico	A		

[I.6] Corte del suministro eléctrico	MA		
[I.7] Condiciones inadecuadas de temperatura o humedad	MA		
[I.11] Emanaciones electromagnéticas	MA		
[E.8] Difusión de software dañino	B	M	
[E.23] Errores de manten./actualización de equipos(HW)	M	B	
[A.6] Abuso de privilegios de acceso	M	M	M
[A.11] Acceso no autorizado	M	M	M
[A.24] Denegación de servicio	MA		
[A.25] Robo de equipos	MA	M	M

Tabla A.10.: Amenazas valoradas - Equipamiento
Fuente: EAR/PILAR 7.1.10.

[L] Instalaciones	**D**	**I**	**C**
Laboratorio de investigación I	**MA**		
[N.1] Fuego	MA		
[N.2] Daños por agua	MA		
[N.*.1] Tormentas	B		
[N.*.2] Tormentas eléctricas	B		
[N.*.4] Terremotos	M		
[N.*.7] Deslizamientos del terreno	B		
[N.*.11] Calor extremo	B		
[I.1] Fuego	MA		
[I.2] Daños por agua	MA		
[I.*] Desastres industriales	MA		
[I.3] Contaminación medioambiental	M		
[I.4] Contaminación electromagnética	M		
[I.8] Fallo de servicios de comunicaciones	B		
[A.6] Abuso de privilegios de acceso	M		
Laboratorio de investigación II	**MA**		
[N.1] Fuego	MA		
[N.2] Daños por agua	MA		
[N.*.1] Tormentas	B		
[N.*.2] Tormentas eléctricas	B		
[N.*.4] Terremotos	M		
[N.*.11] Calor extremo	B		
[I.1] Fuego	MA		
[I.2] Daños por agua	MA		

[I.*] Desastres industriales	MA		
[I.3] Contaminación medioambiental	M		
[I.4] Contaminación electromagnética	M		
[I.8] Fallo de servicios de comunicaciones	B		
[A.6] Abuso de privilegios de acceso	M		

Tabla A.11.: Amenazas valoradas - Instalaciones
Fuente: EAR/PILAR 7.1.10.

[P] Personal	**D**	**I**	**C**
Investigadores	**A**	**M**	**M**
[E.8] Difusión de software dañino	M		B
[E.15] Alteración de la información		B	
[E.18] Destrucción de la información	B		
[E.19] Fugas de información			B
[E.28] Indisponibilidad del personal	M		
[A.5] Suplantación de la identidad			B
[A.6] Abuso de privilegios de acceso			B
[A.11] Acceso no autorizado			B
[A.15] Modificación de la información		M	
[A.19] Revelación de información			M
[A.28] Indisponibilidad del personal	A		
[A.29] Extorsión	M	B	M
[A.30] Ingeniería social (picaresca)	M	B	M
Aux. Investigación	**A**	**M**	**M**
[E.8] Difusión de software dañino	M		
[E.15] Alteración de la información		B	
[E.18] Destrucción de la información	B		
[E.19] Fugas de información			B
[E.28] Indisponibilidad del personal	M		
[A.5] Suplantación de la identidad			B
[A.6] Abuso de privilegios de acceso			B
[A.11] Acceso no autorizado			B
[A.15] Modificación de la información		M	
[A.19] Revelación de información			M
[A.28] Indisponibilidad del personal	A		
[A.29] Extorsión	M	M	M
[A.30] Ingeniería social (picaresca)	M	M	M

Ingenieros de soporte	**A**	**M**	**M**
[E.8] Difusión de software dañino	M		
[E.15] Alteración de la información		B	
[E.18] Destrucción de la información	B		
[E.19] Fugas de información			B
[E.28] Indisponibilidad del personal	A		
[A.5] Suplantación de la identidad			B
[A.6] Abuso de privilegios de acceso			B
[A.11] Acceso no autorizado			B
[A.15] Modificación de la información		M	
[A.19] Revelación de información			M
[A.28] Indisponibilidad del personal	A		
[A.29] Extorsión	A	M	M
[A.30] Ingeniería social (picaresca)	A	M	M
Estudiantes vinculados	**M**		**B**
[E.8] Difusión de software dañino	M		
[E.19] Fugas de información			B
[A.5] Suplantación de la identidad			B
[A.6] Abuso de privilegios de acceso			B
[A.11] Acceso no autorizado			B

Tabla A.12.: Amenazas valoradas - Personal
Fuente: EAR/PILAR 7.1.10.

A.5. Identificación de salvaguardas

Salvaguardas
[IA] Identificación y autenticación
[IA.1] Se dispone de normativa de identificación y autenticación
[IA.3] Identificación de los usuarios
[IA.4] Gestión de la identificación y autenticación de usuario
[AC] Control de acceso lógico
[AC.1] Gestión de privilegios
[AC.2] Imposición del control de acceso
[D] Protección de la Información
[D.1] Se dispone de un inventario de activos de información
[SW] Protección de las Aplicaciones Informáticas (SW)
[SW.start] Puesta en producción

[SW.op] Explotación / Producción
[HW] Protección de los Equipos Informáticos (HW)
[HW.cont] Aseguramiento de la disponibilidad
[HW.7] Instalación
[HW.op] Operación
[HW.CM] Cambios (actualizaciones y mantenimiento)
[AUX] Elementos Auxiliares
[AUX.1] Se dispone de un inventario de equipamiento auxiliar
[AUX.AC] Climatización
[AUX.wires] Protección del cableado
[L] Procedimiento de las instalaciones
[L.1] Se dispone de normativa de seguridad
[L.2] Se dispone de un inventario de instalaciones
[L.design] Diseño
[L.6] Protección frente a desastres
[PS] Gestión del Personal
[PS.3] Relación de personal
[PS.4] Puestos de trabajo
[PS.6] Cambio de puesto de trabajo
[PS.8] Procedimientos de prevención y reacción
[PS.cont] Aseguramiento de la disponibilidad
[IR] Gestión de incidentes
[IR.1] Se dispone de normativa de actuación para la gestión de incidentes
[IR.2] Se dispone de procedimientos para la gestión de incidentes
[IR.4] Gestión del incidente
[IR.5] Cooperación con otras organizaciones
[IR.6] Comunicación de los incidentes de seguridad
[IR.7] Comunicación de las deficiencias de seguridad
[IR.8] Comunicación de los fallos del software
[IR.a] Los fallos y las medidas correctoras se registran y se revisan
[IR.e] Se toman medidas para prevenir la repetición
[tools] Herramientas de seguridad
[tools.AV] Herramienta contra código dañino
[V] Gestión de vulnerabilidades
[V.2] Se han previsto mecanismos para estar informados de vulnerabilidades ...
[tools.V] Herram. de análisis de vulnerabilidades
[V.4] Se analiza el impacto potencial (estimación de riesgos)
[V.5] Pruebas de penetración

[V.7] Reparación de las vulnerabilidades detectadas
[G] Organización
[G.1] Organización interna
[G.2] Documentación técnica (componentes)
[E] Relaciones Externas
[E.1] Acuerdos para intercambio de información y software
[E.2] Acceso externo

Tabla A.13.: Salvaguardas identificadas
Fuente: EAR/PILAR 7.1.10.

A.6. Valoración de las salvaguardas

Salvaguardas	Valor
[IA] Identificación y autenticación	**L0-L2**
[IA.1] Se dispone de normativa de identificación y autenticación	L1
[IA.3] Identificación de los usuarios	L1-L2
[IA.4] Gestión de la identificación y autenticación de usuario	L0-L1
[AC] Control de acceso lógico	**L0-L3**
[AC.1] Gestión de privilegios	L0-L2
[AC.2] Imposición del control de acceso	L0-L3
[D] Protección de la Información	**L0-L1**
[D.1] Se dispone de un inventario de activos de información	L0-L1
[SW] Protección de las Aplicaciones Informáticas (SW)	**L0-L3**
[SW.start] Puesta en producción	L0-L3
[SW.op] Explotación / Producción	L0-L2
[HW] Protección de los Equipos Informáticos (HW)	**L0-L2**
[HW.cont] Aseguramiento de la disponibilidad	L0-L1
[HW.7] Instalación	L0-L1
[HW.op] Operación	L0-L2
[HW.CM] Cambios (actualizaciones y mantenimiento)	L0-L2
[AUX] Elementos Auxiliares	**L0-L3**
[AUX.1] Se dispone de un inventario de equipamiento auxiliar	L0-L3
[AUX.AC] Climatización	L0-L2
[AUX.wires] Protección del cableado	L0-L3
[L] Procedimiento de las instalaciones	**L0-L3**
[L.1] Se dispone de normativa de seguridad	L2-L3
[L.2] Se dispone de un inventario de instalaciones	L1-L3

[L.design] Diseño	L0-L2
[L.6] Protección frente a desastres	L1-L3
[PS] Gestión del Personal	**L0-L3**
[PS.3] Relación de personal	L2-L3
[PS.4] Puestos de trabajo	L0-L3
[PS.6] Cambio de puesto de trabajo	L1
[PS.8] Procedimientos de prevención y reacción	L0
[PS.cont] Aseguramiento de la disponibilidad	L1
[IR] Gestión de incidentes	**L0-L2**
[IR.1] Se dispone de normativa de actuación para la gestión de incidentes	L0
[IR.2] Se dispone de procedimientos para la gestión de incidentes	L0
[IR.4] Gestión del incidente	L1
[IR.5] Cooperación con otras organizaciones	L1
[IR.6] Comunicación de los incidentes de seguridad	L1
[IR.7] Comunicación de las deficiencias de seguridad	L1
[IR.8] Comunicación de los fallos del software	L2
[IR.a] Los fallos y las medidas correctoras se registran y se revisan	L1
[IR.e] Se toman medidas para prevenir la repetición	L1
[tools] Herramientas de seguridad	**L0-L1**
[tools.AV] Herramienta contra código dañino	L0-L1
[V] Gestión de vulnerabilidades	**L0-L1**
[V.2] Se han previsto mecanismos para estar informados de vulnerabilidades..	L1
[tools.V] Herram. de análisis de vulnerabilidades	L1
[V.4] Se analiza el impacto potencial (estimación de riesgos)	L0
[V.5] Pruebas de penetración	L1
[V.7] Reparación de las vulnerabilidades detectadas	L1
[G] Organización	**L0-L1**
[G.1] Organización interna	L0-L1
[G.2] Documentación técnica (componentes)	L0-l1
[E] Relaciones Externas	**L0-L1**
[E.1] Acuerdos para intercambio de información y software	L0-L1
[E.2] Acceso externo	L0-L1

Tabla A.14.: Salvaguardas valoradas
Fuente: EAR/PILAR 7.1.10.

A.7. Impacto y Riesgo

A.7.1. Valores acumulados

Impacto

Activos	Inicial			Con salvaguarda		
	[D]	[I]	[C]	[D]	[I]	[C]
	[8]	**[7]**	**[6]**	**[8]**	**[7]**	**[6]**
[B] Activos esenciales	**[7]**	**[7]**	**[6]**	**[7]**	**[7]**	**[6]**
[B-01] Base de datos	[7]	[7]	[6]	[7]	[7]	[6]
[B-02] Productos Tecnológicos en producción	[7]	[7]	[6]	[7]	[6]	[5]
[B-03] Productos Tecnológicos desarrollados	[7]	[6]	[4]	[7]	[5]	[3]
[B-04] Informes documentales	[7]	[7]	[6]	[7]	[7]	[6]
[IS] Servicios internos	**[5]**	**[0]**	**[4]**	**[5]**	**[0]**	**[4]**
[IS-01] Servicio de internet	[5]	[0]	[4]	[5]	[0]	[4]
[IS-02] Almacenamiento en la nube	[4]	[0]	[0]	[4]	[0]	[0]
[E] Equipamiento	**[8]**	**[6]**	**[6]**	**[8]**	**[6]**	**[6]**
[SW] Aplicaciones	**[8]**	**[6]**	**[4]**	**[8]**	**[6]**	**[4]**
[SW-01] Ofimática	[7]	[4]	[4]	[7]	[4]	[4]
[SW-02] Herram. desarrollo / programación	[8]	[6]	[4]	[8]	[6]	[4]
[SW-03] Herram. adquisición y procesamiento de datos de investigación	[7]	[6]	[4]	[7]	[6]	[4]
[SW-04] Sistema operativo	[7]	[6]	[4]	[7]	[6]	[4]
[HW] Equipos	**[7]**	**[4]**	**[6]**	**[6]**	**[4]**	**[6]**
[HW-01] PC Workstation	[7]	[4]	[6]	[6]	[4]	[6]
[COM] Comunicaciones	**[5]**	**[0]**	**[3]**	**[4]**	**[0]**	**[3]**
[COM-01] Router	[5]	[0]	[3]	[4]	[0]	[3]
[COM-02] Swirch	[5]	[0]	[3]	[4]	[0]	[3]
[COM-03] Access point	[5]	[0]	[3]	[4]	[0]	[3]
[AUX] Elementos auxiliares	**[8]**	**[4]**	**[4]**	**[7]**	**[4]**	**[4]**
[AUX-01] Dispositivo almacenamiento externo	[8]	[4]	[4]	[7]	[4]	[4]
[L] Instalaciones	**[7]**			**[6]**		
[L-01] Laboratorio investigación I	[7]			[6]		
[L-02] Laboratorio investigación II	[7]			[6]		
[P] Personal	**[6]**	**[4]**	**[4]**	**[6]**	**[4]**	**[4]**
[P-01] Investigadores	[6]	[3]	[3]	[6]	[3]	[3]
[P-02] Aux. investigación	[6]	[4]	[4]	[6]	[4]	[4]
[P-03] Ingenieros de soporte	[6]	[4]	[4]	[6]	[4]	[4]
[P-04] Estudiantes vinculados	[4]		[1]	[4]		[1]

Tabla A.15.: Impacto acumulado
Fuente: EAR/PILAR 7.1.10.

Riesgo

Activos	Inicial			Con salvaguarda		
	[D]	[I]	[C]	[D]	[I]	[C]
	{7,1}	**{6,5}**	**{6,8}**	**{6,6}**	**{5,8}**	**{6,2}**
[B] Activos esenciales	**{7,1}**	**{6,5}**	**{6,8}**	**{6,6}**	**{5,8}**	**{6,2}**
[B-01] Base de datos	{5,4}	{6,4}	{6,8}	{5,1}	{5,8}	{6,2}
[B-02] Productos Tecnológicos en producción	{5,4}	{6,4}	{6,8}	{4,8}	{5,6}	{6,0}
[B-03] Productos Tecnológicos desarrollados	{7,1}	{6,5}	{5,6}	{6,6}	{5,7}	{4,8}
[B-04] Informes documentales	{5,4}	{6,4}	{6,8}	{5,1}	{5,8}	{6,2}
[IS] Servicios internos	**{4,8}**	**{1,4}**	**{3,8}**	**{4,5}**	**{1,1}**	**{3,5}**
[IS-01] Servicio de internet	{4,8}	{1,4}	{3,8}	{4,5}	{1,1}	{3,5}
[IS-02] Almacenamiento en la nube	{3,9}	{0,98}	{0,98}	{3,6}	{0,92}	0,92}
[E] Equipamiento	**{6,4}**	**{5,0}**	**{5,6}**	**{6,0}**	**{4,6}**	**{4,7}**
[SW] Aplicaciones	**{6,1}**	**{5,0}**	**{5,6}**	**{5,7}**	**{4,6}**	**{4,7}**
[SW-01] Ofimática	{5,5}	{3,8}	{3,8}	{5,1}	{3,4}	{3,3}
[SW-02] Herram. desarrollo / programación	{6,1}	{5,0}	{3,9}	{5,7}	{4,6}	{3,3}
[SW-03] Herram. adquisición y procesamiento de datos de investigación	{5,5}	{5,0}	{5,6}	{5,1}	{4,6}	{4,7}
[SW-04] Sistema operativo	{5,5}	{5,0}	{5,6}	{5,1}	{4,6}	{4,7}
[HW] Equipos	**{5,8}**	**{3,9}**	**{5,0}**	**{5,4}**	**{3,5}**	**{4,6}**
[HW-01] PC Workstation	{5,8}	{3,9}	{5,0}	{5,4}	{3,5}	{4,6}
[COM] Comunicaciones	**{4,7}**	**{0,73}**	**{3,3}**	**{4,2}**	**{0,65}**	**{2,9}**
[COM-01] Router	{4,7}	{0,73}	{3,3}	{4,2}	{0,65}	{2,9}
[COM-02] Swirch	{4,7}	{0,73}	{3,3}	{4,2}	{0,65}	{2,9}
[COM-03] Access point	{4,7}	{0,73}	{3,3}	{4,2}	{0,65}	{2,9}
[AUX] Elementos auxiliares	**{6,4}**	**{3,9}**	**{3,9}**	**{6,0}**	**{3,5}**	**{3,5}**
[AUX-01] Dispositivo almacenamiento externo	{6,4}	{3,9}	{3,9}	{6,0}	{3,5}	{3,5}
[L] Instalaciones	**{5,1}**			**{4,4}**		
[L-01] Laboratorio investigación I	{5,1}			{4,4}		
[L-02] Laboratorio investigación II	{5,1}			{4,4}		
[P] Personal	**{5,0}**	**{3,7}**	**{4,1}**	**{4,7}**	**{3,5}**	**{3,9}**
[P-01] Investigadores	{4,6}	{3,3}	{4,1}	{4,2}	{3,0}	{3,9}
[P-02] Aux. investigación	{4,6}	{3,7}	{4,1}	{4,2}	{3,5}	{3,9}
[P-03] Ingenieros de soporte	{5,0}	{3,7}	{4,1}	{4,7}	{3,5}	{3,9}
[P-04] Estudiantes vinculados	{3,8}		{2,8}	{3,5}		{2,5}

Tabla A.16.: Riesgo acumulado
Fuente: EAR/PILAR 7.1.10.

A.7.2. Valores repercutidos

Impacto

Activos	Inicial			Con salvaguarda		
	[D]	[I]	[C]	[D]	[I]	[C]
	[8]	[7]	[6]	[8]	[7]	[6]
[B-01] Base de datos	[7]	[7]	[4]	[7]	[7]	[4]
[B-02] Productos Tecnológicos en producción	[7]	[6]	[4]	[7]	[6]	[4]
[B-03] Productos Tecnológicos desarrollados	[7]	[6]	[4]	[7]	[6]	[4]
[B-04] Informes documentales	[3]	[6]	[4]	[3]	[6]	[4]
[IS-01] Servicio de internet	[3]	[1]	[6]	[3]	[1]	[6]
[IS-02] Almacenamiento en la nube	[5]	[2]	[2]	[5]	[2]	[2]
[SW-01] Ofimática	[1]	[2]	[3]	[1]	[2]	[2]
[SW-02] Herram. desarrollo / programación	[8]	[4]	[2]	[8]	[4]	[2]
[SW-03] Herram. adquisición y procesamiento de datos de investigación	[4]	[3]	[4]	[4]	[3]	[4]
[SW-04] Sistema operativo	[1]	[3]	[3]	[1]	[3]	[3]
[HW-01] PC Workstation	[7]	[2]	[2]	[7]	[2]	[2]
[COM-01] Router	[3]	[0]	[1]	[3]	[0]	[1]
[COM-02] Swirch	[3]	[0]	[1]	[3]	[0]	[1]
[COM-03] Access point	[2]	[0]	[1]	[2]	[0]	[1]
[AUX-01] Dispositivo almacenamiento externo	[8]	[6]	[6]	[7]	[6]	[6]
[L-01] Laboratorio investigación I	[4]	[2]	[2]	[4]	[2]	[2]
[L-02] Laboratorio investigación II	[4]	[2]	[2]	[4]	[2]	[2]
[P-01] Investigadores	[7]	[6]	[4]	[7]	[6]	[4]
[P-02] Aux. investigación	[7]	[4]	[2]	[7]	[4]	[2]
[P-03] Ingenieros de soporte	[6]	[4]	[2]	[6]	[4]	[2]
[P-04] Estudiantes vinculados	[3]	[4]	[2]	[3]	[4]	[2]

Tabla A.17.: Impacto acumulado
Fuente: EAR/PILAR 7.1.10.

Riesgo

Activos	Inicial			Con salvaguarda		
	[D]	[I]	[C]	[D]	[I]	[C]
	{7,1}	**{6,4}**	**{6,5}**	**{6,6}**	**{5,8}**	**{6,2}**
[B-01] Base de datos	{5,4}	{6,4}	{5,6}	{5,1}	{5,8}	{5,0}
[B-02] Productos Tecnológicos en producción	{5,4}	{5,8}	{5,6}	{5,1}	{5,2}	{5,0}
[B-03] Productos Tecnológicos desarrollados	{7,1}	{6,5}	{5,6}	{6,6}	{5,7}	{5,0}
[B-04] Informes documentales	{3,0}	{5,8}	{5,6}	{2,7}	{5,2}	{5,0}
[IS-01] Servicio de internet	{3,6}	{2,9}	{6,8}	{3,3}	{2,3}	{6,2}
[IS-02] Almacenamiento en la nube	{4,8}	{3,5}	{4,4}	{4,5}	{2,8}	{3,8}
[SW-01] Ofimática	{1,9}	{3,5}	{5,0}	{1,6}	{2,8}	{4,4}
[SW-02] Herram. desarrollo / programación	{6,1}	{4,7}	{4,4}	{5,7}	{4,0}	{3,8}
[SW-03] Herram. adquisición y procesamiento de datos de investigación	{3,7}	{4,1}	{5,6}	{3,4}	{3,4}	{5,0}
[SW-04] Sistema operativo	{1,9}	{4,1}	{5,0}	{1,6}	{3,4}	{4,4}
[HW-01] PC Workstation	{5,8}	{3,5}	{4,4}	{5,4}	{2,8}	{3,8}
[COM-01] Router	{3,6}	{2,3}	{3,9}	{3,3}	{1,7}	{3,2}
[COM-02] Swirch	{3,6}	{2,3}	{3,9}	{3,3}	{1,7}	{3,2}
[COM-03] Access point	{3,1}	{2,3}	{3,9}	{2,8}	{1,7}	{3,2}
[AUX-01] Dispositivo almacenamiento externo	{6,4}	{5,8}	{6,8}	{6,0}	{5,2}	{6,2}
[L-01] Laboratorio investigación I	{4,1}	{3,5}	{4,4}	{3,7}	{2,8}	{3,8}
[L-02] Laboratorio investigación II	{4,1}	{3,5}	{4,4}	{3,7}	{2,8}	{3,8}
[P-01] Investigadores	{5,8}	{5,8}	{5,6}	{5,4}	{5,2}	{5,0}
[P-02] Aux. investigación	{5,8}	{4,7}	{4,4}	{5,4}	{4,0}	{3,8}
[P-03] Ingenieros de soporte	{5,2}	{4,7}	{4,4}	{4,8}	{4,0}	{3,8}
[P-04] Estudiantes vinculados	{3,5}	{4,7}	{4,4}	{3,1}	{4,0}	{3,8}

Tabla A.18.: Impacto acumulado
Fuente: EAR/PILAR 7.1.10.

B. Anexo: Roles y responsabilidades de la seguridad de la información

La seguridad dentro del entorno de investigación es esencial para salvaguardar la confidencialidad , integridad y privacidad de la información que se maneja al entorno de esta, es por ello, que es necesario de contar con un grupo de profesionales competentes para abordar esta necesidad.

B.1. Identificación de los responsables

La alta dirección deberá de identificar las necesidades del entorno de investigación en resguardar la seguridad de la información, para ello, inicialmente deberá de identificar el perfil del personal competente en cuanto a la seguridad y privacidad de la información, luego deberá establecer a los responsables, sus roles y funciones, sin ocasionar conflicto de intereses o perjuicio alguno al entorno de investigación.
Como resultado, la alta dirección deberá liderar un equipo de trabajo junto a los responsables de la seguridad y privacidad de la información dentro del entorno de investigación, los mismos que deberán tomar acciones, elaborar la documentación correspondiente y desarrollar estrategias para el cumplimiento del modelo de seguridad de la información.

B.2. Perfiles y responsabilidades

Para lograr el cumplimiento del objetivo y alcance del modelo de seguridad, así como también el correcto desempeño de los integrantes del equipo de seguridad y privacidad de las información de debe de contar con los siguientes roles y funciones.

B.2.1. Dirección general o Alta dirección

Es el impulsor y responsable de dirigir la implementación del modelo de seguridad, para ello, debe estar comprometido, tomar las decisiones que correspondan, gestionar la asignación de los recursos necesarios y designar los responsables en la gestión y cumplimiento del objetivo, alcance y metas del modelo de seguridad de la información. En ese sentido, sus responsabilidades son:

- Aprobar los lineamientos estratégicos en materia de seguridad de la información, garantizando la toma de decisiones orientadas al cumplimiento de las estrategias definidas.
- Liderar y apoyar continuamente la aplicación del Modelo de Seguridad de la Información dentro del entorno de investigación.
- Establecer y verificar el cumplimiento de las funciones y responsabilidades asignadas en el cumplimiento del modelo de seguridad de la información.
- Suministrar los recursos necesarios para la implementación del Modelo de seguridad de la información dentro del entorno de investigación.
- Suministrar los recursos necesarios y dar las facilidades en el entrenamiento y capacitación del personal del entorno de investigación.
- Aplicar los procesos disciplinarios correspondiente, establecidos por el comité de seguridad de información.

