Escuela Politécnica Nacional
Facultad de Ingeniería de Sistemas

1. Introducción

El presente documento describe el proceso y los resultados de las **Pruebas de Aceptación** realizadas al sistema **AntCiberDron**, desarrollado en el marco de la asignatura **Metodologías Ágiles**, aplicando la metodología **Extreme Programming (XP)**.

Las Pruebas de Aceptación constituyen una fase fundamental dentro de XP, ya que permiten validar que el sistema implementado cumple con los **requerimientos funcionales** y los **criterios de aceptación definidos en las Historias de Usuario**, desde la perspectiva del usuario final y del cliente (docente). Estas pruebas aseguran que las funcionalidades desarrolladas aportan el valor esperado y se comportan de acuerdo con lo especificado.

En este proyecto, AntCiberDron integra múltiples componentes, entre ellos: autenticación de usuarios, lectura y procesamiento del archivo `Grupo03.csv`, ejecución de misiones, visualización de progreso mediante indicadores de carga, evaluación de tipos de arsenal a través de un **Autómata Finito Determinista (AFD)**, activación de la bomba BBA y gestión del hormiguero virtual con sus respectivas reglas de transformación y alimentación. El sistema se ejecuta en un entorno contenerizado mediante **Docker**, utilizando **Nginx** para la exposición del dashboard XP, lo que garantiza un entorno de despliegue controlado y reproducible.

Las Pruebas de Aceptación se enfocan en verificar el funcionamiento integral del sistema a través de escenarios reales de uso, validando la interacción entre la interfaz gráfica, la lógica de negocio y los datos de entrada. Asimismo, se documentan los resultados obtenidos y las evidencias correspondientes, con el fin de determinar si el sistema se encuentra en condiciones de ser aceptado conforme a los objetivos planteados en el proyecto.

2. Objetivo

2.1. Objetivo General

Validar, mediante Pruebas de Aceptación, que el sistema AntCiberDron cumple correctamente con los requerimientos funcionales y los criterios de aceptación definidos en las Historias de Usuario, asegurando su correcto funcionamiento en un entorno de despliegue basado en Docker y Nginx, conforme a la metodología Extreme Programming (XP).

2.2. Objetivos Específicos

- Verificar el correcto acceso al sistema mediante la autenticación de usuarios autorizados (docente y estudiantes).
- Comprobar la correcta lectura y procesamiento del archivo Grupo03.csv, validando la visualización de datos de misión y coordenadas.
- Validar la ejecución de la misión AntDron2K25, incluyendo la visualización del progreso y los estados de procesamiento.
- Confirmar el funcionamiento del Autómata Finito Determinista (AFD) para la evaluación del tipo de arsenal, verificando los resultados True / False según el lenguaje definido.
- Comprobar la activación de la bomba BBA y la correcta notificación de explosión cuando el autómata determina una cadena válida.
- Validar la gestión del hormiguero virtual, incluyendo el estado inicial de las hormigas, su transformación y las reglas de alimentación establecidas.
- Asegurar que el sistema responde de manera consistente y estable durante la ejecución completa de las pruebas de aceptación.

3. Alcance

Las Pruebas de Aceptación descritas en este documento abarcan la validación funcional del sistema AntCiberDron, considerando su ejecución en un entorno contenerizado y el uso de una interfaz gráfica para la interacción con el usuario. El alcance de las pruebas se centra en verificar que el sistema cumple con los requerimientos establecidos y que las funcionalidades principales operan de manera correcta desde la perspectiva del usuario final

4. Entorno de Pruebas

Las Pruebas de Aceptación del sistema **AntCiberDron** se realizaron en un entorno controlado y reproducible, utilizando contenedores Docker y un servidor web Nginx para la exposición del dashboard del proyecto. Este entorno garantiza consistencia durante la ejecución de las pruebas y permite validar el comportamiento del sistema bajo condiciones similares a un entorno de despliegue real.

4.1. Arquitectura del entorno

El sistema está compuesto por los siguientes elementos:

- **Aplicación AntCiberDron** desarrollada en Java, que integra la lógica de negocio, el autómata BBA, la gestión del hormiguero y la interfaz gráfica del sistema.
- **Dashboard XP**, desplegado en un contenedor Docker y servido mediante **Nginx**, encargado de mostrar la estructura del proyecto y la planificación bajo la metodología XP.
- **Servidor Nginx**, configurado como servidor web para exponer el dashboard a través del navegador.
- **Archivo de configuración docker-compose.yml**, utilizado para orquestar los servicios del sistema.