B.2.2. Responsable de la seguridad de la información

Es el responsable y líder del modelo de seguridad, designado por la alta dirección para dirigir estratégica y operativamente las metas establecidas en el modelo de seguridad. En ese sentido, sus responsabilidades son:

- Aplicar sus conocimientos y habilidades profesionales usando las herramientas y técnicas a su disposición en materia de seguridad de la información con la finalidad de cumplir o superar las expectativas asignadas.
- Identificar los problemas de seguridad existentes entre el entorno de investigación frente al modelo de seguridad de a información y desarrollar acciones correctivas y de mejoras en las estrategias del modelo de seguridad de la información.
- Desarrollar periódicamente análisis de riesgos a los activos de información y definir los tratamientos de los riesgos y amenazas según necesidades del entorno de investigación.
- Planificar, evaluar, coordinar y ejecutar junto a su equipo de trabajo el cumplimiento de las metas establecidas en el ciclo de operación para el cumplimiento del objetivo y alcance del modelo de seguridad.
- Garantizar el manteniendo preventivo y correctivo, resguardo y protección de los activos de información.
- Reportar a la brevedad posible las incidencias y violación de la seguridad y privacidad de la información.

- Desarrollar propuestas de innovación y mejoras en la seguridad y privacidad de la información.
- Programar y liderar las reuniones de trabajo, informativas y de coordinación concerniente al modelo de seguridad de la información.

B.2.3. Comité de seguridad y privacidad de la información

Es un grupo integrado por jefes o responsables de las áreas de un entorno de investigación establecido y dirigido por la alta dirección en coordinación con el responsable de la seguridad de la información. En ese sentido, sus funciones son:

- Aprobar, revisar, modificar o actualizar las políticas, procedimientos, controles y demás documentos vinculados a la Seguridad de la Información.
- Velar por el cumplimiento de las políticas, procedimientos, controles y demás documentos vinculados a la Seguridad de la Información dentro del entorno de investigación.
- Definir y aprobar los procesos disciplinarios según legislación vigente para los incidentes de seguridad de acuerdo a la responsabilidad por el incumplimiento u omisión en la funciones asignadas a los funcionarios y personal del entorno de investigación.
- Tomar conocimiento, monitorizar y supervisar las investigaciones acerca de los incidentes de seguridad de la información, producidos dentro del entorno de investigación.
- Proponer y diseñar proyectos tecnológicos orientados a la mejora y aplicación de Seguridad de la Información dentro del entorno de investigación.
- Fomentar la difusión de las políticas y procedimientos de la Seguridad de la Información dentro de un entorno de investigación.
- Elaborar informes e indicadores acerca de la aplicación y cumplimiento de la Seguridad de la Información dentro del entorno de investigación.
- Convocar a reuniones de trabajo, informativas, de coordinación y de urgencia concerniente al modelo de seguridad de la información.

B.2.4. Propietario del activo

Es el Jefe o responsable de área designado por la alta dirección para gestionar el cumplimiento de la políticas de seguridad y privacidad de la información en los activos de información que se encuentren bajo su responsabilidad y deberá velar que se preserve la confidencialidad, integridad y privacidad de los mismos. En ese sentido, sus responsabilidades son:

- Gestionar oportunamente con el responsable de la seguridad de la información, la implementación de los controles definidos por el modelo de seguridad a fin de salvaguardar la seguridad y privacidad de la información.
- Velar el cumplimiento de la política de uso aceptable del activo.
- Reporte adecuado y oportuno de cualquier modificación, actualización y configuración realizada sobre el activo de información a su cargo.
- Reportar inmediatamente al responsable de la seguridad de la información, las incidencias de seguridad y privacidad de la información en los activos a su cargo.

B.2.5. Custodio del activo

Es el encargado de monitorizar, administrar y operar correctamente los activos de información que se encuentren a su cargo.

- Aplicar los controles de seguridad establecidos por el propietario del activo.
- Velar el cumplimiento de la política de uso adecuado del activo.

B.2.6. Usuario del activo

Es el usuario final y le es asignado uno o mas activos para el desarrollo de sus actividades diarias según sus funciones. En ese sentido, sus responsabilidades son:

- Cumplir con la política de uso adecuado del activo.
- Reportar inmediatamente al propietario del activo las incidencias de seguridad y privacidad de la información.

C. Controles de seguridad de la información

Dominios de seguridad		Objetivos		Controles de seguridad		Amenazas mitigada
A.5	Políticas de Seguridad	A.5.1	Orientación de la Dirección para la Gestión de la seguridad de la información	A.5.1.1	Políticas para la seguridad de la información	[A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.15] Modificación de la información [A.22] Manipulación de programas [E.15] Alteración de la información [E.18] Destrucción de la información
				A.5.1.2	Revisión de las políticas para la seguridad de la información	
A.6	Organización de la Seguridad de la Información	A.6.1	Organización Interna	A.6.1.1	Roles y Responsabilidad para la seguridad de la Información	
		A.6.2	Dispositivos móviles y teletrabajo	A.6.2.1	Política de dispositivos móviles	[A.8] Difusión de software dañino [A.11] Acceso no autorizado
				A.6.2.2	Teletrabajo	[A.11] Acceso no autorizado
A.7	Seguridad de los Recursos Humanos	A.7.1	Antes de asumir el empleo	A.7.1.1	Selección	
				A.7.1.2	Términos y condiciones de empleo	[A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.15] Modificación de la información [A.22] Manipulación de programas
		A.7.2	Durante la ejecución del empleo	A.7.2.1	Responsabilidades de la dirección	
				A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	[A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.15] Modificación de la información [A.22] Manipulación de programas [E.15] Alteración de la información [E.18] Destrucción de la información
		A.7.3	Terminación y cambio de empleo	A.7.3.1	Terminación o cambio de responsabilidades de empleo	[A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado
A.8	Gestión de Activos	A.8.1	Responsabilidad de los activos	A.8.1.1	Inventario de Activos	
				A.8.1.2	Propiedad de los activos	[A.11] Acceso no autorizado
				A.8.1.3	Uso aceptable de los activos	[A.8] Difusión de software dañino [A.15] Modificación de la información [A.22] Manipulación de programas [E.15] Alteración de la información [E.18] Destrucción de la información
		A.8.2	Clasificación de la información	A.8.2.1	Clasificación de la información	[A.11] Acceso no autorizado
				A.8.2.2	Etiquetado de la información	[A.11] Acceso no autorizado [E.15] Alteración de la información [E.18] Destrucción de la información
				A.8.2.3	Manejo de activos	[A.15] Modificación de la información [E.15] Alteración de la información [E.18] Destrucción de la información
		A.8.3	Manejo de medios	A.8.3.1	Gestión de medios removibles	[A.8] Difusión de software dañino [A.11] Acceso no autorizado
				A.8.3.2	Disposición de los medios	
				A.8.3.3	Transferencia de medios físicos	[A.11] Acceso no autorizado [A.15] Modificación de la información

Dominios de seguridad		Objetivos		Controles de seguridad		Amenazas abordadas
A.9	Control de acceso	A.9.1	Requisitos del negocio para el control de acceso	A.9.1.1	Política de control de acceso	[A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.15] Modificación de la información [A.22] Manipulación de programas
		A.9.2	Gestión de acceso de usuario	A.9.2.1	Registro y cancelación del registro de usuarios	[A.11] Acceso no autorizado
				A.9.2.2	Suministro de acceso de usuarios	[A.5] Suplantación de la identidad
				A.9.2.3	Gestión de derechos de acceso privilegiado	[A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado
				A.9.2.6	Retiro o ajuste de los de derechos de acceso	[A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado
		A.9.3	Responsabilidades de usuario	A.9.3.1	Uso de información de autenticación secreta	[A.5] Suplantación de la identidad
		A.9.4	Control de acceso al sistemas y aplicaciones	A.9.4.1	Restricciones de acceso a la información	[A.11] Acceso no autorizado [A.15] Modificación de la información [E.15] Alteración de la información [E.18] Destrucción de la información
				A.9.4.2	Procedimiento de ingreso seguro	[A.5] Suplantación de la identidad
				A.9.4.4	Uso de programas utilitarios privilegiados	[A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.22] Manipulación de programas
A.10	Criptografía	A.10.1	Controles criptográficos	A.10.1.1	Política sobre el uso de controles criptográficos	[A.11] Acceso no autorizado [A.15] Modificación de la información [E.15] Alteración de la información
A.11	Seguridad física y del entorno	A.11.1	Áreas seguras	A.11.1.1	Perímetro de seguridad física	
				A.11.1.3	Seguridad de oficinas, recintos e instalaciones	
		A.11.2	Equipos	A.11.2.2	Servicios de suministro	
				A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	
				A.11.2.7	Disposición segura o reutilización de equipos	
				A.11.2.8	Equipo de usuario desatendido	[A.11] Acceso no autorizado
A.12	Seguridad en las operaciones	A.12.1	Procedimientos operacionales y responsabilidades	A.12.1.1	Procedimientos de operación documentados	[A.5] Suplantación de la identidad [A.11] Acceso no autorizado
		A.12.2	Protección contra códigos maliciosos	A.12.2.1	Controles contra códigos maliciosos	[A.8] Difusión de software dañino
		A.12.3	Copias de respaldo	A.12.3.1	Respaldo de la información	[A.15] Modificación de la información [E.15] Alteración de la información [E.18] Destrucción de la información
		A.12.4	Registro y seguimiento	A.12.4.1	Registro de eventos	[A.11] Acceso no autorizado
				A.12.4.2	Protección de la información de registros	[A.15] Modificación de la información
				A.12.4.3	Registros de administración y operador	[A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado
				A.12.4.4	Sincronización del relojes	
		A.12.5	Control de software operacional	A.12.5.1	Instalación de software en sistemas operativos	[A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.22] Manipulación de programas
		A.12.6	Gestión de la vulnerabilidad técnica	A.12.6.1	Gestión de las vulnerabilidades técnicas	[A.5] Suplantación de la identidad [A.11] Acceso no autorizado
				A.12.6.2	Restricciones sobre la instalación de software	[A.8] Difusión de software dañino [A.11] Acceso no autorizado
		A.12.7	Consideraciones sobre auditorías de sistemas de información	A.12.7.1	Controles de auditoría de sistemas de información	

Dominios de seguridad		Objetivos		Controles de seguridad		Amenazas abordadas
A.13	Seguridad de las comunicaciones	A.13.2	Transferencia de información	A.13.2.1	Políticas y procedimientos de transferencia de información	[A.15] Modificación de la información [E.15] Alteración de la información [E.18] Destrucción de la información
				A.13.2.2	Acuerdos sobre transferencia de información	[A.15] Modificación de la información [E.15] Alteración de la información [E.18] Destrucción de la información
				A.13.2.3	Mensajería electrónica	[A.5] Suplantación de la identidad
				A.13.2.4	Acuerdos de confidencialidad o de no divulgación	[A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado
A.14	Adquisición, desarrollo y mantenimiento de sistemas	A.14.3	Datos de prueba	A.14.3.1	Protección de datos de prueba	[A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado [A.15] Modificación de la información [A.22] Manipulación de programas [E.15] Alteración de la información [E.18] Destrucción de la información
A.15	Relaciones con los proveedores	A.15.1	Seguridad de la información en las relaciones con los proveedores	A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	[A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.11] Acceso no autorizado
A.16	Gestión de incidentes de seguridad de la información	A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	A.16.1.1	Responsabilidades y procedimientos	[A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.15] Modificación de la información [A.22] Manipulación de programas [E.15] Alteración de la información [E.18] Destrucción de la información
				A.16.1.2	Reporte de eventos de seguridad de la información	[A.6] Abuso de privilegios de acceso
A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio	A.17.1	Continuidad de seguridad de la información	A.17.1.1	Planificación de la continuidad de la seguridad de la información	[A.15] Modificación de la información [E.15] Alteración de la información [E.18] Destrucción de la información
A.18	Cumplimiento	A.18.1	Cumplimiento de requisitos legales y contractuales	A.18.1.1	Identificación de la legislación aplicable y requerimientos contractuales	[A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.15] Modificación de la información [A.22] Manipulación de programas
				A.18.1.2	Derechos de propiedad intelectual	[A.15] Modificación de la información
		A.18.2	Revisiones de seguridad de la información	A.18.2.2	Cumplimiento con las políticas y normas de seguridad	[A.5] Suplantación de la identidad [A.6] Abuso de privilegios de acceso [A.8] Difusión de software dañino [A.11] Acceso no autorizado [A.15] Modificación de la información [A.22] Manipulación de programas [E.15] Alteración de la información [E.18] Destrucción de la información
				A.18.2.3	Revisión del cumplimiento técnico	

Tabla C.1.: Controles seleccionado Anexo A - 27001:2013
Fuente: Elaboración propia

D. Anexo: Políticas generales de seguridad y privacidad de la información

Logo institución	**Políticas de seguridad y privacidad de la información.**	**Código**	
		Versión	1.0
		Creación	Irving L. Solsol Vilca
		Aprobación	
		Fecha	

D.1. Política general de seguridad

La dirección general del entorno de investigación, entendiendo que la información es un activo fundamental para la gestión y el desarrollo de proyectos de investigación y que es una prioridad la gestión de la seguridad del activo (información) que circula dentro de las instalaciones, asumiendo los siguientes compromisos:

- Desarrollar, implementar y mantener un modelo de seguridad de la información basado en los lineamiento establecidos en la norma ISO 27001 e ISO 27002.
- Establecer las políticas, procedimientos, controles y documentos vinculados en materia de la seguridad y privacidad del activo.
- Implementar los recursos y medidas necesarias para la prevención y mitigación de los riesgos, minimizando la materialización de las amenazas hacia nuestros activos de información y los procesos vinculados.
- Establecer y mantener metas medibles alineados al objetivo y alcance del modelo de seguridad del activo.
- Buscar a través de las mejoras e innovaciones tecnológicas, la mejora continua de la seguridad y privacidad del activo en los procesos operativos para el desarrollo de la investigación.
- Identificar y cumplir los requisitos legales aplicables a la seguridad y privacidad del activo.

- Brindar y mantener la confianza a nuestros personal y aliados en el cumplimiento de los requisitos aplicables de seguridad y privacidad del activo.

La Presente política es de cumplimiento obligatorio por parte de todo el personal, aliados y terceros que tengan acceso, almacenen, conozcan, procesen o transmitan información del entorno de investigación.

D.2. Políticas de Organización de la Seguridad de la Información

El entorno de investigación para una correcta gestión de la seguridad y privacidad de la información, establece las políticas para la organización interna y el uso de dispositivos móviles y teletrabajo.

D.2.1. Organización Interna

El entorno de investigación estará dirigida por la alta dirección, la misma que deberá de asignar todos los mecanismos y recursos necesarios, así como también brindar todo el apoyo y facilidades para la gestión de la seguridad y privacidad de la información, por lo que deberá:

- Establecer y definir los roles y responsabilidades del equipo que velará por la gestión adecuada de la seguridad y privacidad de la información.
- Adoptar políticas, procedimientos y controles de que ayuden a preservar la seguridad y privacidad de la información.
- Adoptar una o más metodologías que permitan gestionar los riesgos de seguridad y privacidad de la información.

D.2.2. Dispositivos móviles y teletrabajo

El entorno de investigación brinda las condiciones para el uso de dispositivos móviles (portátiles, teléfonos celulares, tabletas, entre otros.) institucionales y de propiedad del personal que haga uso de los servicios del entorno de investigación, de la misma manera, proporciona los mecanismos para que el personal haga uso adecuado y responsable de los equipos móviles de propiedad de la institución.

Dispositivos móviles:

- Establecer y definir las condiciones de uso adecuado de los dispositivos móviles institucionales.

- Proporcionar los mecanismos de seguridad necesarios para la protección e integridad de los dispositivos móviles del entorno de investigación.

- Establecer y validar las configuraciones de seguridad necesarias dentro de las plataformas tecnológicas para los dispositivos móviles institucionales y del personal que haga uso de los servicios del entorno de investigación.

- Establecer métodos de boqueo para el control de acceso a las configuraciones y a los mecanismos de autenticación de los dispositivos móviles institucionales asignados al personal.

- Proporcionar mecanismos de protección y seguridad contra código malicioso para el dispositivo móviles institucional y la información almacenada en ella.

- Implementar mecanismos de seguridad para la detección y monitorio de fuga de información almacenada en los dispositivos móviles institucionales.

Teletrabajo:

- La alta dirección junto al oficial de seguridad deberán aprobar y autorizar las conexiones remotas a los equipos de computo y sistemas de información para el personal lo requiera previa justificación.

- Se deberán aplicar controles y mecanismos de seguridad para establecer una conexión remota segura, así mismo, se deberá de verificar su eficiencia.

- Implementar mecanismos de control para monitorizar las conexiones remotas a equipos de computo y sistemas de información y detectar posibles fugas de información.

- Realizar auditorías de seguridad de todas las conexiones remotas a los equipos de computo y sistemas de información.

D.3. Políticas de Seguridad de los Recursos Humanos

El entorno de investigación entiende que el manejo de la información sensible del personal vinculado al entorno de investigación es de suma importancia para el cumplimiento de la legislación vigente, además de los requisitos establecidos por la institución para la contratación y gestión del personal.

D.3.1. Antes de asumir el empleo

Personal o tercero vinculado:

- Deberá entregar toda información física y digital solicitada por la institución antes, durante y después de su vinculación a la institución.
- Deberá de firmar un acuerdo de aceptación de las políticas, procedimientos y controles de seguridad y privacidad de la información antes de su vinculación a la institución.
- Deberán firmar un acuerdo de confidencialidad y no divulgación de la información de la institución que se conozca, maneje, procese, o almacene.

Institución:

- Asegurarse de acuerdo al perfil requerido la vinculación del personal competente para el puesto requerido.
- Validar la información física y digital proporcionada por el personal y terceros para la vinculación o desempeño de funciones temporales con la institución.
- Hacer firmar los acuerdos de aceptación de las políticas, procedimientos y controles de seguridad y privacidad de la información, así como también, los acuerdos de confidencialidad y no divulgación de la información de la institución que conozca, maneje, procese, o almacene.

D.3.2. Durante la ejecución del empleo

Personal o tercero vinculado:

- Cumplir con las políticas, procedimientos y controles de seguridad vigentes de la institución.
- Asistir a todos las capacitación y entrenamientos programados con el propósito de adquirir o reforzar sus competencias
- Salvaguardar y usar de manera responsable las credenciales y permisos de accesos asignadas a las instalaciones, plataformas tecnológicas y sistemas de información.

Institución:

- Desarrollar actividades para promover la sensibilización y adopción de la cultura de la seguridad y privacidad de la información.

- Gestionar la asignación de credenciales y permisos de accesos a las instalaciones, plataforma digitales y sistemas de información para el cumplimiento y desempeño de sus funciones.
- Brindar las facilidades para el cumplimiento del plan de capacitación y entrenamiento al personal en materia de seguridad y privacidad de la información.
- Almacenar y custodiar de forma segura toda la información personal y sensible del personal vinculado a la institución de acuerdo a legislación vigente.
- Asegurar el cumplimiento y la aplicación de las medidas administrativas de las condiciones de los acuerdos de confidencialidad y aceptación de las políticas de seguridad.

D.3.3. Terminación y cambio de empleo

Personal o tercero vinculado:

- Cumplir con toda la normativizad establecida por la institución para la entrega del cargo.
- Hacer entrega de las credenciales y equipos asignados para el desempeño de sus funciones.

Institución:

- Iniciar y gestionar el proceso cambio de funciones o desvinculación del personal o tercero vinculado a la institución.
- Reportar y gestionar de manera inmediata el cambio de funciones para la actualización o bloqueo de las credenciales y permisos de accesos a las instalaciones, plataformas tecnológicas y sistemas de información.
- Verificar el cumplimiento de los procesos de cambio de funciones o desvinculación del personal a la institución.

D.4. Políticas de Gestión de Activos

El entorno de investigación es propietario de todos los activos (información física y digital) de la institución y entiende la importancia del manejo y uso correcto de los activos que se almacene en los puestos de trabajo, equipos (estaciones de trabajo, dispositivos móviles, impresoras, entre otros.) y servicios tecnológicos (redes, internet, plataformas tecnológicas, sistemas de información, bases de datos, entre otros.), de la institución.

Como propietario de los activos, permite a su personal y terceros, de acuerdo a sus funciones asignadas, poder usar los activos para el cumplir con el propósito de la institución. En ese sentido, el Entorno de investigación asigna responsabilidades a los jefes y responsables de área velar el cumplimiento de políticas, procedimientos y controles establecidos para el uso responsable de los activos.

D.4.1. Responsabilidad de los activos

- Tener un inventario actualizado de los activos de información físicos(formato papel) o digitales (base de datos, correos electrónicos, audio digital, entre otros.) que se encuentre a su cargo.
- Asegurarse que todos los activos (servicios tecnológicos) estén funcionando y operando eficientemente para acceso y uso de todo el personal.
- Gestionar la autorización, permisos, restricciones y bloqueos de accesos a los activos de información.
- Velar el cumplimiento de las guías de uso responsable de los activos de información.
- Gestionar según disposición la recepción, asignación y almacenamiento de los activos de información físicos.

D.4.2. Clasificación de la información

El entorno de investigación entendiendo que cuenta con activos relevante y mucha importancia, debe establecer directrices, así como también proporcionar los recursos necesarios para asegurar la clasificación y manejo de los mismos.
Como propietario de los activos, designa responsabilidades a los jefes y responsables de área la aplicación y cumplimiento de las siguientes directrices.

- Establecer criterios de clasificación para cada activo de acuerdo a su nivel de importancia (Público, uso interno, Restringido o confidencial).
- Establecer criterios de correcto etiquetado para cada activo, según la clasificación recibida.
- Socializar con todo el personal los criterios de clasificación y etiquetado de los activos.
- El equipo de seguridad de la información deberá de establecer controles técnicos, utilizar los recursos necesarios y proveer seguridad para el manejo (acceso y almacenamiento) adecuado de los activos.
- Monitorizar periódicamente el cumplimiento de los controles técnicos, criterios de clasificación y etiquetado de los activos.

D.4.3. Manejo de medios

El entorno de investigación a través del responsable de seguridad proporcionaran criterios y controles para el uso de puertos periféricos y medios de almacenamiento externos.

- Establecer configuraciones y definir los controles para el bloqueo de los puertos periféricos de los activos de información.
- Definir las directrices, las condiciones y responsabilidades para permitir el uso los puertos periféricos de los activos de información.
- Definir Controles y criterios para uso y resguardo de dispositivos de almacenamiento externos.
- Establecer la documentación formal para la solicitud y aprobación de acceso a puertos periféricos y medios de almacenamiento externo.
- Contar con un inventario actualizado de todo el personal que tiene permiso de uso de puertos periféricos y medios de almacenamiento externo.
- Custodiar de forma segura los medios de almacenamiento externo institucionales.
- Definir un procedimiento específico de borrado seguro de datos para los medios de almacenamiento.

D.5. Políticas de Control de acceso

El entorno de investigación como propietario de los activos (Redes, plataforma digitales, sistemas de información, entre otros.) que sirve para el cumplimiento de los propósitos de la institución, entiende que debe de establecer mecanismos y controles para el acceso a sus activos.

D.5.1. Requisitos del negocio para el control de acceso

- Establecer Políticas y procedimientos para el control y gestión de accesos de sus activos.
- Implementar los recursos y mecanismos necesarios para preservar la privacidad y confidencialidad de las autenticaciones y conexiones a los activos.
- Establecer los recursos y mecanismos necesarios para monitorizar y controlar los accesos así como también el uso adecuado y responsable de los activos.
- Definir los perfiles y establecer las credenciales y permisos de acceso al personal y terceros que tendrán acceso al uso y administración de los activos.
- Habilitar el acceso a los activos según el perfil y permisos asignados.

D.5.2. Gestión de acceso de usuario

- Definir y establecer los procedimientos necesarios para la correcta gestión en la asignación de credenciales y permisos de acceso a los activos, asignados al personal o terceros.
- Establecer e implementar los controles necesarios para monitorizar y gestionar los accesos y permisos de las credenciales asignadas al personal y terceros.
- Verificar periódicamente el cumplimiento de los procedimientos y controles establecidos para asignación y gestión de credenciales y permisos asignados al personal y terceros.
- Realizar auditorías periódicas a todos los procedimientos y controles establecidos para la gestión de credenciales y permisos asignados al personal y terceros.

D.5.3. Responsabilidades de usuario

- El usuario es el único responsable de las acciones realizadas con las credenciales y permisos asignados.
- No deberá por ninguna circunstancia compartir con otro personal o tercero las credenciales asignadas.
- Aplicar las políticas y condiciones de uso de las credenciales y permisos asignados para el desarrollo de sus funciones.

D.5.4. Control de acceso al sistemas y aplicaciones

- Velar que exista diferentes tipos de perfiles, credenciales y permisos para los sistemas y aplicaciones que estén en producción y en pruebas o desarrollo.
- Validar todos los permisos asignados a las credenciales del personal y terceros.
- Verificar que los usuarios administradores de los sistemas y aplicaciones lleven un control de todas la transacciones, actualizaciones y registros que se han realizados en los mismos.
- Verificar que todos los sistemas y aplicaciones que se implementen cuenten con mecanismos de autenticación robusto.
- Restringir la instalación de aplicaciones por parte de los usuarios.
- Incentivar que no almacenar las credenciales de las sistemas de información y plataformas tecnológicas en lugares visibles y de fácil acceso, así como también en los navegadores de los activos.

D.6. Políticas de Criptografía

El entorno de investigación como propietario del activo (información digital), busca que el activo de información clasificado como restringido o confidencial, se encuentre cifrada cuando se vaya a transferida, enviar o almacenar en cualquier medio electrónico.

D.6.1. Controles criptográficos

- Adoptar una metodología y herramientas certificadas para aplicar los controles criptográficos.
- Establecer una política para la aplicación de los controles criptográficos requeridos.
- Definir el tiempo de vigencia de las llaves de cifrado y descifrado aplicados a los activos.
- Verificar la adopción de una metodología y uso de herramientas certificadas, así como también el cumplimiento de las políticas de controles criptográficos.

D.7. Políticas de Seguridad física y del entorno

El entorno de investigación deberá proveer e implementar herramientas y mecanismos de seguridad necesarios a todas los activos (áreas, instalaciones y equipos) donde se genere, procese y almacene activos (información física y digital) confidencial y de suma importancia; es por ello que deberá establecer políticas, controles y directrices para prever y mitigar las amenazas existentes a las que se encuentra expuesto.

D.7.1. Áreas seguras

- Identificar y establecer como áreas seguras a las áreas e instalaciones donde se genere, procese y almacene activos de la institución.
- Establecer una política de permisos y control de acceso a las áreas seguras.
- Implementar mecanismos físicos o digitales para el control y registro de los sucesos en las áreas seguras.
- Velar y monitorizar el cumplimiento de las políticas, controles y mecanismos de seguridad dirigidos a preservar la seguridad.

D.7.2. Equipos

- Establecer una política de uso adecuado, operación y de almacenamiento para cada tipo de activo.

- Implementar mecanismos de seguridad necesarios a cada uno de los activos para salvaguardar su privacidad, integridad y confidencialidad.
- Definir métricas y condiciones de seguridad que deberán cumplir los equipos de propiedad de la institución o equipos externos para que se pueda permitirles el acceso a las redes publicas y privadas de la institución.
- Usar los medios necesarios para implementar un sistemas de energía de emergencia para la protección de los activos contra la falla de energía.
- Velar y monitorizar el cumplimiento de las políticas, controles y mecanismos de seguridad establecidos.

D.8. Políticas de Seguridad en las operaciones

El entorno de investigación busca que el desarrollo de las operaciones de generación, procesamiento y almacenamiento de los activos (información física y digital), sean seguras y estén protegidas ante cualquier incidencia de seguridad, por lo que provee directrices, procedimientos y controles de seguridad.

D.8.1. Procedimientos operacionales y responsabilidades

La alta dirección a través del comité de seguridad y privacidad de la información, definen y asignan las responsabilidades a los jefes y responsables de área, por que estos deberán:

- Elaborar la documentación requerida para el desarrollo y ejecución de las operaciones detallando a los responsables de cada operación.
- Elaborar la documentación física y digital requerida para el control y registro de la ejecución de operaciones y administración de los activos de información.
- Socializar y dar las facilidades al acceso a todo el personal autorizado ala documentación de control de operaciones.

D.8.2. Protección contra códigos maliciosos

El responsable de la seguridad de la información proporcionará los mecanismos necesarios para proteger los activos de información en los Equipos y dispositivos móviles de propiedad de la institución, por lo que deberá:

- Gestionar la adquisición e implementación de las herramientas necesarias para la detección, gestión y control de código malicioso.

- Diseñar procedimientos y configuraciones necesarias para integrar e implementar con las herramientas de detección, gestión y control de código malicioso en los activos de información.
- Asegurarse que las herramientas y configuraciones para la detección, gestión y control de código malicioso se adapte a las necesidades de la institución.
- Asegurarse que la integración de herramientas y configuraciones realizadas, permitan la operatividad adecuada de los activos de información.
- Asegurarse de registrar todas las incidencias de seguridad de códigos maliciosos.

D.8.3. Copias de respaldo

El propietario de los activos (información física y digital), junto al responsable de la seguridad de la información deberán:

- Elaborar las directrices para la ejecución y almacenamiento de las copias de respaldo.
- Desarrollar procedimientos seguros para la ejecución del proceso de copias de respaldo.
- Establecer los recursos necesarios para el almacenamiento y acceso seguro para preservar la privacidad e integridad de las copias de respaldo.
- Proveer la infraestructura necesaria para el almacenamiento seguro de las copias de respaldo.

D.8.4. Registro y seguimiento

El entorno de investigación requiere monitorizar la operatividad y el uso adecuado de sus activos de información, para la detección e identificación oportuna de incidencias y fallas, para ello, el responsable de la seguridad de la información deberá:

- Elaborar y diseñar las configuraciones necesarias para la recolección registro de eventos (log) en cada uno de los activos de información.
- Asegurarse que todos los activos de información se encuentren correctamente configurados y tengan sincronizados los relojes digitales internos con la zona horario correcta.
- Implementar los recursos y medios necesarios para el almacenamiento seguro de los registros de eventos preservando la privacidad e integridad, así mismo se deberá garantizar el cumplimiento del tiempo máximo requerido para su almacenamiento.
- Adoptar una metodología y las herramientas necesarias para el procesamiento y análisis de los registros de eventos

- Implementar los recursos necesarios para autorizar, registrar y controlar el accesos y uso seguro de los registros de eventos.

- Establecer los métricas necesarias que permitan la toma de decisiones en la gestión y uso adecuado de los activos de información.

D.8.5. Control de software operacional

El entorno de investigación consciente de que el uso de software operacional (sistema operativo), es indispensable para el funcionamiento de los activos (hardware) de información de la institución, por lo que el responsable de la seguridad de la información deberá:

- Establecer los requisitos necesarios para la adquisición de software operacional, asegurándose que cuente con las licencias el servicio de soporte por parte de su proveedor.

- Definir los roles y responsabilidades del personal o tercero especializado que deberá de hacer las instalaciones, mantenimiento y actualizaciones de los software operacionales.

- Implementar los mecanismos necesarios para controlar y restringir la instalación de software que no haya sido aprobado para su uso.

- Establecer las condiciones para la instalación y configuraciones necesarias y asegurar el correcto funcionamiento de los software operacional.

- Tener inventario actualizado y detallado de todos los software operacional que se este usando en la institución.

D.8.6. Gestión de la vulnerabilidad técnica

El entorno de investigación a través del responsable de la seguridad de la información deberá:

- Desarrollar un plan de trabajo institucional para la detección y gestión de vulnerabilidades técnicas.

- Implementar los mecanismos necesarios para controlar y restringir la instalación de software que no haya sido aprobado para su uso.

- Realizar las auditorías internas que permitan identificar que tipo de software se están usando en los activos de información.

D.9. Políticas de Seguridad de las comunicaciones

El entorno de investigación entiende que la seguridad en toda su infraestructura y servicios de comunicaciones es de mucha importancia para preservar la privacidad y confidencialidad de la información que se encuentra en tránsito y reposos en sus activos de información, en ese sentido:

D.9.1. Transferencia de información

Para la Transferencia de la información, se deberá:

- Establecer las política, procedimientos y controles de seguridad necesarios para la transferencia de información dentro y fuera de la institución.
- Implementar los mecanismos de seguridad necesarios para asegurar la integridad de la información transferida dentro y fuera de la institución
- Elaborar la documentación necesaria para definir los acuerdos de seguridad para la transferencia de información de forma interna y externa.
- Proveer los mecanismos de seguridad necesaria para proteger y asegurar la integridad y confidencialidad de la información compartida a través de mensajería electrónica.
- Desarrollar y asegurar el cumplimiento de acuerdos de confidencialidad y no divulgación de la información transferida internamente y externamente.
- Velar el cumplimiento de las políticas, controles, mecanismos y acuerdos en los procesos de transferencia de información interna y externa.

D.10. Políticas de Adquisición, desarrollo y mantenimiento de sistemas

El entorno de investigación entiende la necesidad salvaguardar la seguridad de los datos utilizados como pruebas para el desarrollo de los proyectos de investigación, para lo cual deberá:

D.10.1. Datos de prueba

- Elaborara los procedimientos y controles de seguridad que se deben aplicar a los datos de prueba para el desarrollo de software
- Asegurarse que los datos de prueba proporcionada a los desarrolladores no contenga información sensible, ni tampoco tenga la clasificación de restringido o confidencial.

- Elaborar e implementar un procedimiento sobre la forma correcta de la disposición final de los datos de prueba.

D.11. Políticas de Relaciones con los proveedores

El entorno de investigación entiende que contar con el servicio de terceros es un proceso estratégico para el cumplimiento de los propósitos de la institución, sin embargo, es preciso definir las políticas, condiciones y acuerdo de confidencialidad y no divulgación para poder brindarles el acceso seguro y controlado a las activos de la institución, por que deberá:

D.11.1. Seguridad de la información en las relaciones con los proveedores

- Establecer una política de seguridad para el acceso y uso de los activos de información a terceros.
- Diseñar y establecer un contrato formal donde especifique los acuerdos de confidencialidad y uso de la información intercambiada entre la institución y terceros, así como también el cumplimiento de las normas y legislación vigente.
- Establecer los requisitos de seguridad que deberán tener los terceros para la transferencia y acceso a la información de la institución.
- Evaluar y gestionar los accesos requeridos a los terceros para el desempeño y desarrollo de sus funciones contratadas.

D.12. Políticas de Gestión de incidentes de seguridad de la información

El entorno de investigación, a través del encargado de la seguridad de la información, deberán:

D.12.1. Gestión de incidentes y mejoras en la seguridad de la información

- Elaborar los procedimientos necesarios para el accionar ante la materialización de un evento o debilidad de seguridad.
- Elaborar los procedimientos correspondientes para el proceso de reporte y comunicación adecuada de un evento o debilidad de seguridad

- Definir las responsabilidades al personal calificado y establecer los procedimientos para el manejo de un evento o debilidad de seguridad.
- Elaborar un informe técnico del evento o debilidad de seguridad y las medidas tomadas para su control.
- Desarrollar un plan de mejora continua de los eventos o debilidades de seguridad.
- Elaborar un informe ejecutivo periódico de todos los sucesos de eventos o debilidades de seguridad.

D.13. Políticas de Cumplimiento

El entorno de investigación es consciente y entiende su compromiso y responsabilidad de velar por el cumplimiento de las normas, acuerdos, requisitos legales y contractuales aplicables para todas sus actividades dentro de las áreas e instalaciones de la institución, es por ello que deberá de establecer un plan de auditorías para revisar y garantizar que todos los procedimientos, mecanismos y controles diseñados para la seguridad y protección de sus activos de información se cumplan de acuerdo a las políticas establecidas.

D.13.1. Cumplimiento de requisitos legales y contractuales

El entorno de investigación deberá:

- Identificar todas normas, acuerdos, requisitos legales y contractuales, para elaborar y establecer las documentación que reglamente el cumplimiento de los mismos.
- Contar con un inventario de todos los activos de su propiedad para identificar y aplicar los mecanismos de seguridad para el cumplimiento de la legislación que proteja el derecho de la propiedad intelectual.

D.13.2. Revisiones de seguridad de la información

- El comité de seguridad periódicamente deberá de realizar supervisiones para verificar el cumplimento de las políticas, procedimientos y otros controles establecidos para la seguridad y protección de los activos de información.
- El responsable de la seguridad de la información deberá de establecer revisiones periódicas sobre el cumplimiento de todos los mecanismos y controles técnicos implementados a los sistemas de información.

E. Anexo: Procedimientos de seguridad de la información

E.1. Procedimiento para el ingreso seguro a los sistemas de información

Lógo institución	**Procedimiento para el ingreso seguro a los sistemas de información**	**Código:**	XXXXXXXX
		Versión:	X.X
		Fecha:	dd / mm / aaaa

E.1.1. Objetivo

Establecer los lineamiento para controlar el acceso a los sistemas de información del entorno de investigación.

E.1.2. Alcance

Este procedimiento es aplicado a los sistemas de información y aplicaciones de propiedad del entorno de investigación desarrollados y adquiridos para las actividades de la institución.

E.1.3. Referencias

- Ley 1581 de 2012 - Régimen de Protección de datos personales.
- Ley 1273 de 2009 - Protección de la información y de los datos.
- ISO/IEC 27001:2013 - Sistemas de Gestión de la Seguridad de la Información.

E.1.4. Definiciones

Aplicaciones: Es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de actividades, herramientas como ofimática, adquisición y procesamiento de datos, desarrollo, entre otros.

Credencial: Es un usuario y contraseña que es asignado únicamente a una persona interna o externa del entorno de investigación sobre un sistema de información o aplicación; su uso es único y exclusivo del mismo con la debida responsabilidad por su cuidado y divulgación.

Cuenta: Es la identificación única que se da a un usuario (personal interno o externo) para el acceso a aplicaciones o servicios de información, junto a unos permisos establecidos, según lo solicitado por el Jefe o responsable de área.

Deshabilitar: Es el proceso que permite revocar las credenciales, permisos o cuenta de las aplicaciones del entorno de investigación de un usuario, según solicitud del jefe o responsable de área.

Inactivar: Proceso por el cual se restringe el acceso de un usuario a través de sus credenciales y permisos asignados a los sistemas de información, aplicaciones y equipos de cómputo del Entorno de investigación por un tiempo o periodo específico.

Información: Es un conjunto de datos generado o adquirido producto de una actividad, que basado en un contexto determinado tienen un significado e importancia para el entorno de investigación.

Password: Es un conjunto de datos conformados por una secuencia alfanumérica que junto a al identificador de una cuenta, permite validar la autenticación de un usuario para el acceso a una aplicación o sistemas de información específico.

Reactivar: Es el procedimiento que permite conceder el acceso de un usuario a los sistemas de información y equipos de cómputo del Entorno de investigación, que previamente se encuentren inactivos, producto de una solicitud del jefe o responsable del área.

Responsable de la Seguridad de la Información: Jefe o responsable de área que responde por la integridad, administración, desarrollo, aceptación, operación, mantenimiento y retiro del sistema de información.

Seguridad de la información: Preservación de confidencialidad, integridad y disponibilidad de la información.

Servicios informáticos: Herramientas tecnológicas a los que un usuario puede acceder mediante la cuenta asignada.

Usuario: Una persona que usa el servicio de tecnologías de la información (TI).

Usuario administrador: Es una cuenta de usuario que posee con todos los permisos, privilegios y características necesarias para el acceso y gestión de un sistema de información o aplicación y cuyas acciones o modificaciones afectan directa o indirectamente las funciones de las mismas.

Workstation: Es el equipo de computo usado para la adquisición, procesamiento y gestión de la información (generación, transformación, almacenamiento, protección, y recuperación de datos).

E.1.5. Crear, modificar, inactivar y reactivar usuarios en los sistemas de información y aplicaciones

Creación de usuarios y modificación de accesos.

El Área de recursos Humanos junto a los jefes o responsables de área, deberán dirigir la solicitud de la creación o modificación de usuarios a través del correo institucional del Entorno de investigación adjuntando el formato de solicitud con su sustento correspondiente al propietario de los sistemas de información, aplicaciones, servicios informáticos y equipos workstation, la solicitud deberá de especificar:

- Acción a realizar (creación o modificación).
- Tipo de cuenta de usuario (red, aplicativo, correo institucional, entre otros.).
- Rol de la cuenta (usuario o administrador).
- Permisos de la cuenta (lectura, lectura y escritura, eliminación o creación).
- Sustento de la solicitud.

En caso de que se requiera alguna aclaración sobre la solicitud, se pedirá información adicional a través del correo institucional al jefe o responsable de área solicitante.
Para el caso de la creación de usuarios, las credenciales generadas se entregarán directamente al usuario a través de los medios aprobados para la notificación
Para el caso de modificación de roles o perfiles, esto será notificado al correo institucional del usuario con copia al solicitante.

Inactivar, reactivar y deshabilitar las cuentas de usuarios y permisos.

El Área de recursos Humanos junto a los jefes o responsables de área, deberán dirigir la solicitud de inactivar, reactivar o deshabilitar las cuentas de usuario o permisos a través del correo institucional del Entorno de investigación adjuntando el formato de solicitud con su sustento correspondiente al propietario de los sistemas de información, aplicaciones o servicios de red, la solicitud deberá de especificar:

- Acción a realizar (inactivar, reactivar o deshabilitar).
- Tipo de cuenta de usuario (red, aplicativo, correo institucional, entre otros.).
- Rol de la cuenta (usuario o administrador)
- Permisos de la cuenta (lectura, lectura y escritura, eliminación o creación).
- Sustento y tiempo de inactivación y reactivación.
- Sustento para deshabilitar.

En caso de que se requiera alguna aclaración sobre la solicitud, se pedirá información adicional a través del correo institucional al jefe o responsable de área solicitante.
Las acciones realizadas serán notificadas a través del correo institucional al solicitante.

E.1.6. Registro de accesos de usuarios y administración de los sistemas de información y aplicaciones

Registro de accesos de administración de los sistemas de información y aplicaciones

La administración de los sistemas de información y aplicaciones por parte del usuario encargado, serán previa solicitud de acceso y autorización del propietario de los sistemas de información. Toda acción realizada en la administración de las diversas plataformas tecnológicas, tendrá que generar registros y se deberá documentar:

- Las credenciales que se esta usado para el acceso.
- Las actividades y acciones realizados en los sistemas de información y aplicaciones.
- Las actividades y acciones realizados en las Bases de datos.
- Las actividades y acciones realizados en los servidores.
- Las actividades y acciones realizados en las workstation.
- Las actividades y acciones realizados en los equipos y dispositivos de de comunicaciones y de seguridad.

El acceso deberá ser únicamente con las credenciales asignadas al usuario designado, la cual es intransferible.
Los registros y documentación generados servirán como sustentos según necesidad.

Registro de accesos de usuarios a los sistemas de información y aplicaciones

Los usuarios deberán ingresar a los sistemas de información, aplicaciones y servicios informáticos, usando las credenciales asignadas para sus actividades, las mismas que son intransferibles. Toda acción realizada por el usuario en los sistemas de información y aplicaciones, tendrán que generar registros de:

- Las credenciales que se esta usado para el acceso.
- Las actividades y acciones realizados en los sistemas de información y aplicaciones.
- Las actividades y acciones realizados en las workstation.

El acceso deberá ser únicamente con las credenciales asignadas al usuario designado, la cual es intransferible.
Los registros generados servirán como sustentos según necesidad.

E.1.7. Acceso y uso seguro de los sistemas de información, aplicaciones y tecnologías de información

Todos los usuarios para el accesos y uso seguro, deberán:

- Usar contraseñas alfanuméricas.
- Asegurarse de que el ingreso de las credenciales de acceso sea privado.
- Cambiar la clave de acceso de acuerdo a las políticas establecidas.
- Cerrar sesión de los sistemas de información y aplicaciones cuando se ya no se requiera su uso o al terminar la jornada laboral.
- Cada vez que se ausente de los equipos de computo, bloquear la sesión de usuario.

E.1.8. Responsabilidades

Usuarios: Es responsable de:

- Aplicar todos los controles, procedimientos y políticas que están a su alcance para la seguridad y privacidad de la información.

Recursos humanos: Es responsable de:

- Coordinar con los jefes o responsables de área la solicitud de crear y asignar los permisos de accesos para los nuevos usuarios.
- Coordinar con los jefes o responsables de área la solicitud de modificar, inactivar, reactivar o deshabilitar las cuentas y permisos de accesos de los usuarios según sustento.
- Proteger y resguardar los datos personales de los usuarios.

Jefes o responsables de área: Es responsable de:

- Proveer los sustentos requeridos para la solicitud de crear, modificar, inactivar, reactivar o deshabilitar las cuentas y permisos de accesos de los usuarios.

Responsable de la Seguridad de la Información: Es responsable de:

- Aprobar y gestionar la atención de las solicitudes de crear, modificar, inactivar, reactivar o deshabilitar las cuentas y permisos de accesos de los usuarios.
- Proteger y resguardar los datos personales de los usuarios.
- Registrar y documentar todas las actividades y acciones realizados en los sistemas de información y aplicaciones por parte de todos los usuarios.
- Informar al área de Recursos Humanos y a los jefes o responsables de área los incidentes de seguridad en los sistemas de información y aplicaciones que puedan surgir por parte de los usuarios.
- Mantener actualizado el procedimiento para el ingresos seguro a los sistemas de información.

Elaboró	**Revisó**	**Aprobó**
Nombres y Apellidos:	Nombres y Apellidos:	Nombres y Apellidos:
Cargo:	Cargo:	Cargo:

E.2. Procedimiento de protección contra código malicioso

Lógo institución	**Procedimiento de protección contra código malicioso**	**Código:**	XXXXXXXX
		Versión:	X.X
		Fecha:	dd / mm / aaaa

E.2.1. Objetivo

Establecer los lineamientos a seguir para el cumplimiento de los controles de seguridad en la protección contra la protección de Código malicioso.

E.2.2. Alcance

Este procedimiento es aplicado a todos los workstation y dispositivos móviles de propiedad del Entorno de investigación adquiridos para el desarrollos de las actividades de la institución.

E.2.3. Referencias

- Ley 1581 de 2012 - Régimen de Protección de datos personales.
- Ley 1273 de 2009 - Protección de la información y de los datos.
- ISO/IEC 27001:2013 - Sistemas de Gestión de la Seguridad de la Información.

E.2.4. Definiciones

Virus: Es un programa que buscará duplicarse en la memoria y en los discos, pero de una manera sutil que no se notará inmediatamente. Los virus son uno de los varios tipos de software malicioso o malware.

Malware: Software diseñado para infiltrarse o dañar un sistema informático, sin el consentimiento informado del propietario con el propósito de secuestrar, espiar, robar información de los sistemas de información.

Troyano: Es un programa malicioso que se disfraza o se incrusta dentro de un software legítimo. El término se deriva del mito clásico del Caballo de Troya. Hay dos tipos comunes de troyanos. Uno, es software útil que ha sido corrompido por un delincuente informático que inserta código malicioso que se ejecuta mientras se usa el programa. El otro tipo es un programa independiente que se disfraza de otra cosa, como un juego o un archivo de imagen, con el fin de engañar al usuario para que se convierta en una complicidad mal dirigida que se necesita para llevar a cabo los objetivos del programa.

Gusano: Es un gusano de computadora es un programa de computadora que se replica a sí mismo. Utiliza una red para enviar copias de sí mismo a otros sistemas y puede hacerlo sin la intervención del usuario. A diferencia de un virus, no necesita conectarse a un programa existente. En general, los gusanos siempre dañan la red y consumen ancho de banda, mientras que los virus siempre infectan o corrompen los archivos de un equipo objetivo.

Workstatión: Es el equipo de computo usado para la adquisición, procesamiento y gestión de la información (generación, transformación, almacenamiento, protección, y recuperación de datos).

Dispositivos móviles: Es el equipo portátiles, teléfonos celulares, tabletas y otros, usados por los usuarios para el desarrollo de actividades adicionales a las funciones asignadas.

E.2.5. Consideraciones para abordar la protección

La protección contra código malicioso se deberán abordar principalmente implementando un software de Antivirus con sus respectivas configuraciones y actualización controladas de software y de base de datos de firmas, es por ellos que se tiene que tener en cuenta los siguientes niveles de protección:

Selección de software antivirus

El entorno de investigación, a través del responsable de la seguridad de la información, deberá de analizar, evaluar y adquirir un software antivirus que se adapte a las necesidades de la institución.

Administración centralizada

Se deberá implementar una Administración centralizada que permita la gestión de toda la infraestructura de control contra código malicioso (configuraciones, controles, actualizaciones, entre otros), que deberá permitir obtener informes y hacer el seguimiento de los brotes o infecciones presentadas dentro de la institución.

Servidores de archivos y sistemas de información

Estos activos de información contiene la mayoría de los datos críticos del Entorno de investigación, es por ello, que es indispensable proteger de los códigos maliciosos. Para la instalación y configuración de un software de antivirus en los servidores, el responsable de los controles de antivirus deberá tener algunas consideraciones, como por ejemplo:

- ¿Cuándo debe ejecutarse un análisis programado?

- ¿Qué archivos, tipos de archivos, directorios o unidades deben excluirse de un análisis?
- ¿Qué tipo de extensiones de archivos deberán bloquearse desde la administración centralizada?
- ¿Cómo se deberán manejar los archivos infectados?

Equipos workstation y dispositivos móviles

Los equipos workstation y dispositivos móviles, son los activos de información más difícil de gestionar y controlar, ya que estos al interactuar con los usuarios para el desarrollo de actividades laborales, interactuar con dispositivos de almacenamiento externos y el acceso constante a internet, permiten que estos equipos estén expuestos a riesgos considerables.
En ese sentido, el usuario no debe ni necesita tener acceso a las configuraciones del software antivirus instalado en los equipos workstation y dispositivos móviles, por lo que el responsable de los controles de antivirus con la aprobación del responsable de la seguridad de la información y en coordinación con el soporte técnico deberán de configurar los equipos para restringir:

- La posibilidad de deshabilitar el servicio antivirus.
- La posibilidad de desactivar o cancelar un análisis programado.
- La posibilidad de desactivar el análisis en tiempo real.

E.2.6. Instalación de software de antivirus

Todos los equipos workstation, dispositivos móviles y servidores que funcionan bajo las plataformas de Windows, linux, Mac OS y Android de propiedad del Entorno de investigación dentro del entorno deben de tener instalado el software de antivirus y deberá estar configurada para actualizarse automáticamente.
El personal de soporte técnico, deberá de aplicar las configuraciones y los controles de seguridad, para que le software se desempeñe y realice trabajos predeterminados y programados según las políticas definidas. Así mismo, se deberá de aplicar las configuraciones definidas para evitar que los usuarios no puedan cancelar las tareas programadas, ni a las configuraciones de seguridad del software antivirus.