4.2. Configuración de Docker y Nginx

El entorno de pruebas se ejecuta mediante **Docker Compose**, el cual define un servicio principal denominado xp-dashboard, configurado de la siguiente manera:

- **Imagen construida desde un Dockerfile** ubicado en el proyecto.
- **Puerto expuesto:** 3000, mapeado al puerto 80 del contenedor.
- **Nombre del contenedor:** xp-dashboard.
- **Variable de entorno:** NODE_ENV=production.
- **Volumen montado:** la carpeta XP del proyecto, permitiendo el acceso directo a los artefactos XP desde el contenedor.

La ejecución del entorno se realiza mediante el siguiente comando:

docker-compose up -d

Una vez iniciado el contenedor, el dashboard XP se encuentra disponible en la siguiente URL:

http://localhost:3000

4.3. Herramientas y tecnologías utilizadas

- **Lenguaje de programación:** Java
- **Interfaz gráfica:** Java GUI
- **Contenerización:** Docker y Docker Compose
- **Servidor web:** Nginx
- **Gestor de dependencias frontend:** Node.js (para el dashboard)
- **Sistema operativo anfitrión:** Windows

4.4. Datos y archivos utilizados en pruebas

- **Archivo de entrada:** Grupo03.csv, ubicado dentro del proyecto y utilizado para la ejecución de la misión.
- **Usuarios de prueba:** docente e integrantes del Grupo 03, previamente registrados en el sistema.

5. Roles y responsables de aceptación

En el desarrollo del proyecto **AntCiberDron**, los roles y responsabilidades fueron asignados conforme a las distintas **fases de la metodología Extreme Programming (XP)**, garantizando una adecuada distribución del trabajo y la correcta validación de los entregables en cada etapa del proyecto.

5.1. Roles por fase del proyecto

Fase de Planificación

- **Responsables:**
    - Ricardo Villareal
    - Cristian Robles
    - Anthony Chiluiza
    - Julio Arrobo

En esta fase se definieron los requerimientos, historias de usuario, alcance del proyecto y planificación general bajo la metodología XP.

Fase de Diseño

- **Responsables:**
    - Anthony Chiluiza
    - Ricardo Villareal

Durante esta fase se elaboraron los diagramas y el diseño del sistema, incluyendo la arquitectura, los diagramas UML y la estructura general de la aplicación.

Fase de Desarrollo

- **Responsables:**
    - Julio Arrobo
    - Cristian Robles

En esta etapa se implementaron las funcionalidades del sistema AntCiberDron, incluyendo la lógica de negocio, la interfaz gráfica, el autómata BBA, la gestión del hormiguero y la integración del archivo CSV.

Fase de Pruebas de Aceptación

- **Responsables:**
    - Ricardo Villareal
    - Julio Arrobo

Los responsables de esta fase ejecutaron las **Pruebas de Aceptación**, validando el cumplimiento de los requerimientos y criterios definidos en las historias de usuario, documentando los resultados y recopilando las evidencias correspondientes.

6. Datos de prueba

Los **datos de prueba** utilizados en las Pruebas de Aceptación del sistema **AntCiberDron** fueron definidos con el objetivo de validar el correcto funcionamiento de las funcionalidades principales del sistema en escenarios reales de uso. Estos datos permiten comprobar el comportamiento del sistema ante diferentes entradas y condiciones, garantizando la confiabilidad de los resultados obtenidos.

6.1. Usuarios de prueba

Para la ejecución de las pruebas de aceptación se utilizaron los siguientes usuarios registrados en el sistema:

- **Docente**
    - Usuario: patmic
    - Contraseña: 123
- **Estudiante – Grupo 03**
    - Usuario: 2200223473
    - Contraseña: 123

Estos usuarios fueron empleados para validar el acceso al sistema, la visualización de información del equipo y la ejecución de las funcionalidades disponibles según el perfil.

6.2. Archivo de entrada CSV

Se utilizó como dato de prueba principal el archivo:

- **Nombre del archivo:** Grupo03.csv
- **Ubicación:** dentro del proyecto AntCiberDron
- **Contenido:**
    - Geoposición
    - Horarios (Lunes a Viernes)
    - Tipo de arsenal

Este archivo es procesado por el sistema durante la ejecución de la misión, permitiendo validar la lectura correcta de los datos y su uso en la lógica de negocio.

6.3. Datos de prueba para el Autómata BBA

Para la validación del **Autómata Finito Determinista (AFD)** se utilizaron cadenas de prueba correspondientes al lenguaje definido por el grupo, considerando casos válidos e inválidos.