E.2.7. Actualización de software de antivirus

Las actualizaciones del software antivirus y las bases de datos de firmas, deberán estar controladas por el responsable de los controles de antivirus, con el propósito de evitar cualquier incidencia de seguridad o errores en las actualizaciones, ese sentido:

- Todas las actualizaciones de software y base de datos de firmas, se deberá gestionar desde la administración centralizada del servidor de antivirus y los equipos workstation y dispositivos móviles deberán estar configurados para que se actualicen desde el servidor de antivirus de acuerdo a las políticas establecidas.
- Para el caso de una nueva versión del software de antivirus, primero se actualizará en el servidor para que realice pruebas que permitan identificar cualquier inconveniente con los sistemas de información. Una vez realizada las pruebas necesarias, se procederá a dar pase la actuación.
- Para el caso actualizaciones de base de datos de firmas, las actualizaciones se deberán de ser diarias, en todos los equipos workstation, dispositivos móviles y servidores, en el caso que haya equipos que estén fuera de las instalaciones del entorno de investigación, estos deberán de actualizar al momento de conectarse a la red institucional.

E.2.8. Actividades para prevenir la aparición de código malicioso

Hacer mantenimiento regular del software antivirus

Los brotes de virus son típicamente causados por la aparición de nuevas técnicas y códigos maliciosos que aún no han sido detectados, por lo que es una de las causas de que logre hacer una infección y pueda propagarse rápidamente, pese a tener implementado el software de antivirus. Es por ello, que se debe monitorizar periódicamente las publicaciones del proveedor del software antivirus y verificar que se realicen las descargas correctas de las base de datos de firmas más recientes.

Monitorizar las incidencias del software de antivirus

El software antivirus debe estar funcionando correctamente para proteger todos los activos de información que están a su alcance y al tener implementado una administración centralizada, debe proporcionar información en tiempo real sobre el estado de los programas antivirus instalados en todos los activos de información y de la red.

Ataques intencionales de virus desde dentro y fuera de la red

Si un código malicioso entra en la red debido a una falla del software o a la negligencia de un empleado, es importante que el virus no se propague sin obstáculos y que el usuario comunique cualquier problema que pueda detectar en su computadora.

Aparición de código malicioso

La administración centralizada deberá ser capaz de evitar y controlar los aparición de código malicioso, para ello se deberá:

- Verificar que las bases de datos de firmas sean las más recientes, de no ser así, desplegar la versión más reciente proveída por parte del proveedor de antivirus.
- Generan un informe de registro completo de los eventos de virus en los activos de información y la red.
- Tener la capacidad de aplicar nuevos controles de seguridad remotamente para controlar la propagación del código malicioso y verificar que no quede ningún código de virus en ningún activo de información y en la red.

E.2.9. Concientización sobre código malicioso

Se deberá de desarrollar los planes de capacitación periódicas e informar a los usuarios finales de los peligros de los códigos maliciosos mediante la adopción de la cultura de seguridad de la información.

E.2.10. Informes

El responsable de los controles de antivirus deberá de generar y enviar al responsable de la seguridad de información un informe periódico sobre los incidentes y problemas en el Software Antivirus, el mismo que deberá de desarrollar estrategias y dar recomendaciones para corregir los incidentes y problemas reportados.

E.2.11. Responsabilidades

Usuarios: Es responsables de:

- Comunicar al soporte técnico del área de tecnologías cualquier problema, incidente o comportamiento anómalo del equipo workstation, dispositivos móviles o medios de almacenamiento externo de propiedad del Entorno de investigación que este a su cargo.
- Asegurarse que el software de antivirus se actualicen.
- Asegúrese de que las tareas de análisis del software de antivirus se ejecuten y se completen.

Soporte técnico: Es responsable de:

- Registrar la información proporcionada por los usuarios finales en relación con los brotes de antivirus o de código malicioso.
- Cuando se identifica la fuente de un virus, notificar al responsable de los controles de Antivirus sobre la infección por el virus y hacer un seguimiento de las medidas tomadas para rectificar.

- Aplicar los procedimientos y controles técnicos y de seguridad para la contención y desinfección de los códigos maliciosos (virus, malware, entre otros.) que se hayan identificado.

Responsable de los controles de antivirus: Es responsable de:

- Manténgase informado sobre las últimas amenazas de código malicioso (virus, malware, entre otros.).
- Manténgase al día con los parches de seguridad.
- Actualizar los archivos de definición de código malicioso (virus, malware, entre otros.). al menos una vez al día hábil o cuando se detecta un brote importante.
- Asegurarse de que el software antivirus de los del equipo wokstation, dispositivos móviles no esté desactivado.
- Si se encuentra una infección, aislar el equipo wokstation o dispositivos móviles de acuerdo con las políticas y procedimientos establecidos.
- Realizar un análisis técnico de los informes proporcionados por el software antivirus y realizar las tareas necesarias de acuerdo con los resultados de estos informes.
- Revisar qué causó el brote de virus y desarrollar una estrategia para cerrar estas amenazas potenciales en el futuro: bloquear cualquier archivo con más de una extensión de tipo de archivo, bloquear tipos de archivo que a menudo son portadores de virus (.exe, .bin, .bat y otras extensiones de archivo recomendadas por el proveedor del antivirus).

Responsable de la Seguridad de la Información: Es responsable de:

- Mantener actualizado el procedimiento de protección contra código malicioso.
- Revisar el análisis técnico realizado por el Responsable de los controles de antivirus.
- Sensibilización permanente de los usuarios a través de comunicaciones internas o boletines de seguridad.
- Liderar el programa de concienciación sobre seguridad de la información.

E.3. Procedimiento de transferencia de información

Lógo institución	**Procedimiento de transferencia de información.**	**Código:**	XXXXXXXX
		Versión:	X.X
		Fecha:	dd / mm / aaaa

E.3.1. Objetivo

Establecer los lineamientos a seguir para preservar la confidencialidad e integridad de en la transferencia de información.

E.3.2. Alcance

Este procedimiento es aplicado a toda información de propiedad de la institución y deberá ser adoptada por todo el personal interno que tenga acceso a información física y digital.

E.3.3. Referencias

- Ley 1581 de 2012 - Régimen de Protección de datos personales.
- Ley 1273 de 2009 - Protección de la información y de los datos.
- ISO/IEC 27001:2013 - Sistemas de Gestión de la Seguridad de la Información.

E.3.4. Definiciones

Activo de información: Es un componente (datos, información, accesorios, hardware, software, instalaciones, recursos humanos, entre otros.) que tiene un valor de importancia para una organización y que puede estar expuesto a riesgos y amenazas.

Confidencialidad: Propiedad de la información que hace que los datos solo puedan estar disponible y accesible por los usuarios que cuenten con la autorización correspondiente.

Copia no controlada: Es cualquier información o documento que no se encuentre almacenada en dispositivos de almacenamiento interno de los servidores o workstation de la institución que haya sido transferido a un tercero, haya sido impreso o no este etiquetada según su clasificación.

Importancia del activo: Es el valor que refleja la protección empleada y aplicada a un activo de información para preservar su integridad, confidencialidad y disponibilidad.

Integridad: Propiedad que consiste en preservar la exactitud y estado completo delos datos almacenados en la base de datos

Propietario del activo de información: Es el jefe o responsable del área donde se ha generado o se almacena el activo de información.

E.3.5. Proceso de transferencia de información

Solicitud de transferencia

Se deberá verificar la procedencia de la solicitud de transferencia de información:

1. **Solicitud interna:**
   - El personal interno que recepciona la solicitud deberá de dirigir la misma al propietario del activo de información para su evaluación y autorización.
2. **Solicitud externa:**
   - Las solicitudes deberán de ingresar a través de los canales administrativos establecidos por la alta dirección.
   - Se deberá de evaluar la solicitud y se notificará al solicitante el tratamiento a realizar a través de los medios autorizados por la alta dirección.
   - Si la solicitud procede, se notificará al propietario del activo de información para la gestionar la transferencia de la información.

Gestionar y preparar la información para su transferencia

El propietario del activo de información, deberá de coordinar con el personal interno a su cargo para elaborar o diligenciar la información solicitada según su clasificación:

1. **Información clasificada como pública**
   - Elaborar o consolidar la información requerida en el formato establecido.
   - Registrar la elaboración en el inventario de control de transferencia de información.
2. **Información clasificada como de uso interno, Restringido o confidencial:**
   - Elaborar o consolidar la información requerida en el formato establecido.
   - Asegurarse que la información a transferir no incumplan los derechos de autor ni de propiedad intelectual.
   - Aplicar los filtros necesarios para que la información a proporcionar no incumpla los acuerdos de privacidad y confidencialidad adquiridos por la institución.

- Aplicar los mecanismos de seguridad proporcionados por el responsable de la seguridad de la información, para que la información a transferir no sea alterada o modificada.
- Asegurarse que el solicitante firme los acuerdos de confidencialidad y no divulgación de la información proporcionada.
- Registrar la elaboración en el inventario de control de transferencia de información.

Autorizar la transferencia

El propietario del activo de información para autorizar la transferencia de información deberá:

- Realizar el control de la información que se ha elaborado o preparado, con base a la gestión y preparación de la información para su transferencia.
- Dar el visto bueno para la transferencia de la información.
- Firmar el documento de autorización de transferencia de información.
- Registrar la autorización en el inventario de control de transferencia de información.

Realizar la transferencia

Para efectuar la transferencia de la información se deberá de realizar de acuerdo a solicitud, por lo que:

- Para las solicitudes internas, serán atendidas a través de mensajería electrónica institucional.
- Para las solicitudes externas, la información será enviada a la oficina administrativa que ha notificado la solicitud a través de mensajería electrónica institucional.
- Para el caso de información que represente un gran volumen de almacenamiento, se deberá coordinar con el responsable de la seguridad de la información para coordinar la entrega a través de medios tecnológicos.

E.3.6. Consideraciones de información transferida

- Toda información que tenga la clasificación de pública, uso interno, Restringido o confidencial que haya sido aprobado para su transferencia a un personal externo mediante autorización del propietario del activo de información, será considerado como copia no controlada para la institución.

- Los mecanismos de seguridad aplicados a los activos de información para su transferencia, solo es para asegurar que la información no sea alterada o modificada.

E.3.7. Responsabilidades

Personal Externo: Es responsable de:

- Resguardar la información recibida bajo los términos, condiciones y acuerdos adquiridos con la institución.

Personal interno: Es responsable de:

- Aplicar y cumplir con lo establecido por el procedimiento de transferencia de información.
- Reportar a su jefe cualquier incidente en la transferencia de información.

Jefe o responsable de área: Es responsable de:

- Aplicar y cumplir con lo establecido en el proceso de transferencia de información.
- Velar que el personal a su cargo adopte las políticas de seguridad y cumpla con lo establecido por el proceso de transferencia de información.
- Reportar al responsable de la seguridad de la información cualquier incidente sucedido en la transferencia de la información.

Responsable de la seguridad de la información: Es responsable de:

- Mantener actualizado el procedimiento de transferencia de información.
- proveer los medios tecnológicos necesarios para apoyar la transferencia de información que represente un gran volumen de almacenamiento.
- Proveer las herramientas necesarias y recursos tecnológicos para resguardar la confidencialidad e integridad en la transferencia de información.
- Implementar los mecanismos necesarios para monitorizar el tipo de información que se comparte a través de mensajería electrónica.

E.4. Procedimiento de manejo de medios

Lógo institución	**Procedimiento de manejo de medios.**	**Código:**	XXXXXXXX
		Versión:	X.X
		Fecha:	dd / mm / aaaa

E.4.1. Objetivo

Establecer los lineamientos a seguir para preservar la confidencialidad e integridad de la información en el uso de medios de almacenamiento externo.

E.4.2. Alcance

Este procedimiento es aplicado a todo usuario que tiene autorización de acceso y uso de medios de almacenamiento externo.

E.4.3. Referencias

- Ley 1581 de 2012 - Régimen de Protección de datos personales.
- Ley 1273 de 2009 - Protección de la información y de los datos.
- ISO/IEC 27001:2013 - Sistemas de Gestión de la Seguridad de la Información.

E.4.4. Definiciones

Activo de información: Es un componente (datos, información, accesorios, hardware, software, instalaciones, recursos humanos, entre otros.) que tiene un valor de importancia para una organización y que puede estar expuesto a riesgos y amenazas.

Custodio del medio de almacenamiento: Es el encargado de resguardar la integridad del dispositivo y la confidencialidad de la información contenida.

Confidencialidad: Propiedad de la información que hace que los datos solo puedan estar disponible y accesible por los usuarios que cuenten con la autorización correspondiente.

Integridad: Propiedad que consiste en preservar la exactitud y estado completo delos datos almacenados en la base de datos.

Medio removible: Es un dispositivo externo (CD, DVD, memorias flash USB, Disco duro externo entre otras.) utilizado para almacenar información.

Propietario del activo de información: Es el jefe o responsable del área donde se ha generado o se almacena el activo de información.

E.4.5. Manejo de medios

Solicitud de uso de puertos periféricos USB y unidades ópticas de CD/DVD

Para habilitar los puertos periféricos USB o unidades ópticas de CD/DVD de los equipos workstation, se deberá:

1. **usuario interno:**
   - Deberá de justificar y solicitar al propietario del activo la gestión para habilitar de los puertos periféricos USB o unidades ópticas de CD/DVD.
2. **Propietario del activo:**
   - Deberá de evaluar si la justificación y solicitud amerita gestionar la habilitación.
   - Dirigir la solicitud al responsable de la seguridad de información, habilitar de los puertos periféricos USB o unidades ópticas de CD/DVD de una activo de información específico.
3. **Responsable de la seguridad de la información:**
   - Deberá de gestionar con su equipo de trabajo, la habilitación de los puertos periféricos USB o unidades ópticas de CD/DVD del activo solicitado.
   - Aplicar las configuraciones y controles establecidos para controlar la posible aparición e infección de código malicioso.
   - Implementar los mecanismos de seguridad para el borrado seguro de datos y cifrado de información.
   - Hacer firmar al propietario del activo de información y al personal interno el acuerdo de responsabilidad del uso de puertos periféricos USB o unidades ópticas de CD/DVD.

Uso de medios removibles

- El usuario antes de conectar el medio removible, deberá de asegurarse que se encuentre en perfecto estado, que no se encuentre sucio o que no tenga o haya tenido contacto con ningún tipo de líquido.
- EL usuario interno antes de utilizar el medio removible, deberá de realizar el escaneo contra código malicioso.

- El usuario no deberá dejar conectado el medio removible una vez se haya dejado de usar o al retirarse de su estación de trabajo.
- El usuario deberá resguardar el medio removible que contenga información en un lugar seguro para prevenir el acceso a personal no autorizado.

Transferencia de medios removibles

- Tomar todas las medidas de seguridad para prevenir la perdida o extravío del medio removible durante el transporte.
- Tomar todas las medidas de seguridad para prevenir que el medio removible pueda ser afectado por contacto con líquidos, golpes o caídas.
- Considerar cifrar la información almacenada en el medio removible, para salvaguardar la confidencialidad e integridad de la información en casos de robo o asaltos.
- La persona diferente al usuario interno que pretenda o vaya transportar el medio removible fuera de las instalaciones de la institución, será considerado como custodio.

Disposición de medios removibles

1. **medios removibles con conexión USB (Disco duro externo o memorias)**
   - El usuario deberá de realizar el borrado seguro de los datos almacenados.
   - El usuario deberá resguardar el medio removible en un lugar seguro.
2. **medios removibles ópticos (CD/DVD)**
   - El usuario deberá resguardar el medio removible en un lugar seguro para prevenir el acceso y uso a personal no autorizado.
   - Si su uso ya no es dispensable, evaluar la necesidad de destrucción del medio removible.

E.4.6. Responsabilidades

usuario interno: Es responsable de:

- Hacerse responsable por el uso de los medios removibles.
- Aplicar las medidas de seguridad proporcionadas por el responsable de la seguridad de la información.

Custodio: El custodio deberá:

- Hacerse responsable por garantizar que se preserve la confidencialidad e integridad de la información y del medio removible durante su transporte.

Propietario del activo de información: El propietarios deberá:

- Hacerse responsable por las autorizaciones del uso de los puertos periféricos USB o unidades ópticas de CD/DVD.
- Asegurarse que el usuario interno use los puertos periféricos y medios removibles de acuerdo a lo establecido para el uso de medios removibles.

Responsable de la seguridad de la información: El propietarios deberá:

- Gestionar la atención de las solicitudes de habilitación de puertos periféricos USB o unidades ópticas de CD/DVD.
- Proporcionar los mecanismos de seguridad para el uso adecuado de medios removibles.

Elaboró	**Revisó**	**Aprobó**
Nombres y Apellidos:	Nombres y Apellidos:	Nombres y Apellidos:
Cargo:	Cargo:	Cargo:

F. Anexo: Comparación de mecanismos de seguridad de bases de datos NoSQL

BD / Mecanismo	Autenticación	Autorización	Cifrado de datos en tránsito	Cifrado de datos en reposo
Mongo DB	- SCRAM (Salted Challenge Response Authentication Mechanism). - x.509 Autenticación de certificados. **Nota:** Autenticación proxy LDAP y autenticación Kerberos, disponibles en MongoDB Enterprise.	- Control de acceso basado en roles (RBAC). **Nota:** No habilitado por defecto.	- Certificados TLS/SSL. **Nota:** - Modo FIPS, disponible en MongoDB Enterprise. - A partir de la versión 4.0, TLS 1.0 está desactivado en los sistemas en los que está disponible TLS 1.1+.	- Motor de almacenamiento encriptado. - Cifrado de nivel de aplicación. **Nota:** Disponible para empresas.
CouchDB	- Admin Party. - Basic. - Cookies. - Autenticación Proxy. **Nota:** - Certificados SSL/TSL soportados desde la versión 1.1.0. - A partir de la versión 1.3.0, utiliza el algoritmo de cifrado PBKDF2 para las contraseñas almacenadas.	- Basado en roles y privilegios.	- TLS / Certificados SSL. **Nota:** soporta de forma nativa sin el uso de un servidor proxy.	- No proporciona cifrado para sus datos.
Hbase	- HDFS, ZooKeeper. - Kerberos. **Nota:** No comprueba la autenticación de forma predeterminada.	- Acceso simple para el usuario (basado en roles). - Asegurando el acceso a HDFS y ZooKeeper. - Etiquetas de control de acceso (ACL). **Nota:** - ACL está disponible a partir de HBase 0.92 (CDH4). - No verifica la autorización por defecto.	- SSL/TLS. - SASL. **Nota:** Debe estar configurado para tener una conexión segura (HTTPS).	- Cifrado de datos transparente (TDE).
Cassandra	- Nombre de usuario y contraseña. - Cassandra Auténtica Integrada. - Autenticación JMX estándar. **Nota:** No comprueba la autenticación de forma predeterminada.	- Autorización interna. - Acceso JMX. **Nota:** No verifica la autorización por defecto.	- Certificados TLS/SSL.	- Cifrado de datos transparente (TDE).
BigTable	- Identidad en la nube. **Nota:** Servicio gratuito.	- Gestión de acceso (Cloud IAM). - Basado en roles y privilegios.	- Certificados TLS.	- Cifrado por defecto. - Claves de cifrado administradas por el cliente (CMEK) con Cloud KMS. - Claves de cifrado proporcionadas por el cliente (CSEK).
DynamoDB	- Gestión de Identidad y Acceso (IAM) de AWS. **Nota:** Servicio gratuito.	- Basado en roles y privilegios de AWS Identity and Access Management.	- Certificados SSL/TLS. **Nota:** Todos los datos están cifrados excepto los datos DAX (servicio indirecto de almacenamiento en caché de escritura).	- CMK propiedad de AWS (predeterminado). - CMK administrado por AWS (pagado). **Nota:** AWS KMS es el servicio que gestiona el cifrado.
Neo4j	- Proveedor de autenticación nativa. **Nota:** Sólo para empresas. - Proveedor de autenticación LDAP. - Autenticación Kerberos de inicio de sesión único. - Proveedores de autenticación de plugins personalizados.	- Roles nativos **Nota:** Sólo para empresas. - Control de acceso basado en roles. - Control de acceso a sub gráfos.	- Certificados SSL/TLS.	- Sólo da recomendaciones y no especifica ningún mecanismo de cifrado. - Recomienda el uso de Bitlocker.
GraphDB	- Local - LDAP (estándar x.500.) - Autenticación básica. **Nota:** La autenticación local genera tokens de acceso.	- Basado en roles (RBAC1) y privilegios a través de Spring Security.	- Certificados SSL/TLS seleccionados con el servidor Tomcat. - Protocolo HTTPS en el servidor. **Nota:** Los ajustes de certificación deben estar habilitados.	- No proporciona cifrado para sus datos. **Nota:** Los datos almacenados en el disco duro en binario.

Tabla F.1.: Mecanismos de seguridad disponibles en bases de datos NoSQL
Fuente: Elaboración propia.

G. Pruebas de requisitos funcionales

G.1. Autenticación de Usuario

Acceso con usuario o clave incorrectos

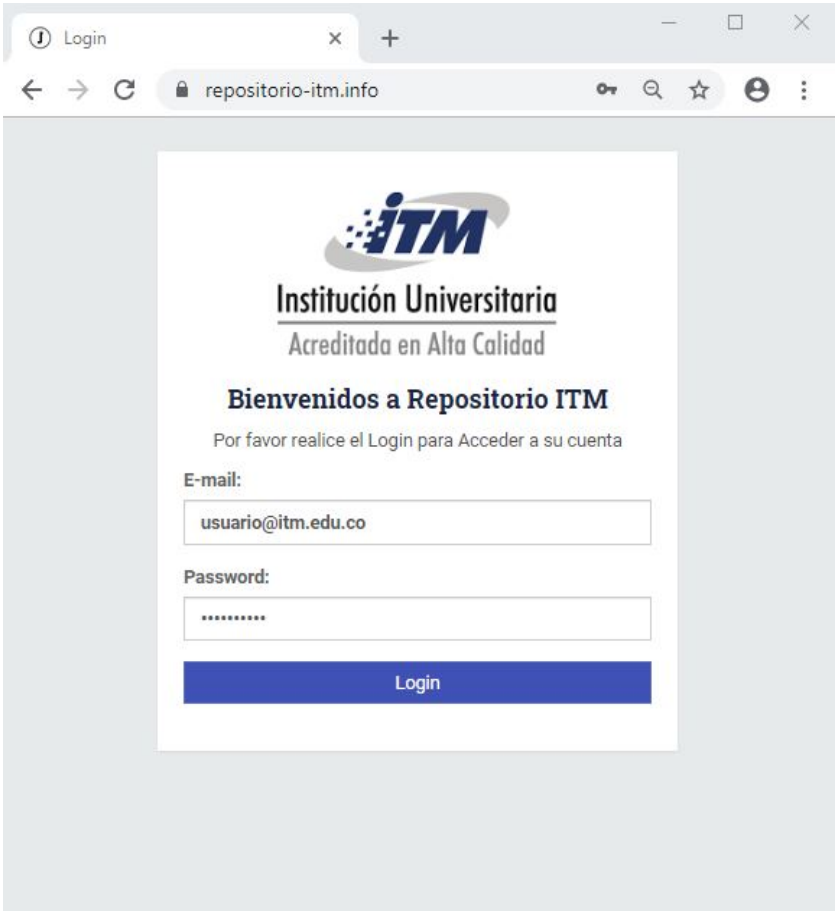


Figura G.1.: Formulario login

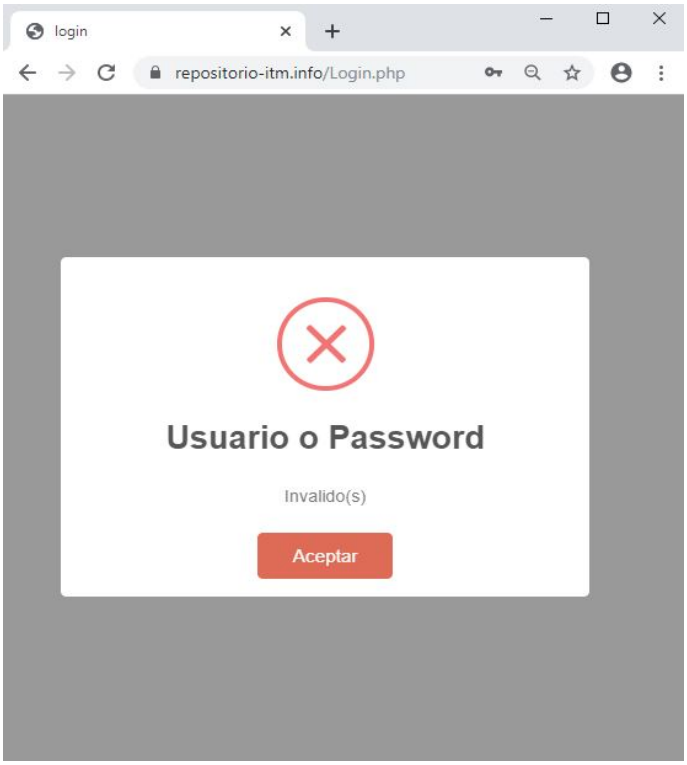


Figura G.2.: Credenciales incorrectos

Validación de tocken incorrecto

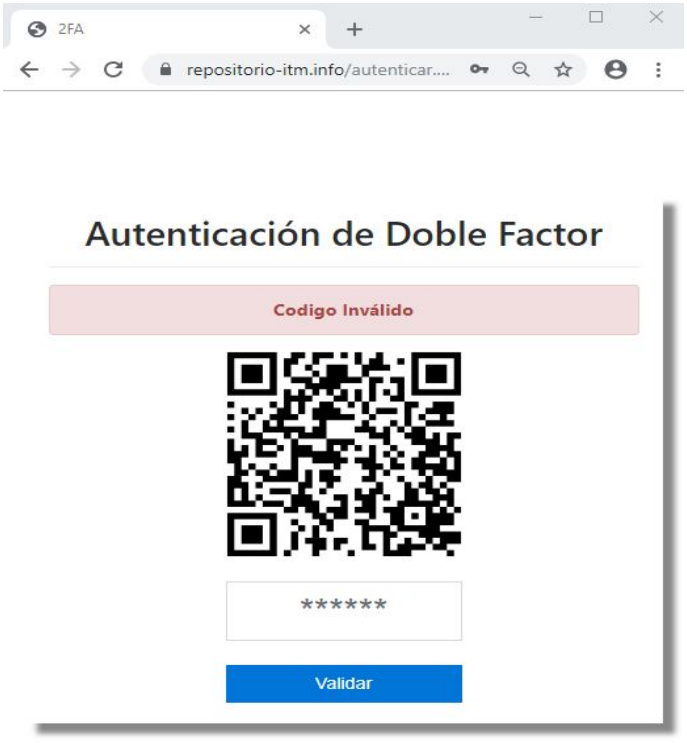


Figura G.3.: Tocken incorrecto

Acceso con usuario, clave y tocken correctos

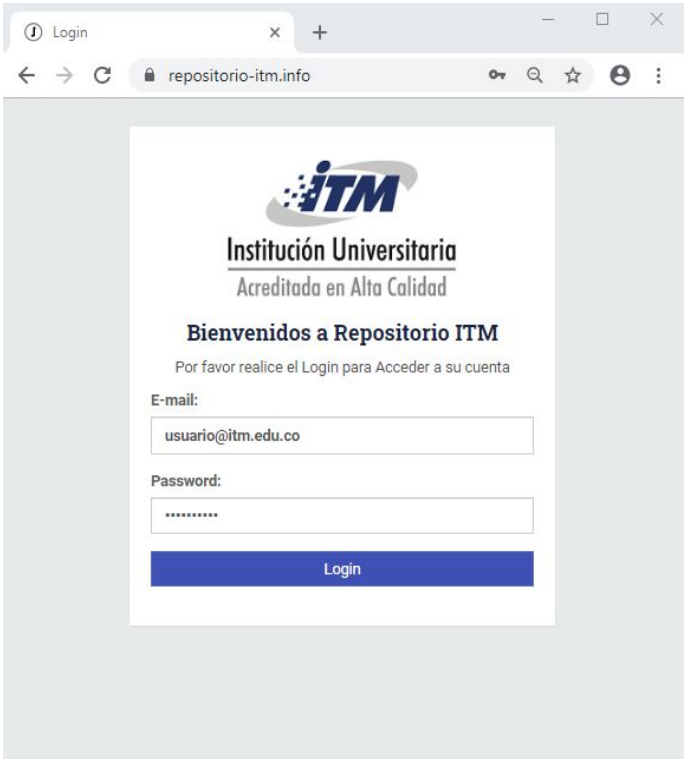


Figura G.4.: Formulario login

Figura G.5.: Generación de tocken de validación de ID

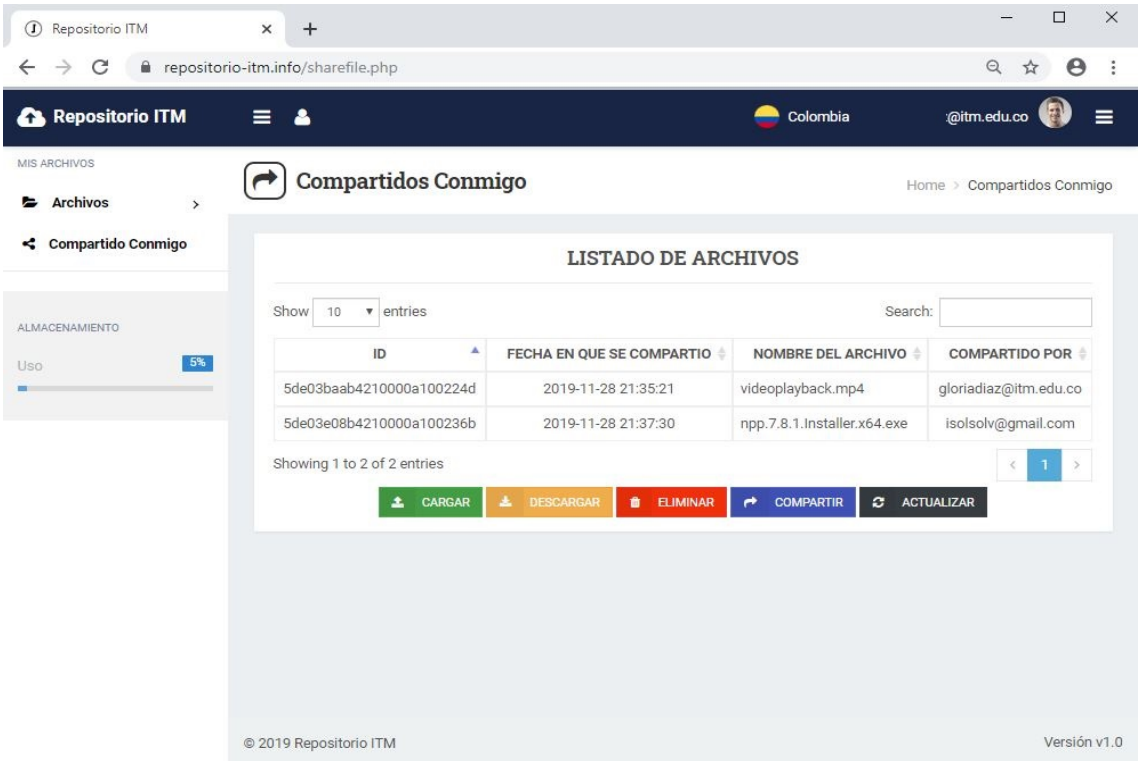


Figura G.6.: Interfaz de Usuario (Front-end).

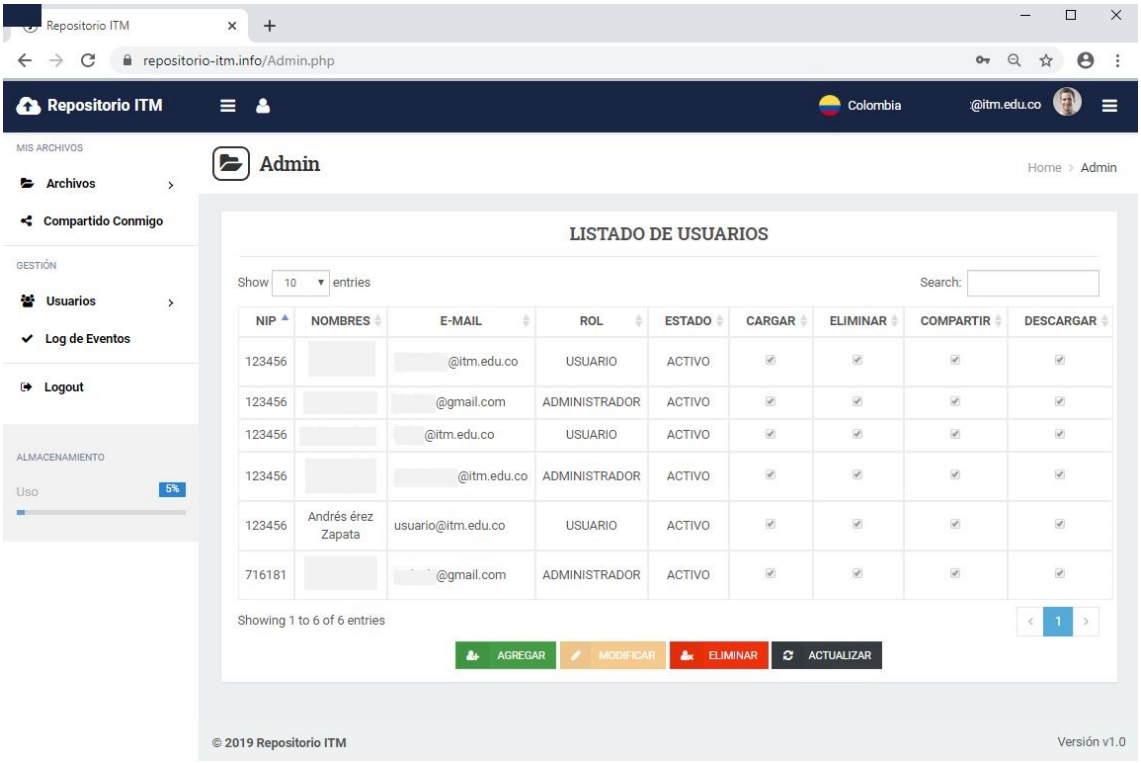


Figura G.7.: Interfaz de Administrador (Front-end).

G.2. Gestión de usuarios

Crear usuarios

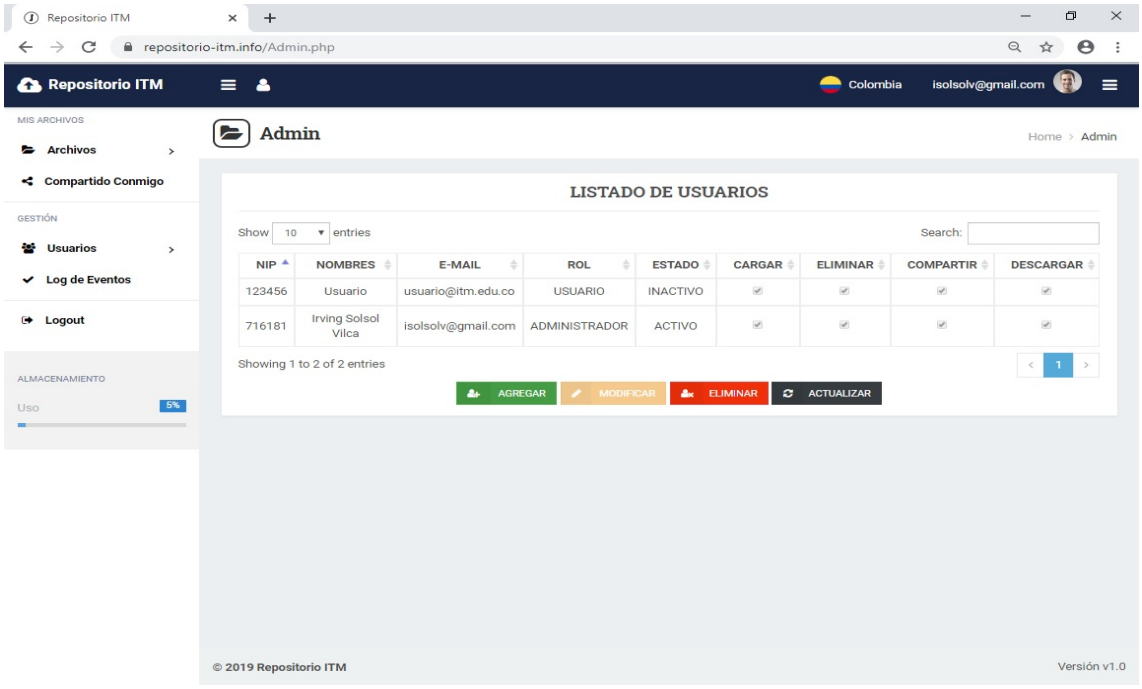


Figura G.8.: Listado de usuarios.

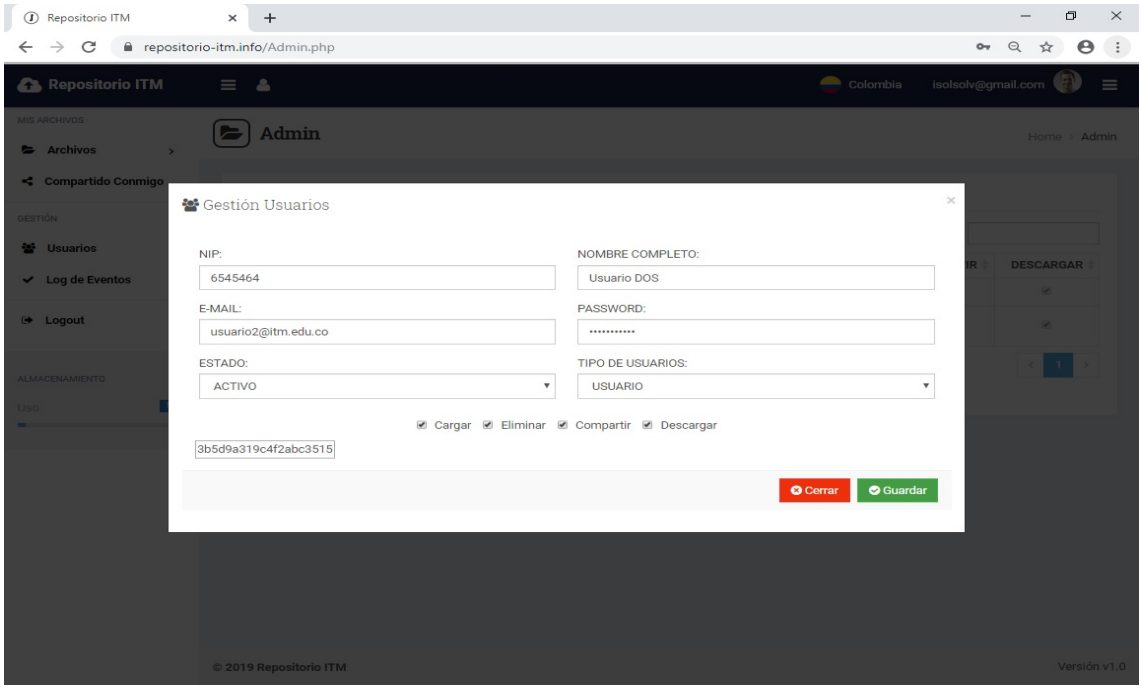


Figura G.9.: Formulario de creación de usuario.

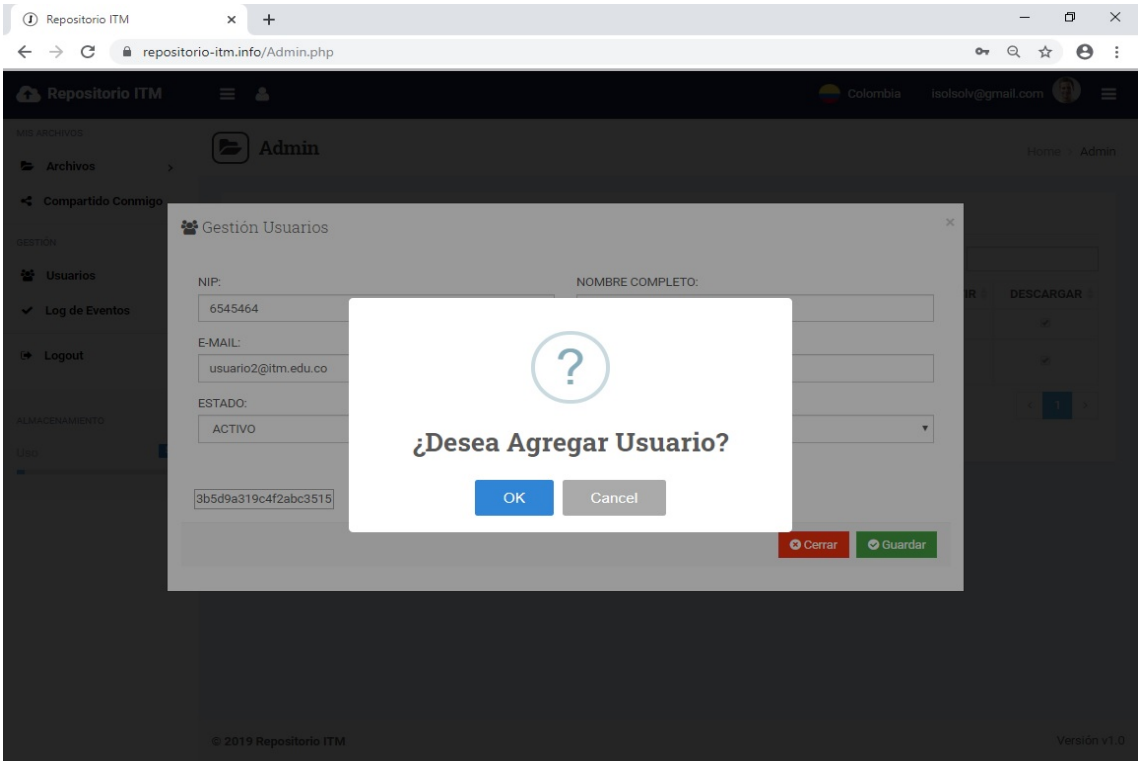


Figura G.10.: Mensaje de confirmación de agregar usuario.

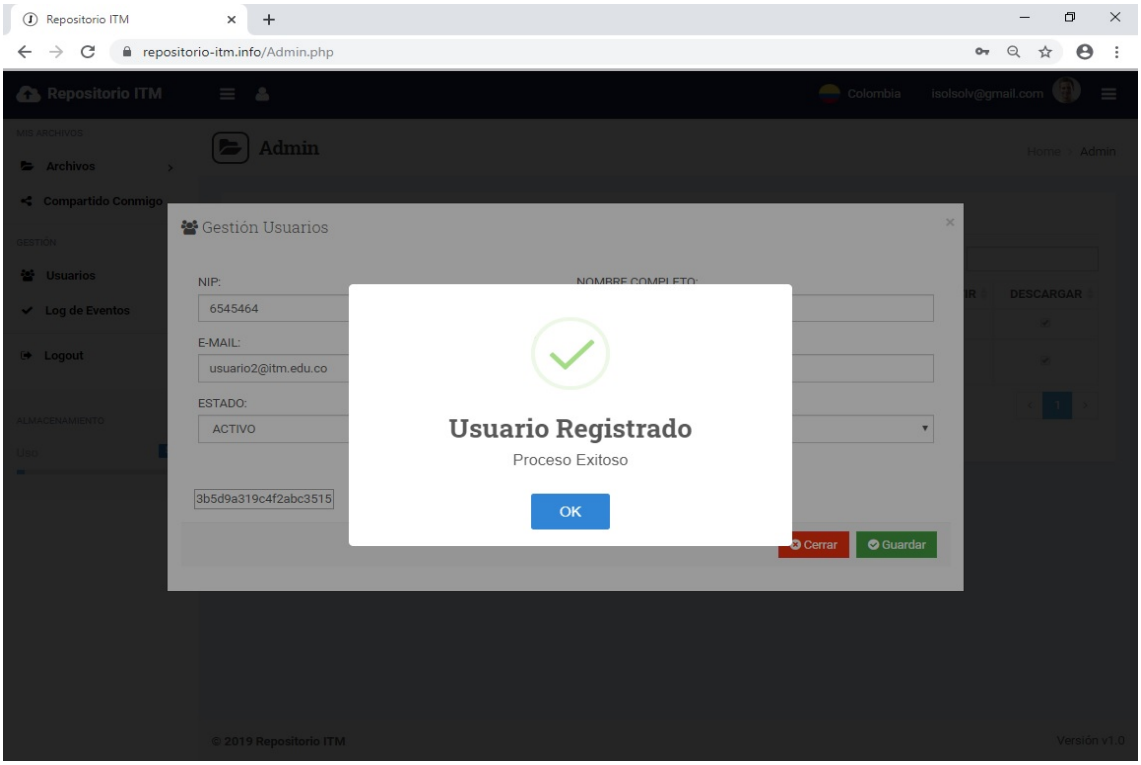


Figura G.11.: Mensaje de usuario registrado.

Modificar usuarios

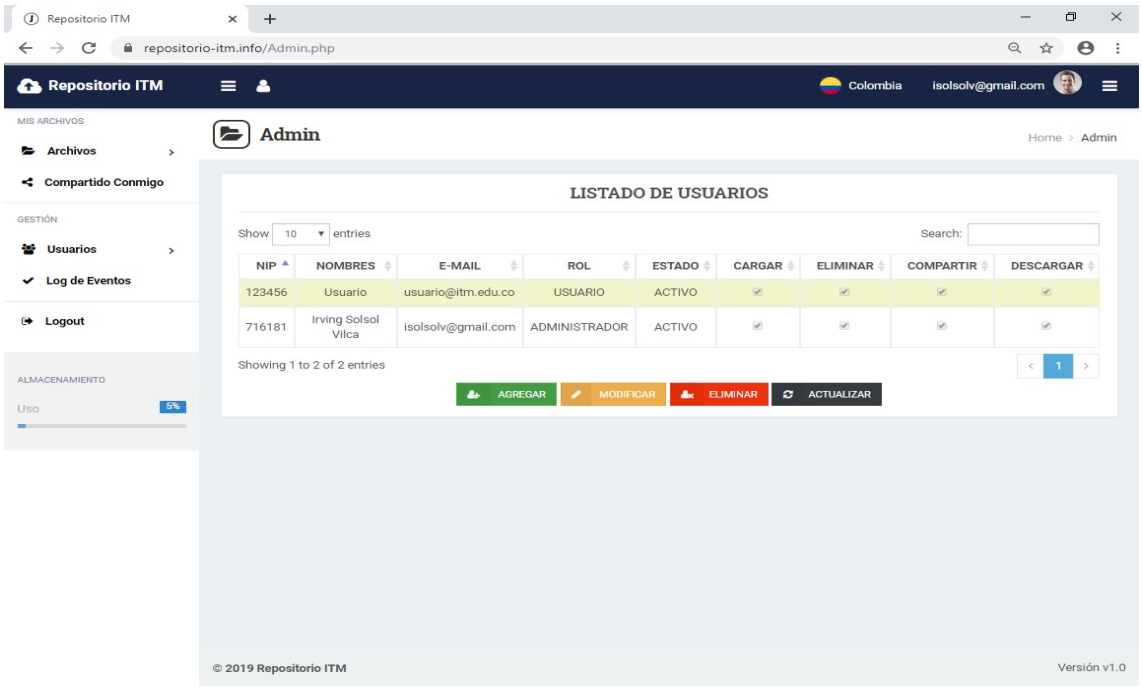


Figura G.12.: Listado de usuarios.

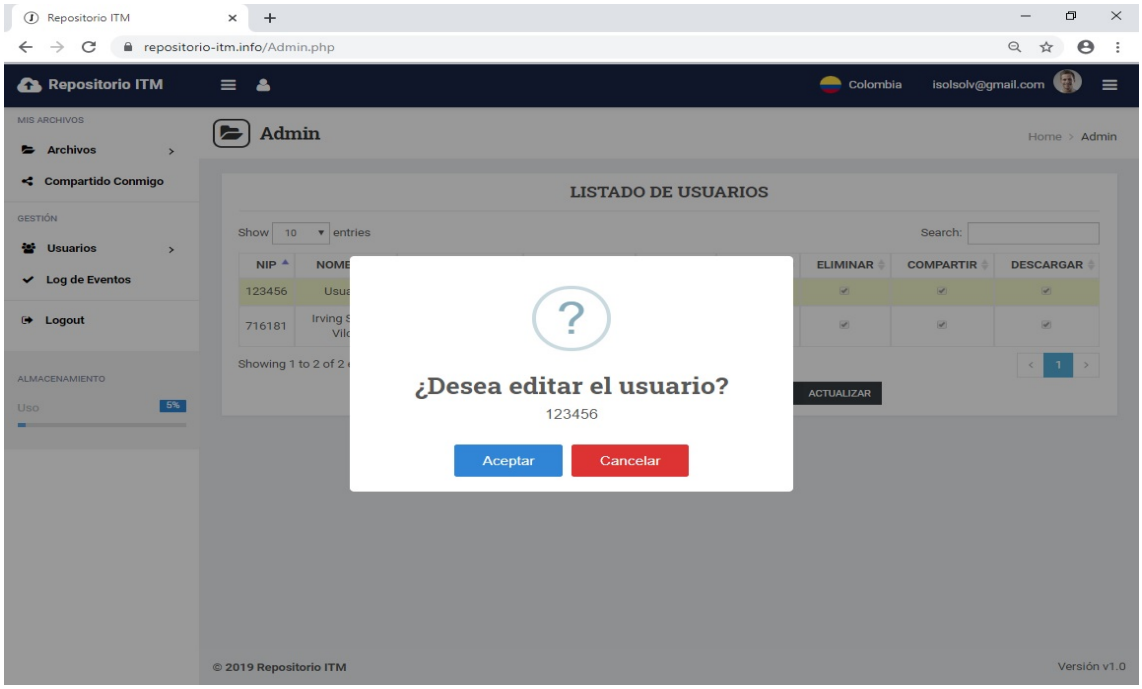


Figura G.13.: Mensaje de confirmación de modificación.