- **Alfabeto:** { a, b, c, d, t }
- **Cadenas válidas (ejemplo):**
    - a
    - ab
    - abcdt
    - abcdtttt
- **Cadenas inválidas (ejemplo):**
    - ac
    - ba
    - abcdx

Estas cadenas permitieron verificar la correcta evaluación del tipo de arsenal y la respuesta del sistema mediante resultados **True / False**, así como la activación o no de la bomba BBA.

6.4. Datos de prueba del Hormiguero Virtual

Para la validación del módulo **Hormiguero Virtual** se consideraron los siguientes datos de prueba:

- **Estado inicial:** HLarva
- **Alimento inicial:** Néctar
- **Tipo de hormiga del grupo:** HZángano
- **Estado energético:** 100%
- **Armamento configurado:** Metralleta M4A1 + Láser X-5000
- **Bomba BBA:** instalada y funcional

Estos datos permitieron validar la transformación de la hormiga, el estado del dron y la coherencia de la información presentada en la interfaz.

7. Estrategia y metodología de ejecución (XP)

Las **Pruebas de Aceptación** del sistema **AntCiberDron** se ejecutaron siguiendo los principios de la metodología **Extreme Programming (XP)**, en la cual el cliente y el equipo de desarrollo validan de manera temprana y continua que el sistema cumple con los requerimientos establecidos y aporta el valor esperado.

En XP, las pruebas de aceptación se basan directamente en las **Historias de Usuario**, por lo que cada caso de prueba fue diseñado para verificar el cumplimiento de los **criterios de aceptación** definidos para cada funcionalidad del sistema.

7.1. Enfoque de ejecución

La estrategia de ejecución de las pruebas de aceptación se basó en los siguientes lineamientos:

- Las pruebas se realizaron **al finalizar la fase de desarrollo**, una vez que las funcionalidades estuvieron completamente implementadas.
- Cada prueba fue ejecutada desde la **perspectiva del usuario final**, utilizando la interfaz gráfica del sistema.
- Se validaron escenarios reales de uso, simulando la operación normal del sistema durante la ejecución de una misión.
- Los resultados obtenidos fueron comparados con los resultados esperados definidos en las historias de usuario.

7.2. Relación con las Historias de Usuario

Cada **Caso de Prueba de Aceptación (UAT)** fue trazado directamente a una o más **Historias de Usuario**, garantizando que:

- Todas las funcionalidades críticas fueran validadas.
- No existan pruebas aisladas sin relación con los requerimientos.
- El avance del sistema pueda ser evaluado objetivamente en función de su aceptación.

7.3. Proceso de ejecución de las pruebas

El proceso seguido para la ejecución de las pruebas de aceptación fue el siguiente:

1. Despliegue del entorno de pruebas mediante **Docker Compose**.
2. Acceso al sistema a través del navegador utilizando el dashboard XP servido por **Nginx**.
3. Autenticación del usuario correspondiente (docente o estudiante).
4. Ejecución de las funcionalidades a validar (carga de CSV, ejecución de misión, evaluación de arsenal, hormiguero).
5. Verificación de los resultados obtenidos frente a los resultados esperados.
6. Registro del estado de cada prueba (Aprobada / Rechazada).
7. Recolección de evidencias mediante capturas de pantalla y mensajes de salida del sistema.

7.4. Evidencias y validación

Para cada caso de prueba ejecutado se recopiló evidencia visual, la cual incluye:

- Capturas de la interfaz gráfica del sistema.
- Mensajes de estado generados durante la ejecución de la misión.
- Resultados de evaluación del autómata (True / False).
- Estados del hormiguero y del dron.

Estas evidencias permiten respaldar objetivamente los resultados obtenidos y facilitan la validación final del sistema por parte del docente.

8. Casos de Prueba de Aceptación (UAT)

Las Pruebas de Aceptación se definieron a partir de las **Historias de Usuario** y los **Requerimientos Funcionales**, siguiendo la metodología **Extreme Programming (XP)**. Cada caso de prueba valida una funcionalidad observable por el usuario final y cuenta con criterios claros de aceptación.