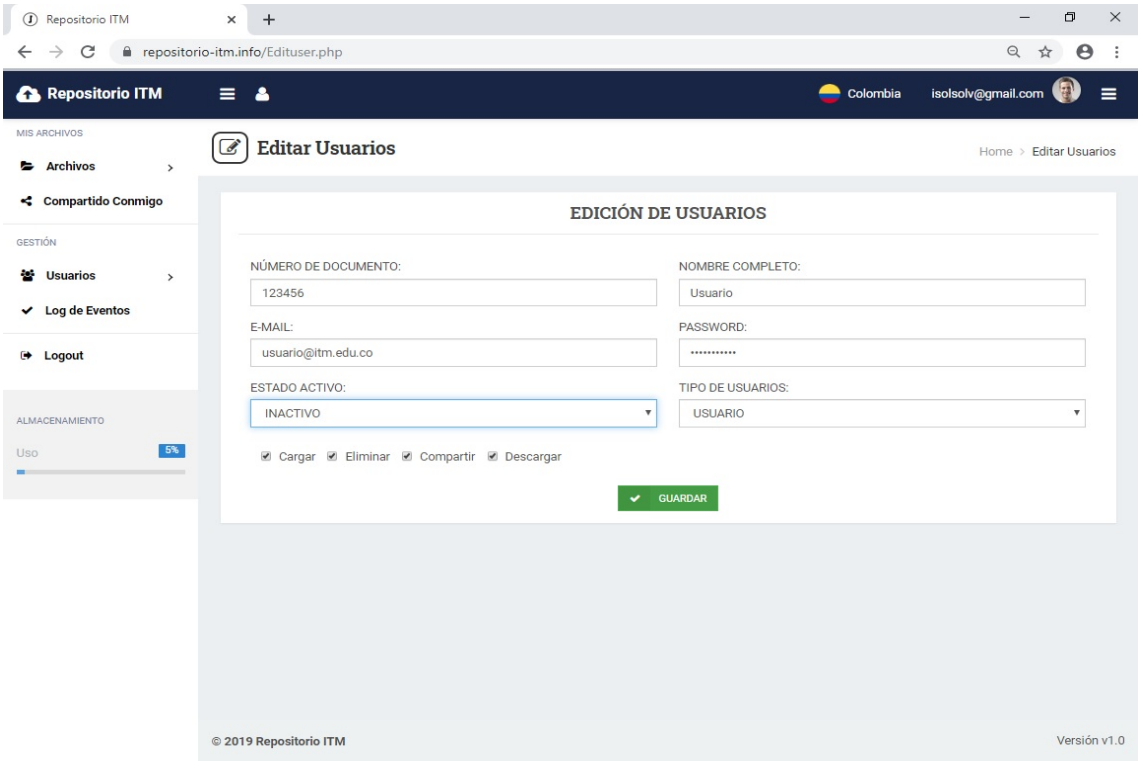


Figura G.14.: Formulario para modificar usuario.

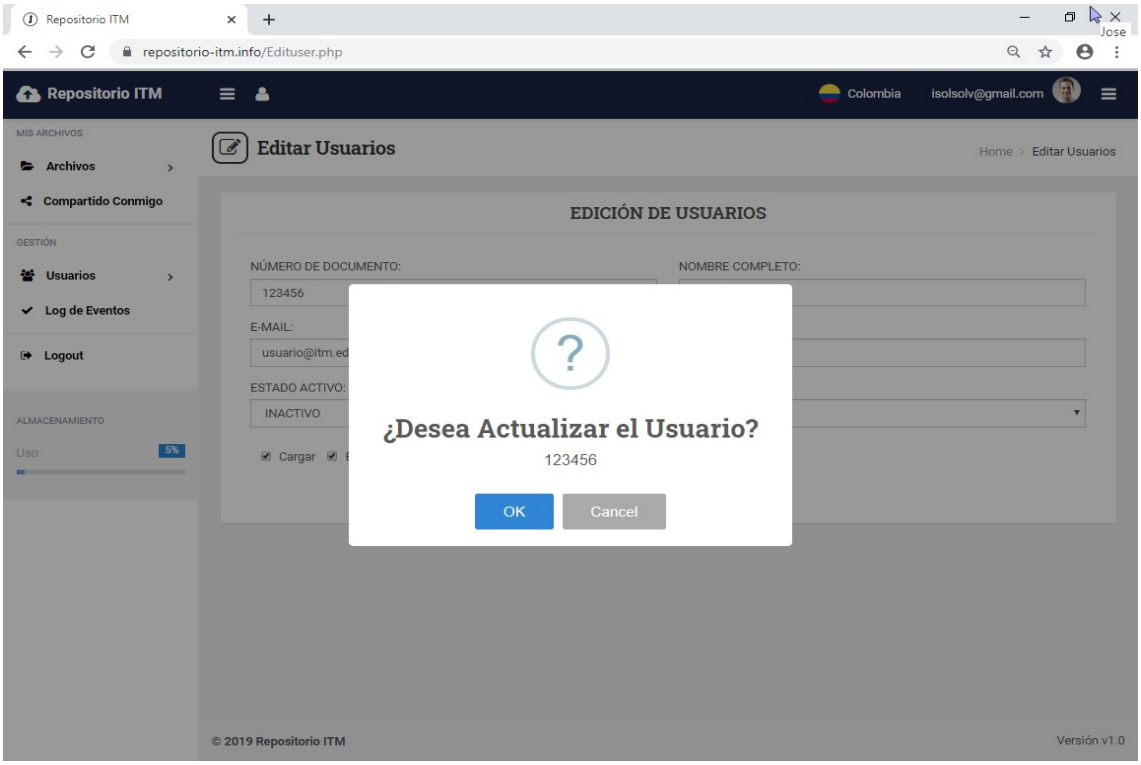


Figura G.15.: Mensaje de confirmación de modificación.

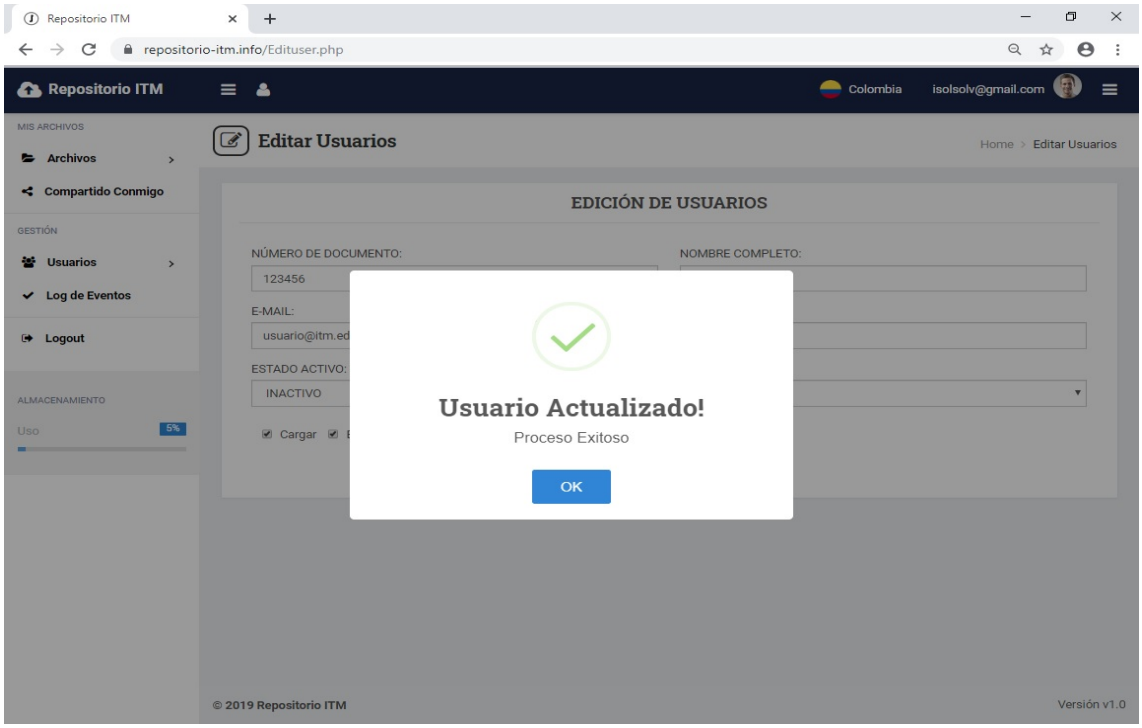


Figura G.16.: Mensaje de modificación exitosa.

Eliminar usuarios

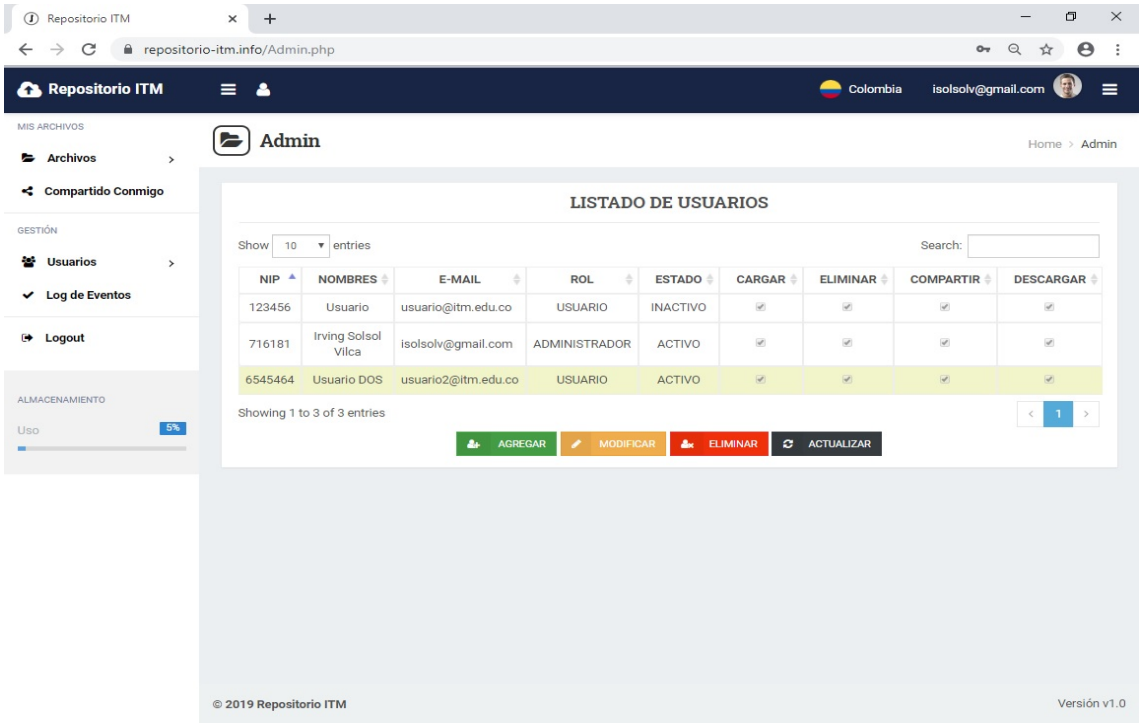


Figura G.17.: Listado de usuarios.

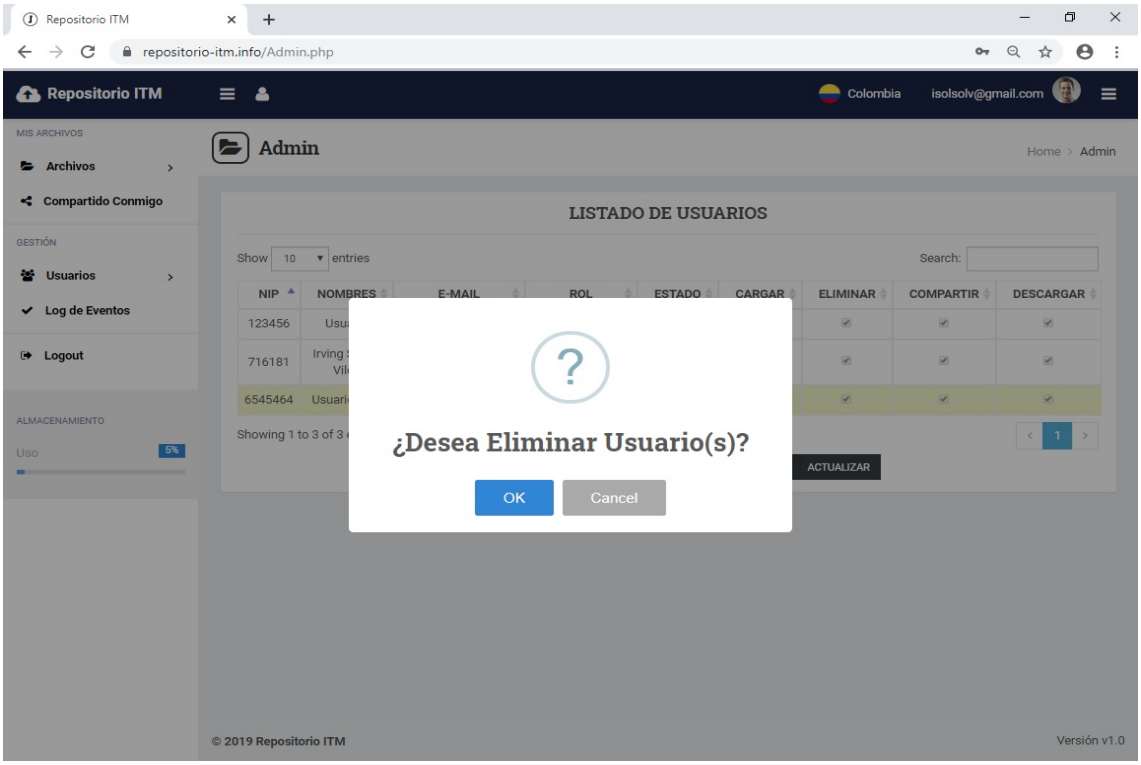


Figura G.18.: Mensaje de confirmación para eliminar.

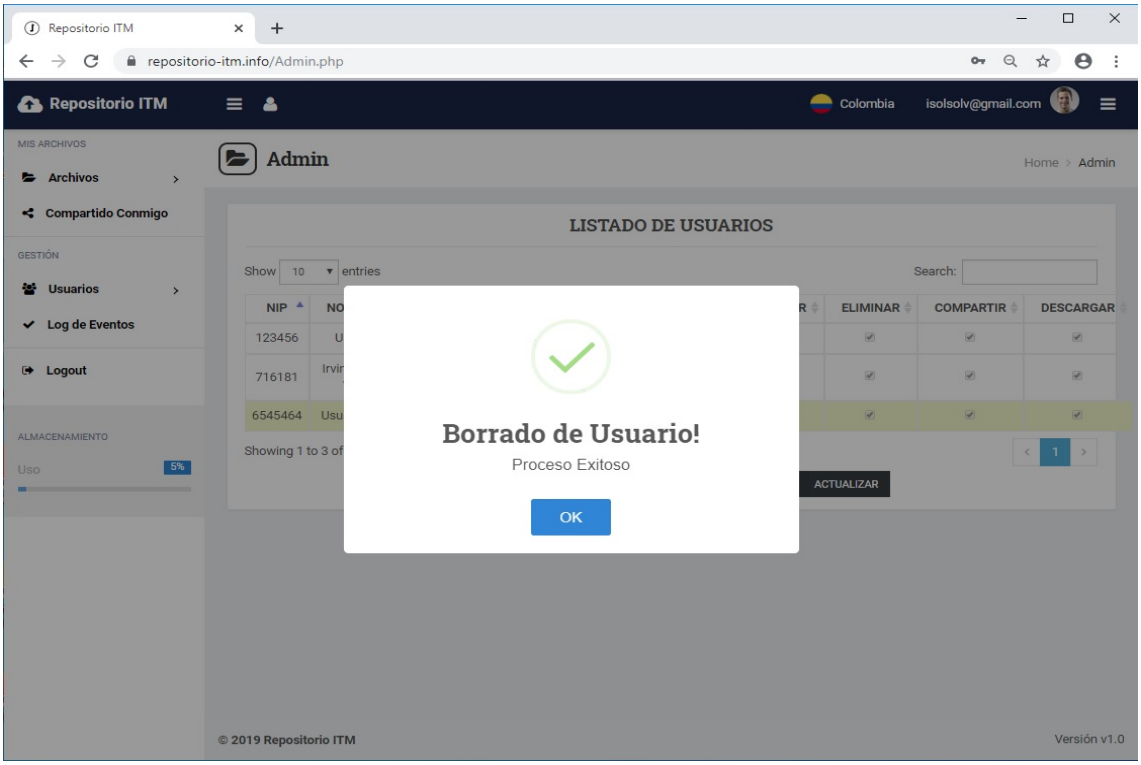


Figura G.19.: Mensaje de usuario elimando.

G.3. Gestión de archivos

Carga de datos

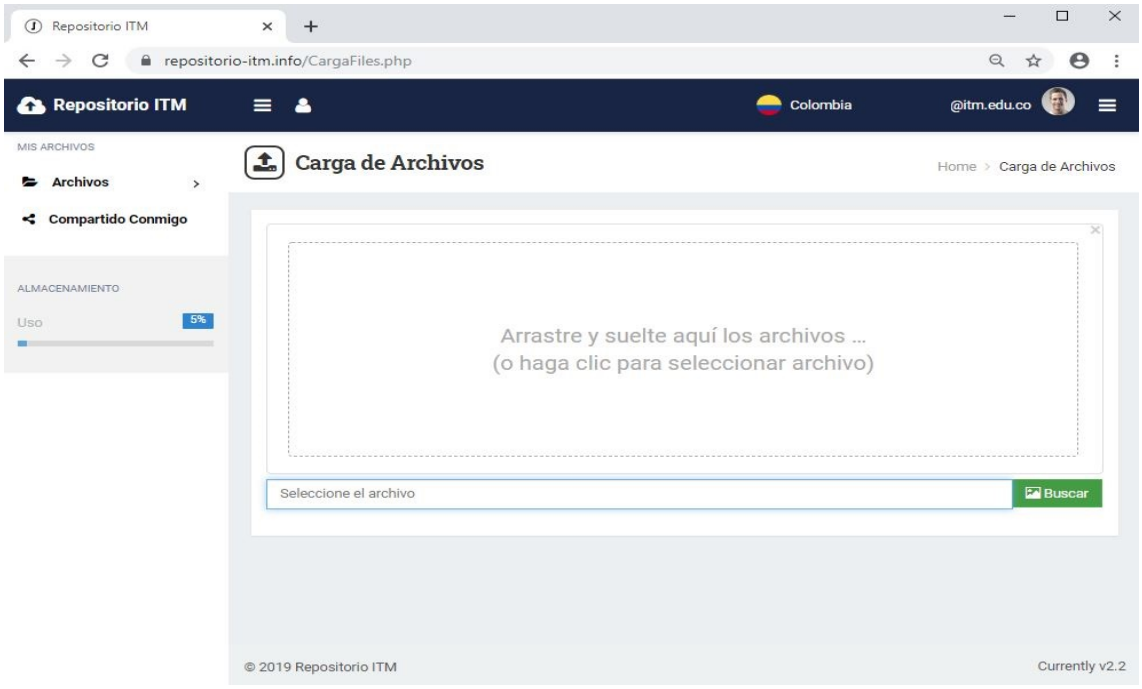


Figura G.20.: Interfaz de carga.

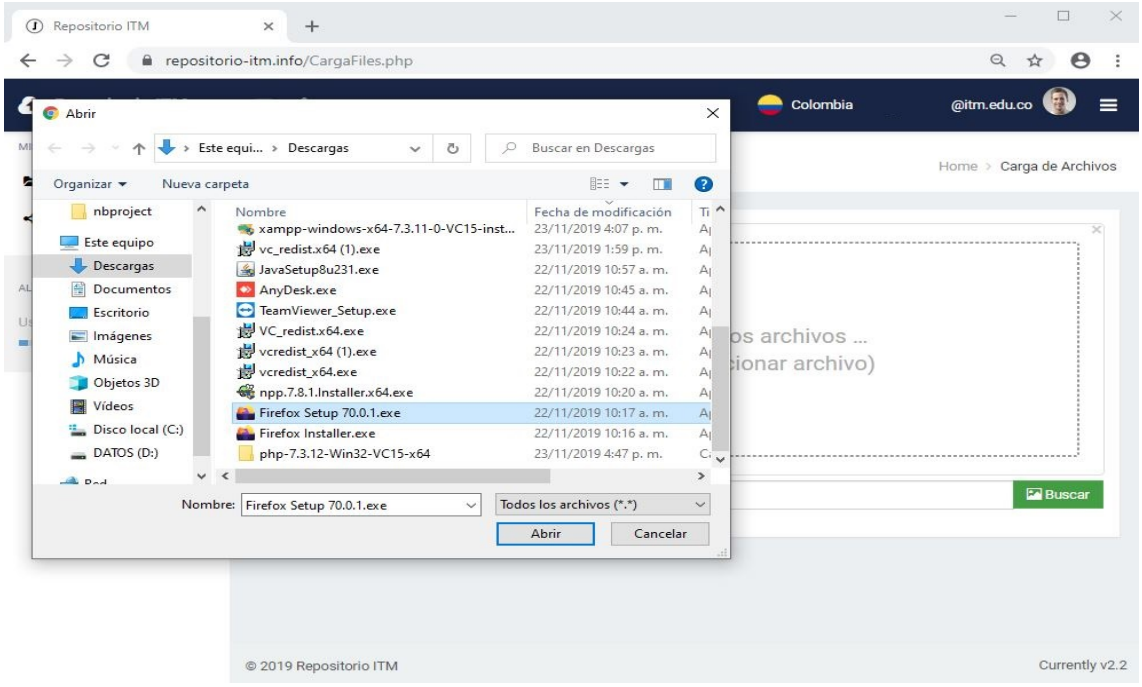


Figura G.21.: Selección de archivo.

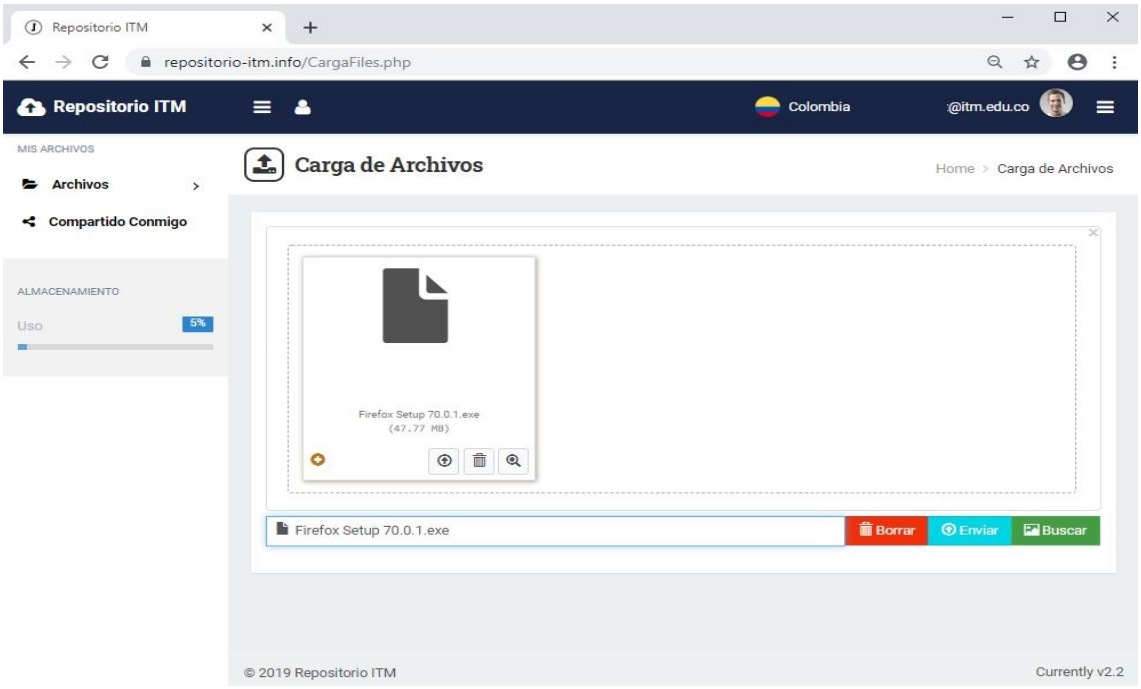


Figura G.22.: Archivo seleccionado.

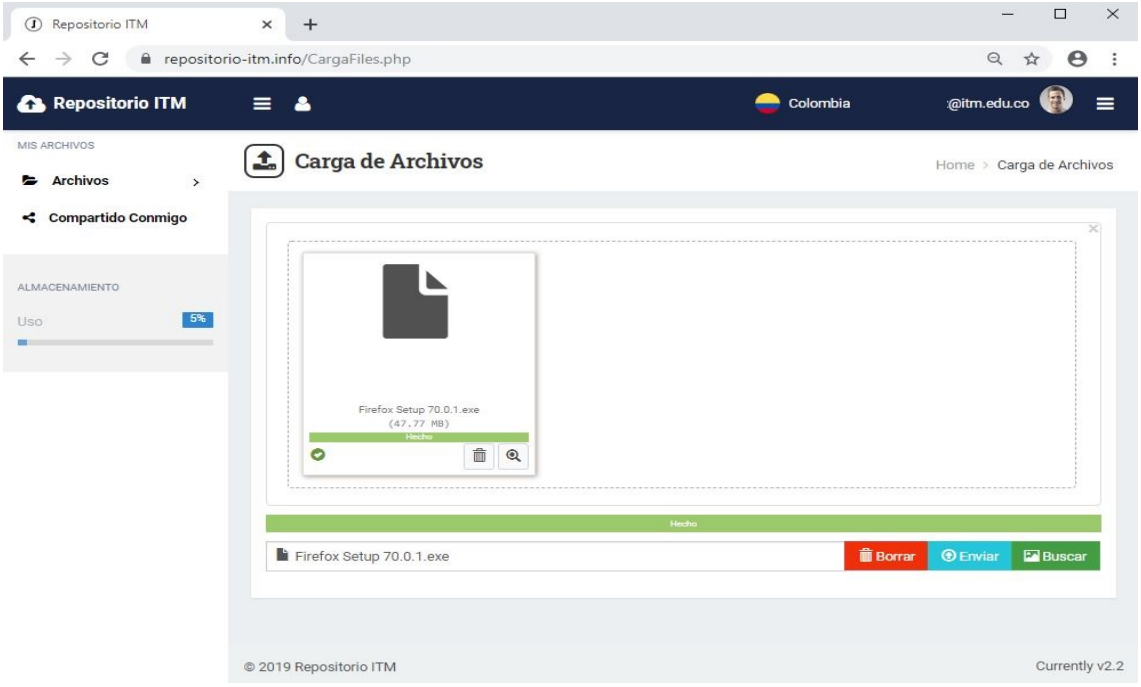


Figura G.23.: Proceso de carga exitosa.

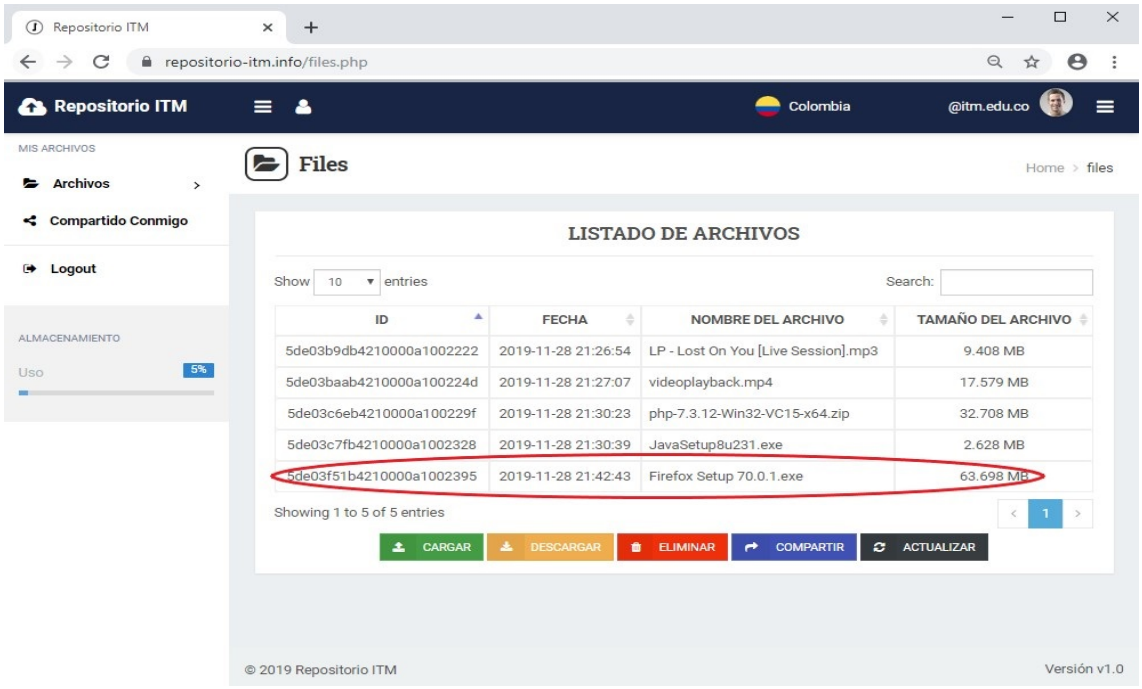


Figura G.24.: Lista de archivo cargado.

Descarga de datos

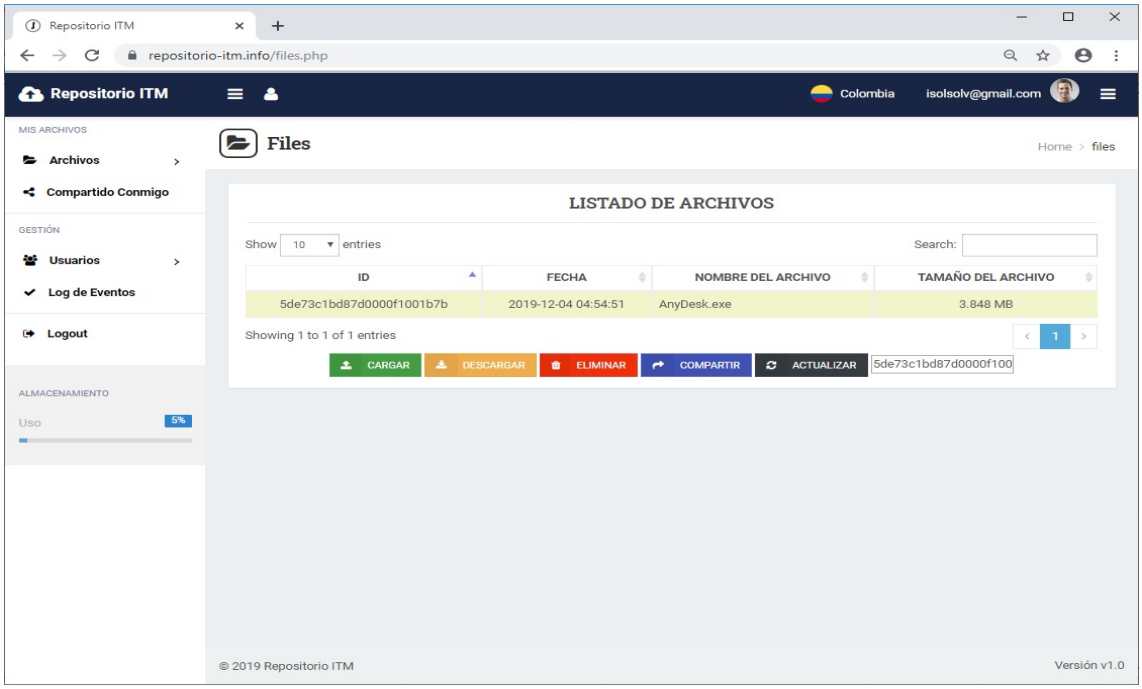


Figura G.25.: Listado de archivos.

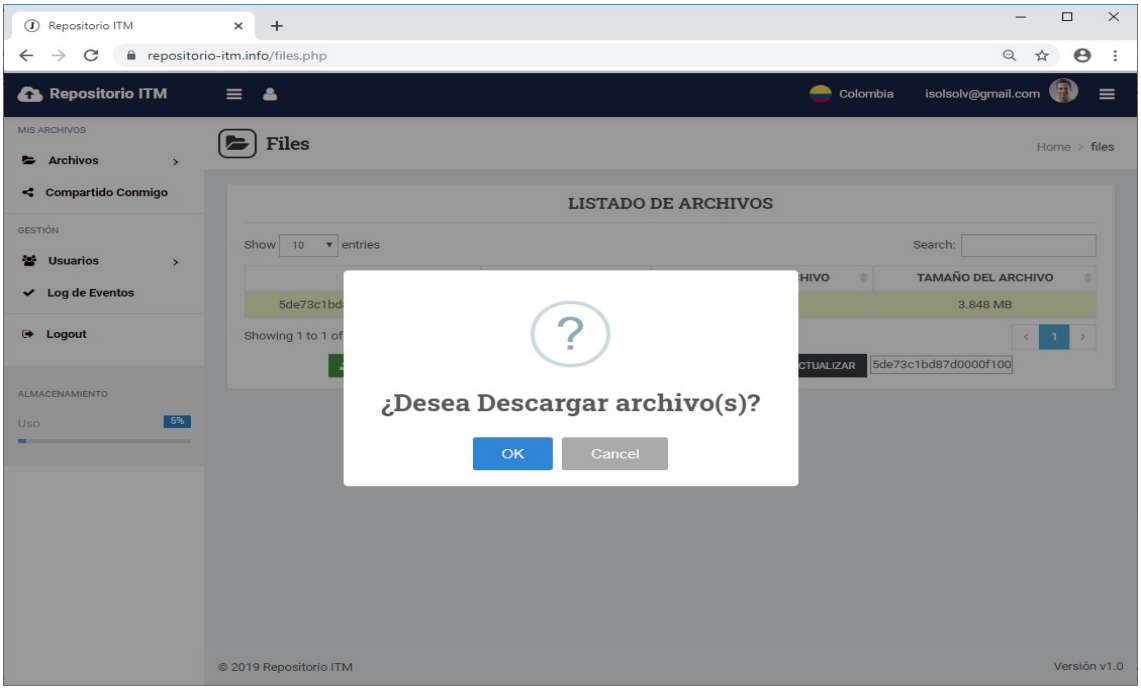


Figura G.26.: Mensaje de confirmación de descarga.

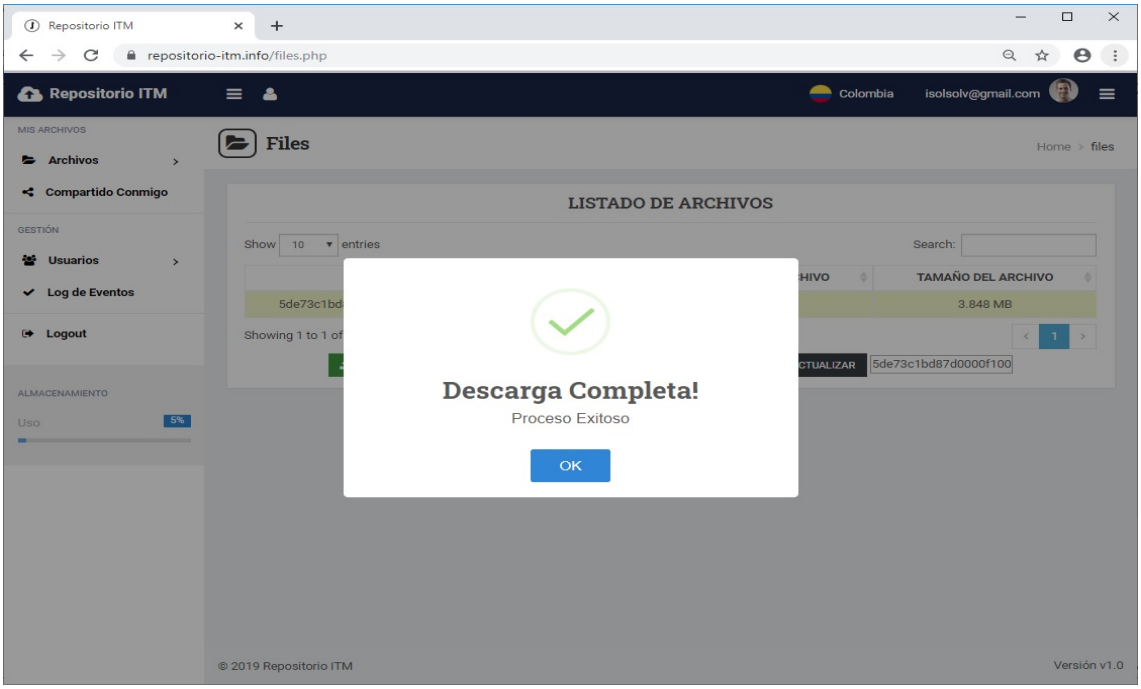


Figura G.27.: Mensaje de descarga exitosa.

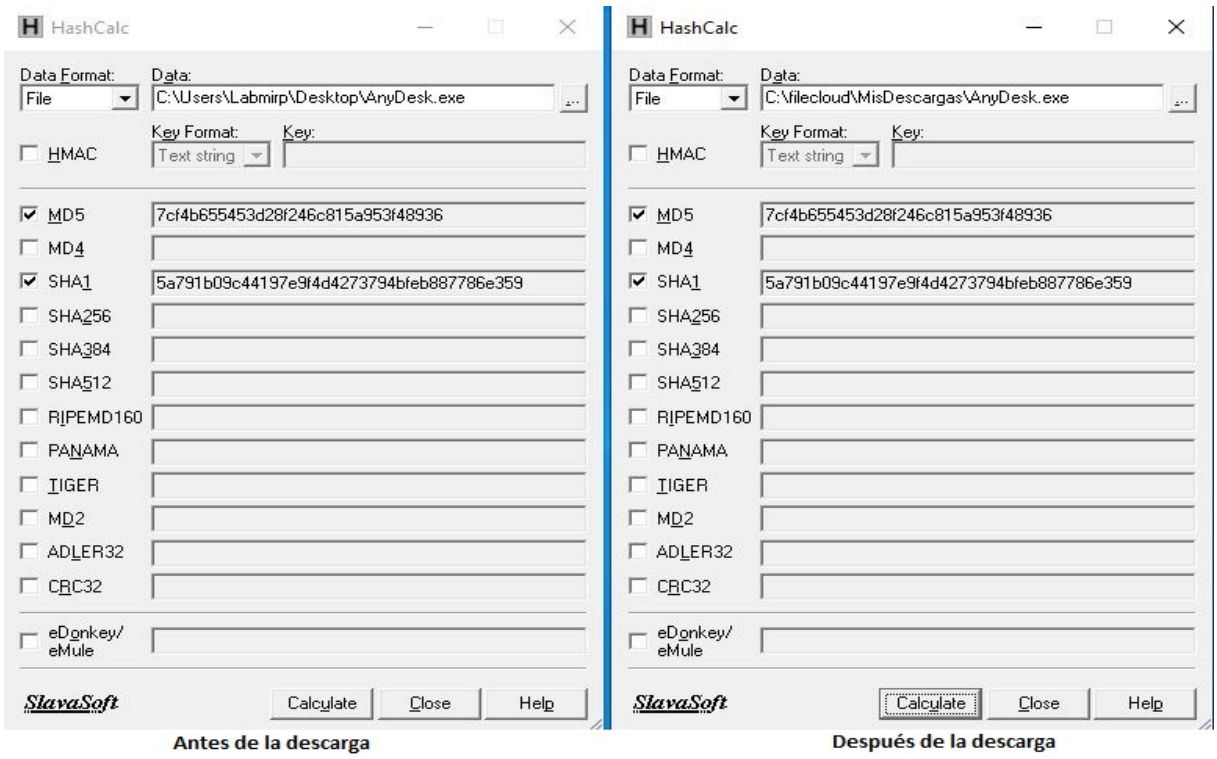


Figura G.28.: Verificación de integridad del archivo.

Compartición de datos

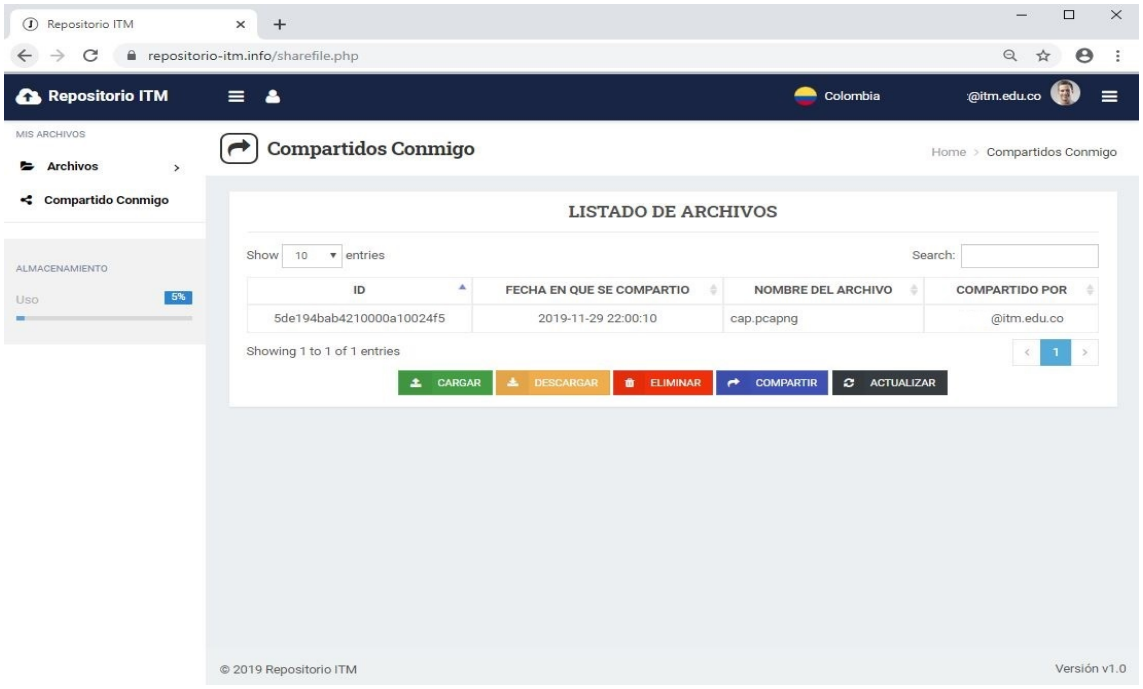


Figura G.29.: Lista de archivo cargados.

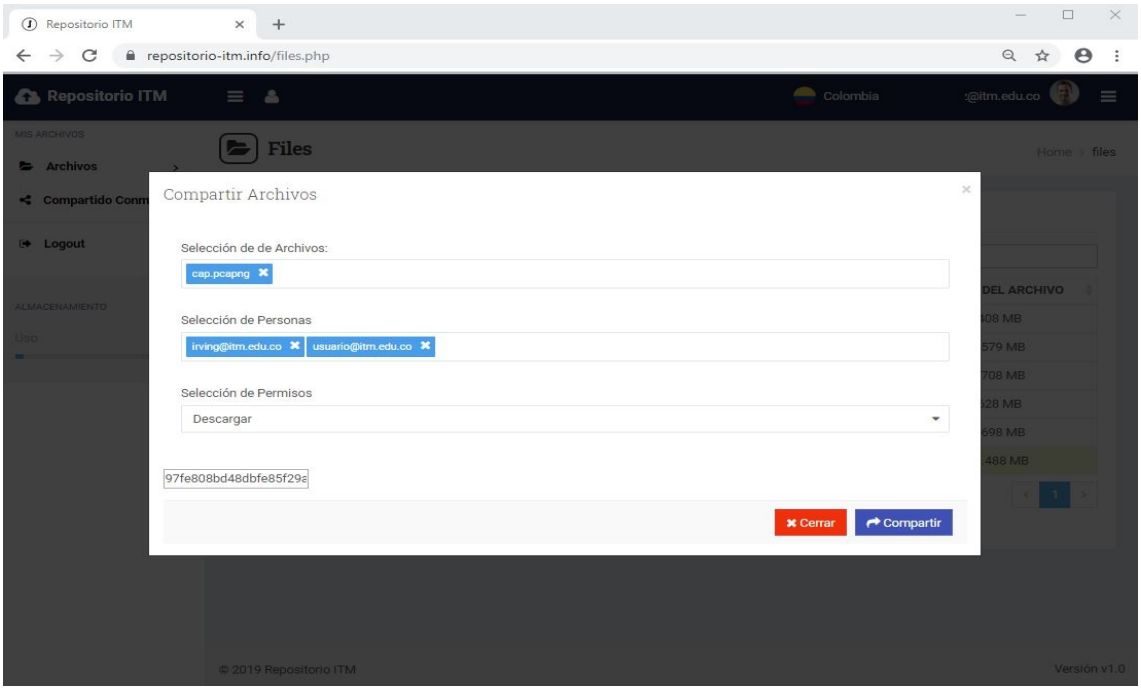


Figura G.30.: proceso de compartir archivos.

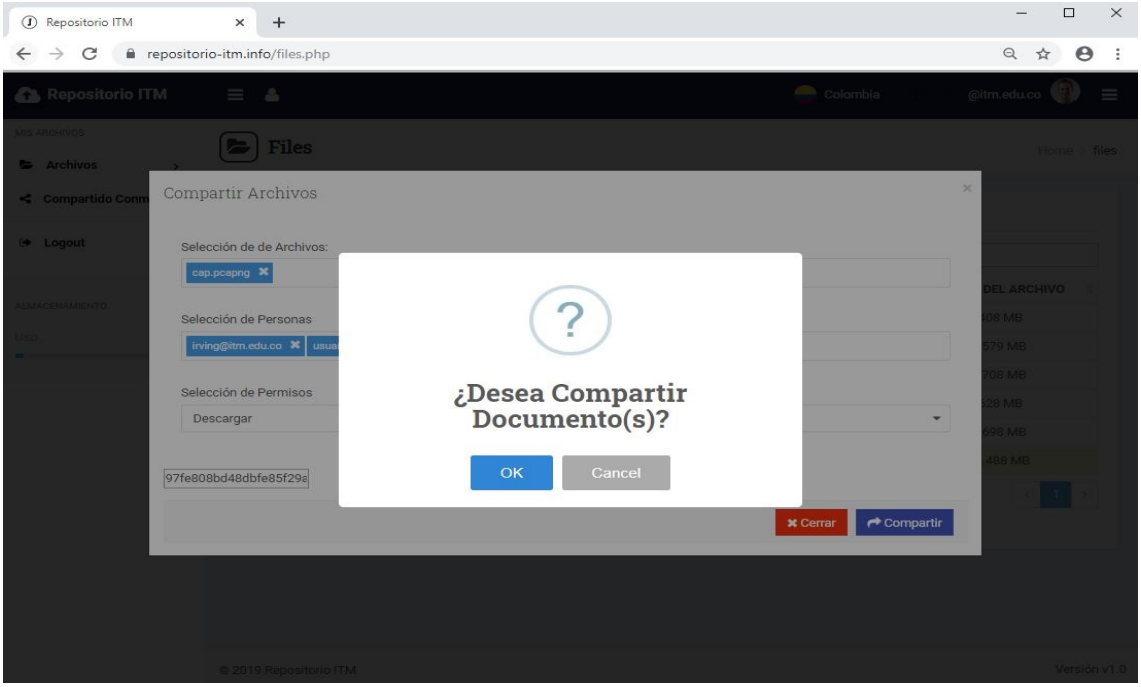


Figura G.31.: Mensaje de advertencia.

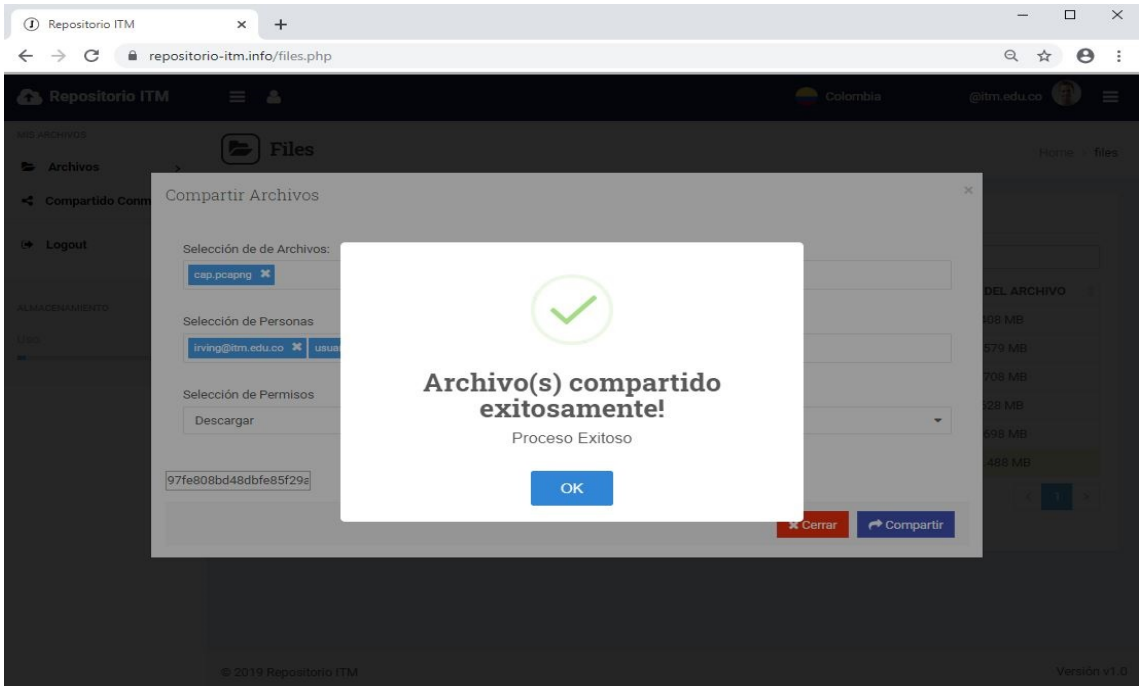


Figura G.32.: Compartición exitosa.

G.4. Auditoría

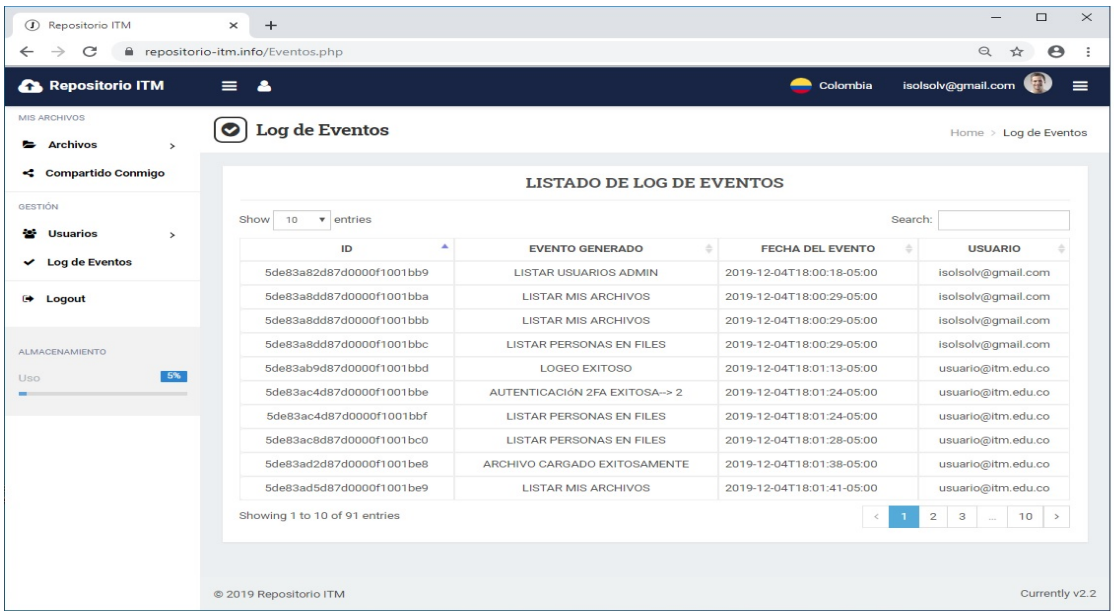


Figura G.33.: Registro de eventos de usuario.