8.1. Estructura de un Caso de Prueba UAT

Cada caso de prueba de aceptación se documenta con la siguiente estructura:

- **ID del Caso de Prueba**
- **Historia(s) de Usuario asociada(s)**
- **Requerimiento(s) asociado(s)**
- **Descripción**
- **Precondiciones**
- **Datos de prueba**
- **Pasos de ejecución**
- **Resultado esperado**
- **Resultado obtenido**
- **Evidencia**
- **Estado** (Aprobado / Rechazado)

8.2. Casos de Prueba de Aceptación

8.2.1. UAT-01 – Autenticación de usuario

- **Historia de Usuario:** HU-02 Autenticar Usuario
- **Requerimiento:** RF02 Autenticación de usuarios
- **Descripción:** Validar que el usuario pueda acceder al sistema mediante credenciales válidas.
- **Precondiciones:** Sistema desplegado y en ejecución.
- **Datos de prueba:**
  - Usuario: 2200223473
  - Contraseña: 123
- **Pasos:**
  - Ejecutar el sistema AntCiberDron.
  - Ingresar las credenciales del usuario.
  - Confirmar el acceso.
- **Resultado esperado:** El sistema permite el acceso y muestra la interfaz principal con los datos del equipo.
- **Resultado obtenido:** El sistema permitió el acceso y mostró la interfaz principal con los datos del equipo.
- **Evidencia:** Ver Anexo – Figura 1
- **Estado:** APROBADO

8.2.2. UAT-02 – Visualización de datos del equipo

- **Historia de Usuario:** HU-03 Mostrar Datos de Equipo
- **Requerimiento:** RF03 Visualización del equipo

- **Descripción:** Verificar que se muestre correctamente la información del grupo y sus integrantes.
- **Precondiciones:** Usuario autenticado.
- **Datos de prueba:** Usuario Grupo 03.
- **Pasos:**
    - Acceder al sistema.
    - Visualizar el encabezado de la aplicación.
- **Resultado esperado:**
  Se muestran el nombre del proyecto, grupo, integrantes y docente responsable.
- **Resultado obtenido:** UAT-02 – Visualización correcta de los datos del equipo del Grupo 03 en el sistema AntCiberDron
- **Evidencia:** Ver Anexo – Figura 2
- **Estado:** APROBADO

8.2.3. UAT-03 – Carga y lectura del archivo CSV

- **Historia de Usuario:** HU-01 Leer archivo CSV
- **Requerimiento:** RF01 Lectura de archivo Grupo##.csv
- **Descripción:** Validar la correcta lectura del archivo Grupo03.csv.
- **Precondiciones:** Archivo CSV disponible en el proyecto.
- **Datos de prueba:** Grupo03.csv.
- **Pasos:**
    - Iniciar el sistema.
    - Ejecutar la misión.
- **Resultado esperado:**
  El sistema carga el archivo y muestra las coordenadas, horarios y tipo de arsenal.
- **Resultado obtenido:** El sistema carga correctamente el archivo *Grupo03.csv* y muestra de forma adecuada las coordenadas, los horarios, el tipo de arsenal y el estado de cada registro durante la ejecución de la misión.
- **Evidencia:** Ver Anexo – Figura 3
- **Estado:** APROBADO

8.2.4. UAT-04 – Ejecución de misión y visualización de progreso

- **Historia de Usuario:** HU-04 Mostrar loading
- **Requerimiento:** RF04 Procesamiento de misión
- **Descripción:** Verificar la ejecución secuencial de la misión con indicador de progreso.
- **Precondiciones:** CSV cargado correctamente.
- **Pasos:**
    - Presionar el botón Ejecutar Misión.
- **Resultado esperado:**
  Se muestra el progreso de procesamiento y mensajes de estado por coordenada.
- **Resultado obtenido:** El sistema ejecuta la misión de forma secuencial, mostrando el avance del procesamiento mediante el indicador de progreso y los mensajes de estado correspondientes a cada coordenada.
- **Evidencia:** Ver Anexo – Figura 4
- **Estado:** APROBADO

8.2.5. UAT-05 – Evaluación de arsenal mediante Autómata BBA (cadena válida)

- **Historia de Usuario:** HU-05 / HU-06 Evaluar Arsenal
- **Requerimiento:** RF05 Autómata BBA
- **Descripción:** Validar que el autómata acepte una cadena válida.
- **Datos de prueba:** a, ab, abcdtttt

- **Pasos:**
  - Ingresar una cadena válida en el módulo Autómata BBA.
  - Ejecutar la evaluación.
- **Resultado esperado:**
  El sistema devuelve **True** y activa la bomba BBA.
- **Resultado obtenido:** El autómata BBA evalúa correctamente la cadena ingresada como válida y el sistema devuelve el resultado **EXPLOTAR**, activando la bomba BBA conforme a lo esperado.
- **Evidencia:** Ver Anexo – Figura 5
- **Estado:** APROBADO