G.5. Cifrado de datos

Cifrado de datos en tránsito

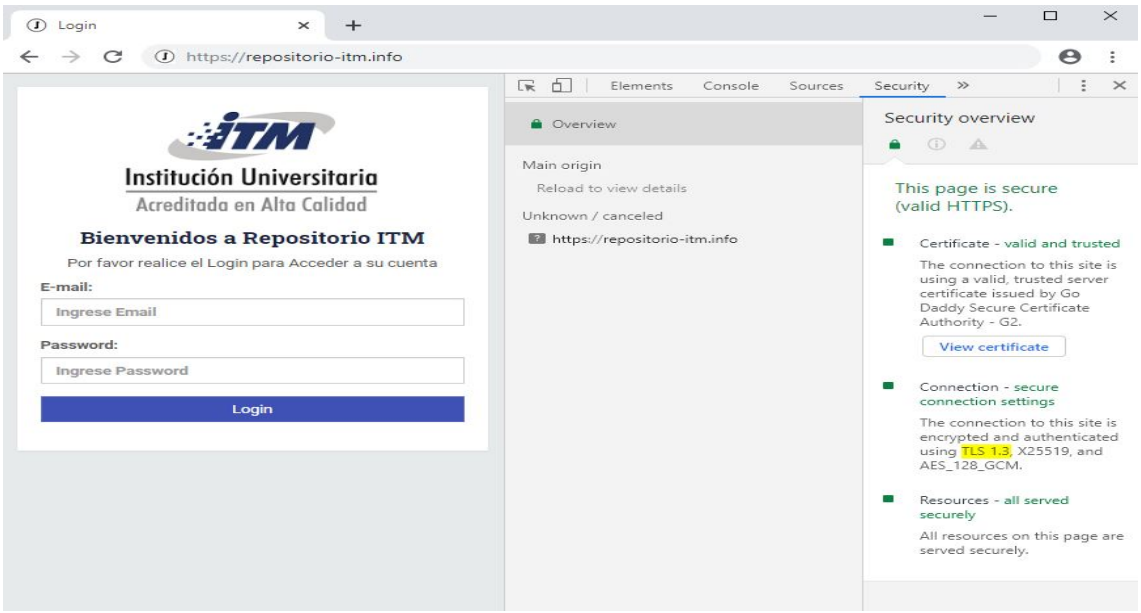


Figura G.34.: Certificado digital TLS 1.3 anexado al dominio.

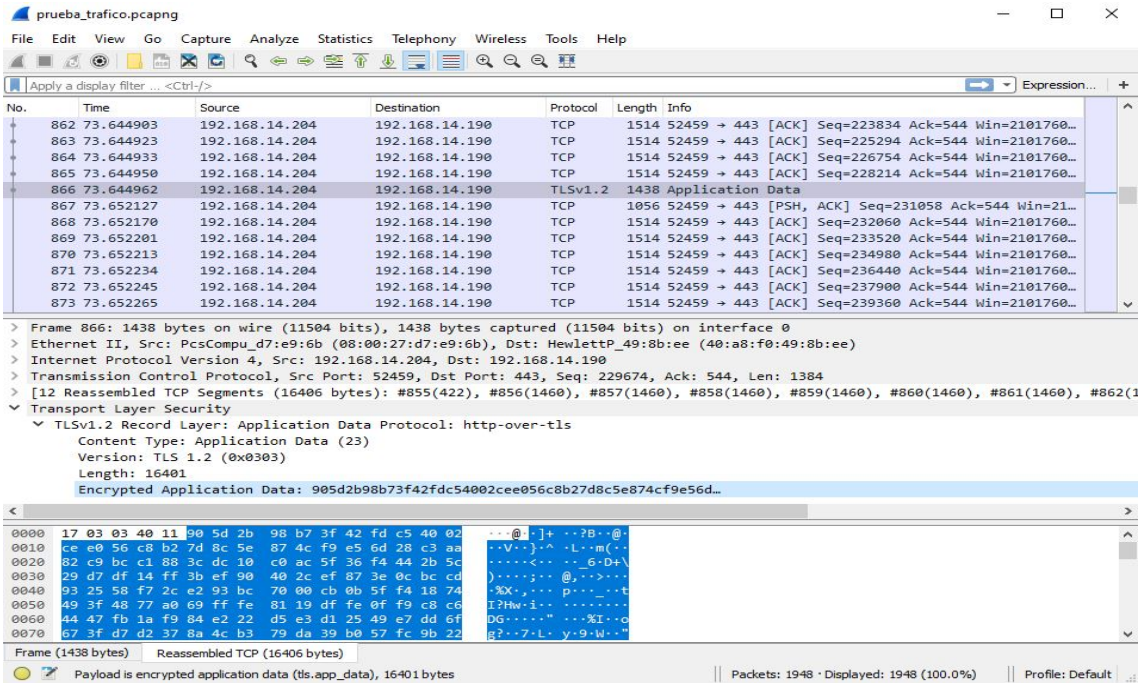


Figura G.35.: Captura de trafico de datos en tránsito.

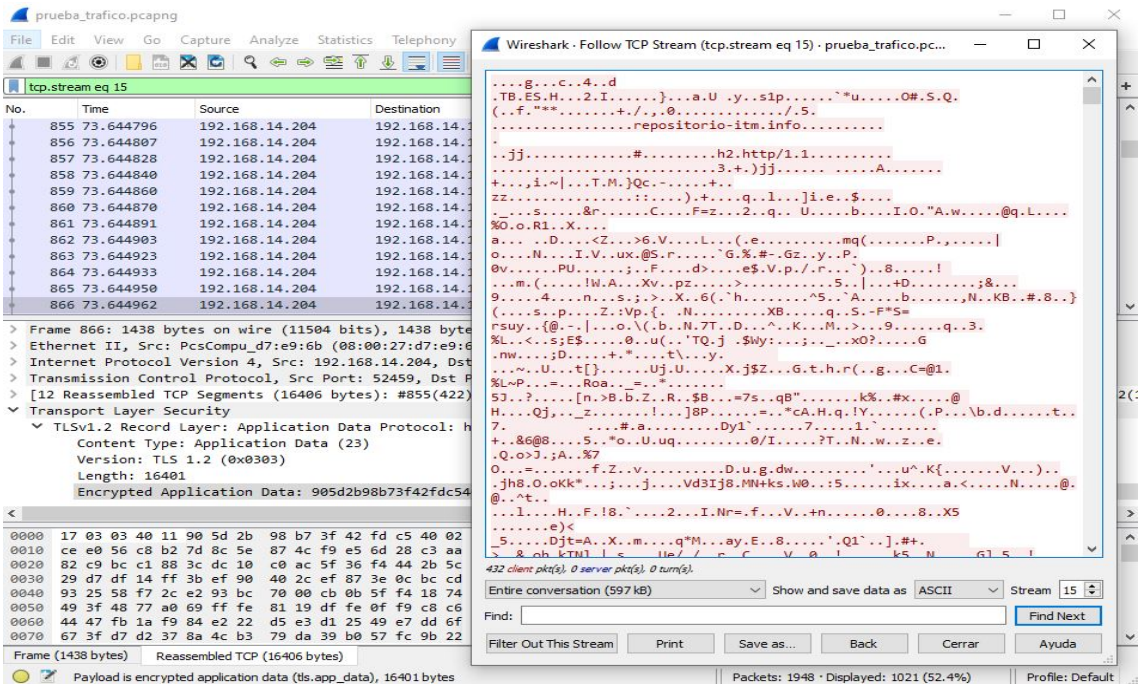


Figura G.36.: Detalle de paquete de dato en tránsito capturado.

Cifrado de datos en reposo

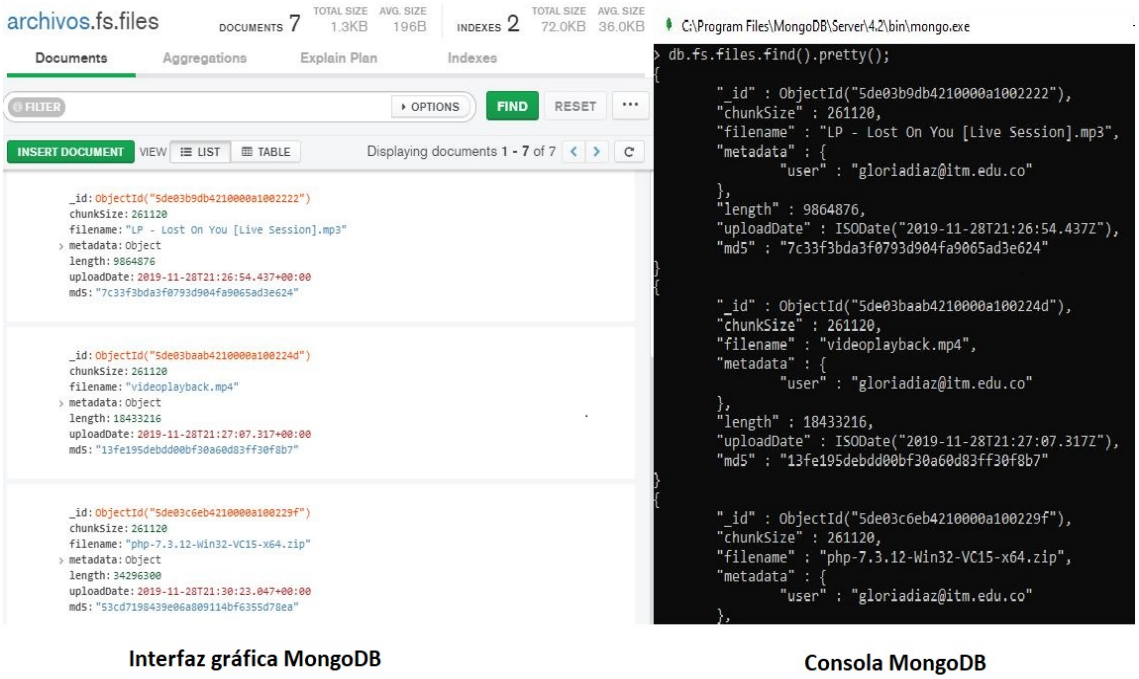


Figura G.37.: Información almacenada en fs.files.

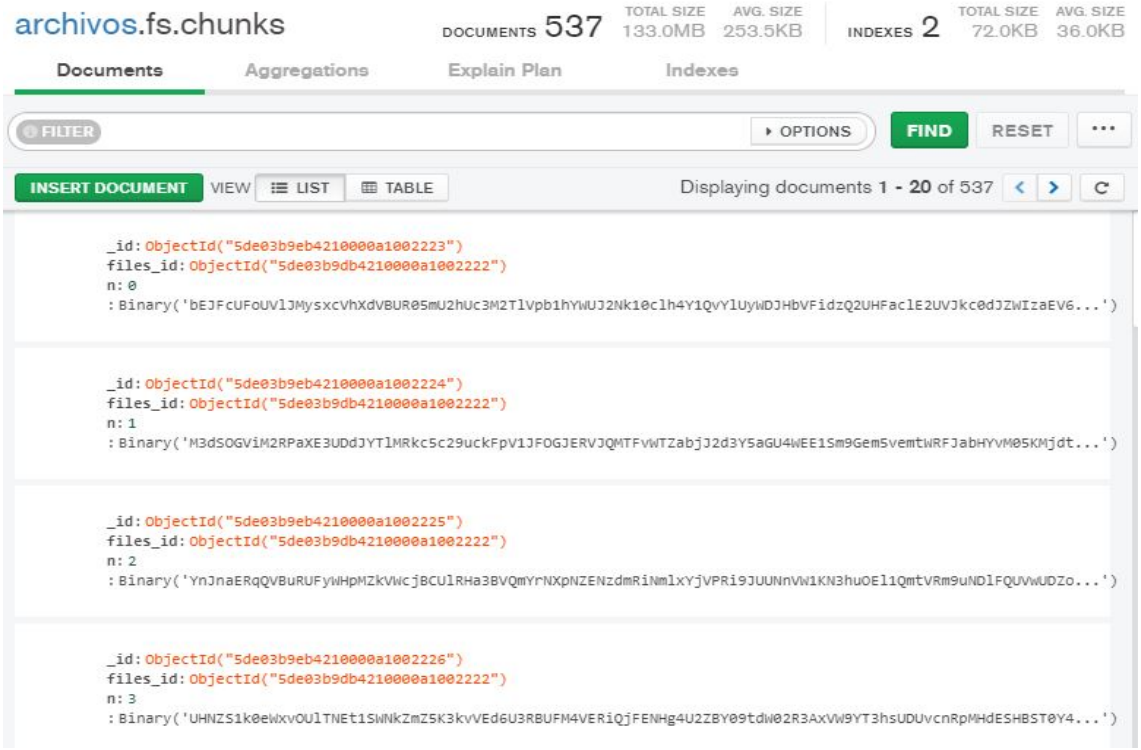


Figura G.38.: Información almacenada en fs.chunks - interfaz gráfica.

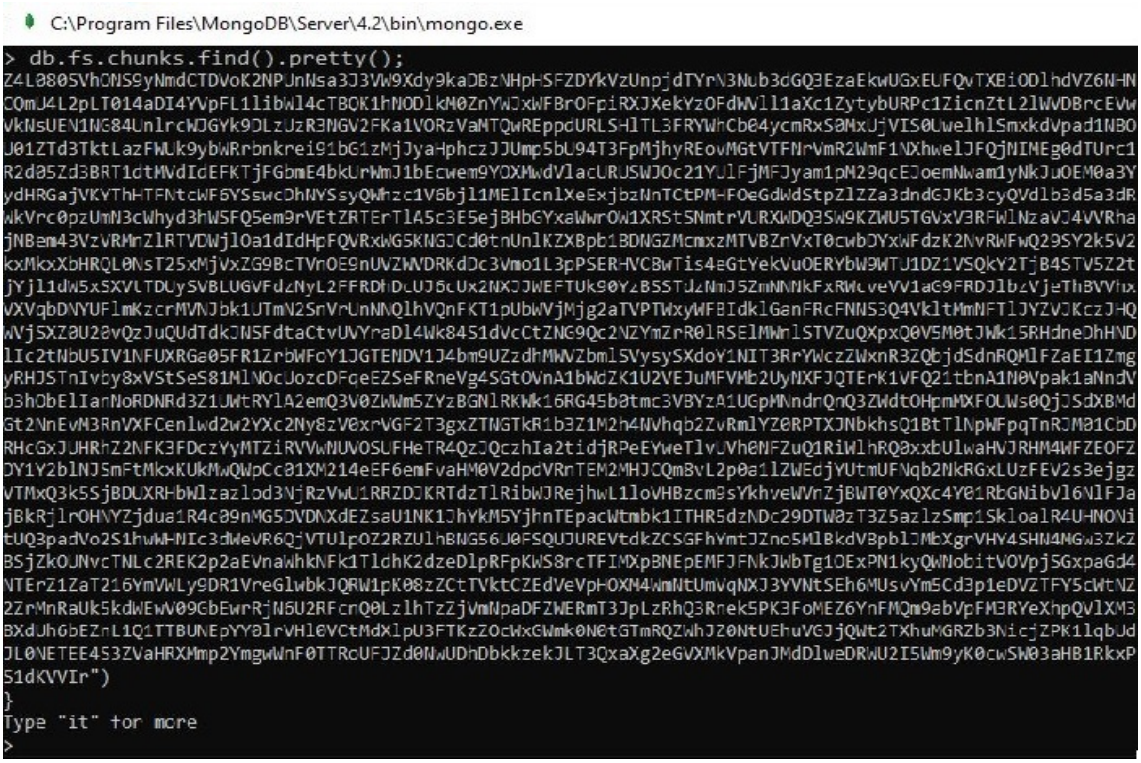


Figura G.39.: Información almacenada en fs.chunks - Consola.

G.6. Base de datos MongoDB

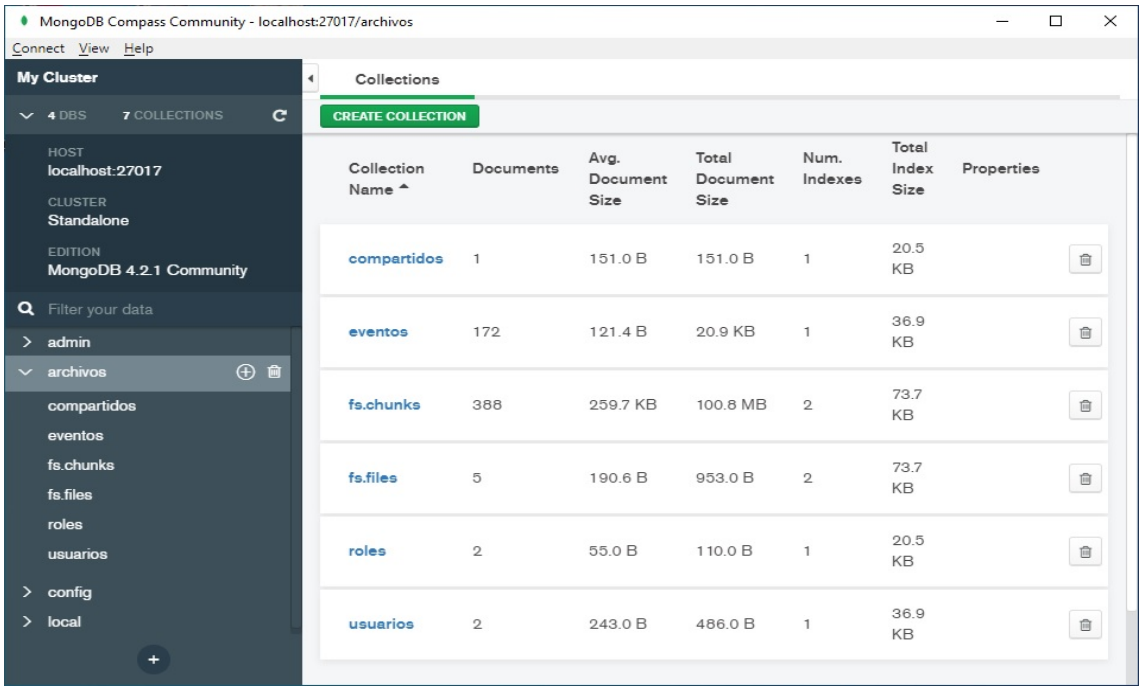


Figura G.40.: Interfaz gráfica de MongoDB.

H. Reporte de escaneo de vulnerabilidades

acunetix

Developer Report

Acunetix website audit

04 December 2019

WEB APPLICATION SECURITY

Generated by Acunetix Reporter

Scan of https://repositorio-itm.info/

Scan details

Scan information	
Start time	04/12/2019, 23:23:29
Start url	https://repositorio-itm.info/
Host	https://repositorio-itm.info/
Scan time	4 minutes, 54 seconds
Profile	Full Scan

Threat level

Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

Alerts distribution

Total alerts found	6
High	0
Medium	0
Low	3
Informational	3

Alerts summary

Login page password-guessing attack

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: Low
CWE	CWE-307

Affected items	Variation
/Login.php	1

Possible sensitive directories

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/nbproject	1

/nbproject/private	1

Broken links

Classification	
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
/nbproject	1
/nbproject/private	1

Possible username or password disclosure

Classification	
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CVSS3	Base Score: 7.5 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: High Integrity Impact: None Availability Impact: None
CWE	CWE-200

Affected items	Variation
/plugins/font-awesome/css/font-awesome.min.css	1

Alerts details

Login page password-guessing attack

Severity	**Low**
Reported by module	Scripting (Html_Authentication_Audit.script)

Description

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

References

Blocking Brute Force Attacks (http://www.owasp.org/index.php/Blocking_Brute_Force_Attacks)

Affected items

/Login.php
Details
The scanner tested 10 invalid credentials and no account lockout was detected.
Request headers

```
POST /Login.php HTTP/1.1
Content-Length: 149
Content-Type: application/x-www-form-urlencoded
Referer: https://repositorio-itm.info/
Host: repositorio-itm.info
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
itoke=b0c036750fb4ccab760946639c3723fc2dbb277b2749bd3ccc5e31f6a54aafa9&signupInputEmail1=p0P
SCOU8%40repositorio-itm.info&signupInputPassword=3mrAkX55
```

Possible sensitive directories

Severity	**Low**
Reported by module	Scripting (Possible_Sensitive_Directories.script)

Description

A possible sensitive directory has been found. This directory is not directly linked from the website.This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Impact

This directory may expose sensitive information that could help a malicious user to prepare more advanced attacks.

Recommendation

Restrict access to this directory or remove it from the website.

References

Web Server Security and Database Server Security (http://www.acunetix.com/websitesecurity/webserver-security/)

Affected items

/nbproject
Details
Request headers

```
GET /nbproject HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Cookie: PHPSESSID=14dq9hdn77sldt5llgt6pnbl30
Host: repositorio-itm.info
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

/nbproject/private
Details
Request headers

```
GET /nbproject/private HTTP/1.1
Accept: acunetix/wvs
Range: bytes=0-99999
Cookie: PHPSESSID=14dq9hdn77sldt5llgt6pnbl30
Host: repositorio-itm.info
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
```

Broken links

Severity	**Informational**
Reported by module	Crawler

Description

A broken link refers to any link that should take you to a document, image or webpage, that actually results in an error. This page was linked from the website but it is inaccessible.

Impact

Problems navigating the site.

Recommendation

Remove the links to this file or make it accessible.

Affected items

/nbproject

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /nbproject/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://repositorio-itm.info/nbproject/
Cookie: PHPSESSID=14dq9hdn77sldt5llgt6pnbl30
Host: repositorio-itm.info
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

/nbproject/private

Details

For a complete list of URLs linking to this file, go to Site Structure > Locate and select the file (marked as "Not Found") > select Referrers Tab from the bottom of the Information pane.

Request headers

```
GET /nbproject/private/ HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://repositorio-itm.info/nbproject/private/
Cookie: PHPSESSID=14dq9hdn77sldt5llgt6pnbl30
Host: repositorio-itm.info
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Possible username or password disclosure

Severity	**Informational**
Reported by module	Scripting (Text_Search_File.script)

Description

A username and/or password was found in this file. This information could be sensitive.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

Recommendation

Remove this file from your website or change its permissions to remove access.

Affected items

/plugins/font-awesome/css/font-awesome.min.css

Details

Pattern found:

```
pass:before
```

Request headers

```
GET /plugins/font-awesome/css/font-awesome.min.css HTTP/1.1
Pragma: no-cache
Cache-Control: no-cache
Referer: https://repositorio-itm.info/
Cookie: PHPSESSID=sq5esaeovrctsi0g6l1h26b8r4
Host: repositorio-itm.info
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko)
Chrome/41.0.2228.0 Safari/537.21
Accept: */*
```

Scanned items (coverage report)

https://repositorio-itm.info/
https://repositorio-itm.info/css
https://repositorio-itm.info/css/bootstrap.min.css
https://repositorio-itm.info/css/demo
https://repositorio-itm.info/css/demo/jasmine.css
https://repositorio-itm.info/css/fonts
https://repositorio-itm.info/css/style.css
https://repositorio-itm.info/css/sweetalert.css
https://repositorio-itm.info/data
https://repositorio-itm.info/fonts
https://repositorio-itm.info/fonts/glyphicons-halflings-regular.woff2
https://repositorio-itm.info/img
https://repositorio-itm.info/img/thumbs
https://repositorio-itm.info/index.php
https://repositorio-itm.info/js
https://repositorio-itm.info/js/bootstrap.min.js
https://repositorio-itm.info/js/demo
https://repositorio-itm.info/js/encrypt.js
https://repositorio-itm.info/js/jquery-2.1.1.min.js
https://repositorio-itm.info/js/scripts.js
https://repositorio-itm.info/js/sweetalert.min.js
https://repositorio-itm.info/js/sweetalert2.js
https://repositorio-itm.info/js/sweetalert2.min.js
https://repositorio-itm.info/login.php
https://repositorio-itm.info/Login.php
https://repositorio-itm.info/nbproject
https://repositorio-itm.info/nbproject/private
https://repositorio-itm.info/plugins
https://repositorio-itm.info/plugins/bootstrap-select
https://repositorio-itm.info/plugins/bootstrap-select/bootstrap-select.min.css
https://repositorio-itm.info/plugins/bootstrap-select/bootstrap-select.min.js
https://repositorio-itm.info/plugins/fast-click
https://repositorio-itm.info/plugins/fast-click/fastclick.min.js
https://repositorio-itm.info/plugins/font-awesome
https://repositorio-itm.info/plugins/font-awesome/css
https://repositorio-itm.info/plugins/font-awesome/css/font-awesome.min.css
https://repositorio-itm.info/plugins/font-awesome/fonts
https://repositorio-itm.info/plugins/font-awesome/fonts/fontawesome-webfonte0a5.woff2
https://repositorio-itm.info/plugins/pace
https://repositorio-itm.info/plugins/pace/pace.min.css
https://repositorio-itm.info/plugins/pace/pace.min.js
https://repositorio-itm.info/plugins/switchery
https://repositorio-itm.info/plugins/switchery/switchery.min.css
https://repositorio-itm.info/plugins/switchery/switchery.min.js
https://repositorio-itm.info/vendor
https://repositorio-itm.info/ws