8.2.6. UAT-06 – Evaluación de arsenal mediante Autómata BBA (cadena inválida)

- **Historia de Usuario:** HU-05 / HU-06 Evaluar Arsenal
- **Requerimiento:** RF05 Autómata BBA
- **Datos de prueba:** ac, ba, abcdx
- **Resultado esperado:**
  El sistema devuelve **False** y no se activa la bomba BBA.
- **Resultado obtenido:** El autómata BBA evalúa correctamente la cadena ingresada como inválida y el sistema devuelve el resultado **NO EXPLOTAR**, sin activar la bomba BBA, conforme a lo esperado.
- **Evidencia:** Ver Anexo – Figura 6
- **Estado:** APROBADO

8.2.7. UAT-07 – Visualización de coordenada cuando explota BBA

- **Historia de Usuario:** HU-14 Notificar explosión BBA
- **Requerimiento:** RF05 Autómata + BBA
- **Descripción:** Validar que se muestre la coordenada asociada cuando ocurre una explosión.
- **Precondiciones:** Cadena válida evaluada.
- **Resultado esperado:**
  El sistema muestra la coordenada correspondiente a la explosión.
- **Resultado obtenido:** El sistema, tras evaluar una cadena válida mediante el Autómata BBA, activa la bomba y muestra correctamente la coordenada asociada a la explosión durante la ejecución de la misión.
- **Evidencia:** Ver Anexo – Figura 7
- **Estado:** APROBADO

8.2.8. UAT-08 – Validación del Hormiguero Virtual

- **Historia de Usuario:** HU-07 a HU-11 Gestión de hormigas
- **Requerimiento:** RF04 Evolución de hormigas
- **Descripción:** Validar el estado del hormiguero virtual.
- **Pasos:**
  - Acceder a la pestaña **Hormiguero**.
- **Resultado esperado:**
  Se muestra el estado inicial HLarva, la transformación a HZángano, energía, armamento y estado del dron.
- **Resultado obtenido:** El sistema muestra correctamente el estado del hormiguero virtual, incluyendo el estado inicial de las hormigas, la transformación a HZángano, el nivel de energía, el armamento asignado y el estado operativo del dron.
- **Evidencia:** Ver Anexo – Figura 8
- **Estado:** APROBADO

8.2.9. UAT-09 – Bloqueo del sistema tras intentos fallidos de autenticación

- **Historia de Usuario:** HU-02 Autenticar Usuario
- **Requerimiento:** RF02 Autenticación de usuarios
- **Descripción:** Verificar que el sistema bloquee el acceso cuando se ingresan credenciales incorrectas en tres intentos consecutivos.
- **Precondiciones**
  - Sistema desplegado y en ejecución.
  - Usuario registrado en el sistema.
- **Datos de prueba**
  - Usuario: 2200223473
  - Contraseña incorrecta: xxx
- **Pasos**
  - Ejecutar el sistema AntCiberDron.
  - Ingresar el usuario con una contraseña incorrecta.
  - Repetir el proceso hasta completar tres intentos fallidos.
  - Intentar acceder nuevamente al sistema.
- **Resultado esperado:** El sistema bloquea el acceso del usuario tras el tercer intento fallido y no permite el ingreso a la aplicación.
- **Resultado obtenido:** Tras ingresar credenciales incorrectas en tres intentos consecutivos, el sistema muestra el mensaje "Acceso denegado. Sistema bloqueado" y no permite el inicio de sesión, cumpliendo con el comportamiento esperado.
- **Evidencia:** Ver Anexo – Figura 9
- **Estado:** APROBADO

9. Registro de incidencias

Durante la ejecución de las **Pruebas de Aceptación (UAT)** del sistema **AntCiberDron**, se realizó el seguimiento de posibles incidencias con el objetivo de identificar fallos o desviaciones respecto a los resultados esperados.

Tras la ejecución de los nueve (9) casos de prueba**,** no se detectaron incidencias funcionales ni críticas**.** Todas las pruebas cumplieron con los criterios de aceptación definidos en las historias de usuario y requerimientos del sistema.

10.Resultados

Los resultados obtenidos durante la ejecución de las **Pruebas de Aceptación (UAT)** del sistema **AntCiberDron** demuestran que la aplicación cumple correctamente con los requerimientos funcionales definidos en el proyecto.
Las nueve pruebas de aceptación ejecutadas fueron **aprobadas**, validando aspectos clave como la autenticación de usuarios, la carga y procesamiento de archivos CSV, la ejecución de misiones, la evaluación de arsenal mediante el Autómata BBA, la visualización de coordenadas y el estado del hormiguero y del dron.
En general, el sistema presentó un comportamiento estable con las historias de usuario, confirmando que se encuentra en condiciones adecuadas para su uso conforme a los objetivos planteados.

11.Conclusiones

Las **Pruebas de Aceptación (UAT)** realizadas al sistema **AntCiberDron** permitieron comprobar que las funcionalidades implementadas cumplen con los requerimientos funcionales y los criterios de aceptación definidos en las historias de usuario, conforme a la metodología Extreme Programming (XP)**.**
Los resultados obtenidos evidencian que el sistema responde correctamente en escenarios reales de uso, destacando la autenticación de usuarios, la ejecución de misiones, la validación del arsenal

mediante el autómata BBA y la gestión del hormiguero virtual. Asimismo, no se identificaron incidencias críticas durante la fase de pruebas.
En conclusión, el sistema **AntCiberDron** se considera apto para su aceptación y entrega, al cumplir de manera satisfactoria los objetivos establecidos para el proyecto.

12.Anexos

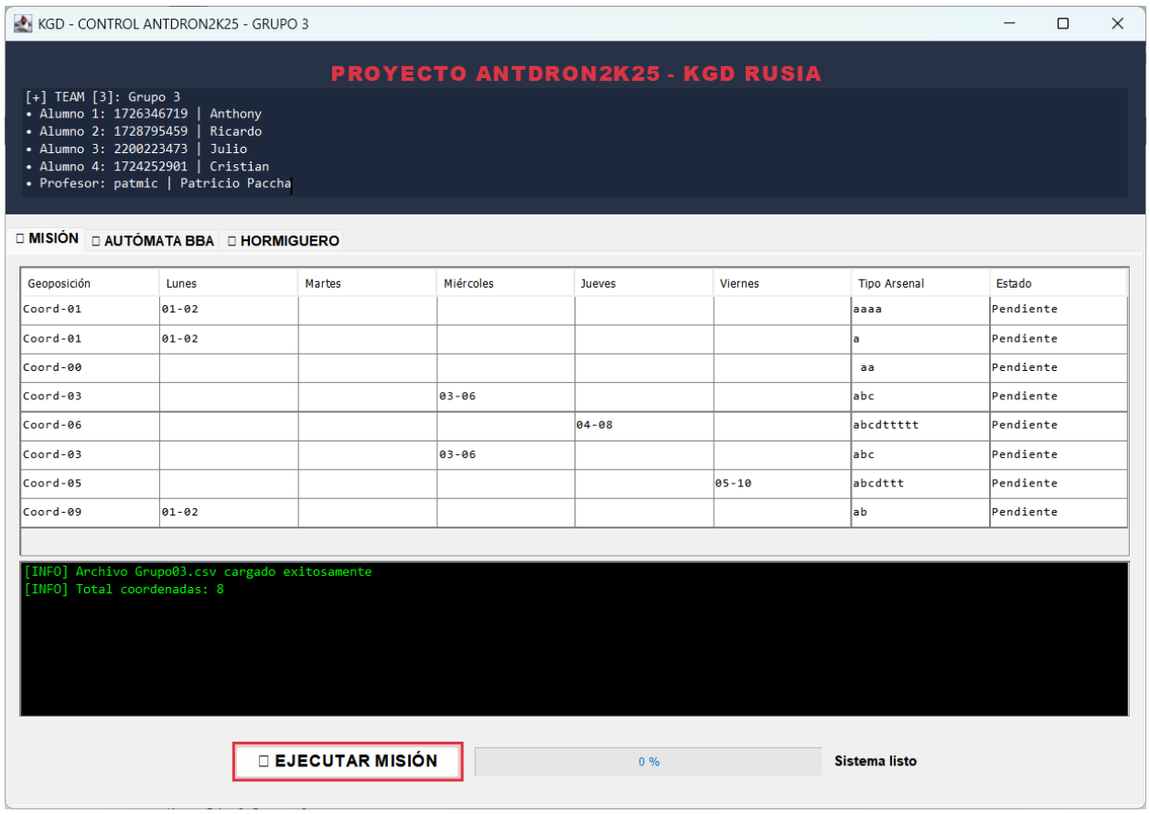

Figura 1. UAT-01 – Acceso exitoso al sistema AntCiberDron y visualización de la interfaz principal del Grupo 03

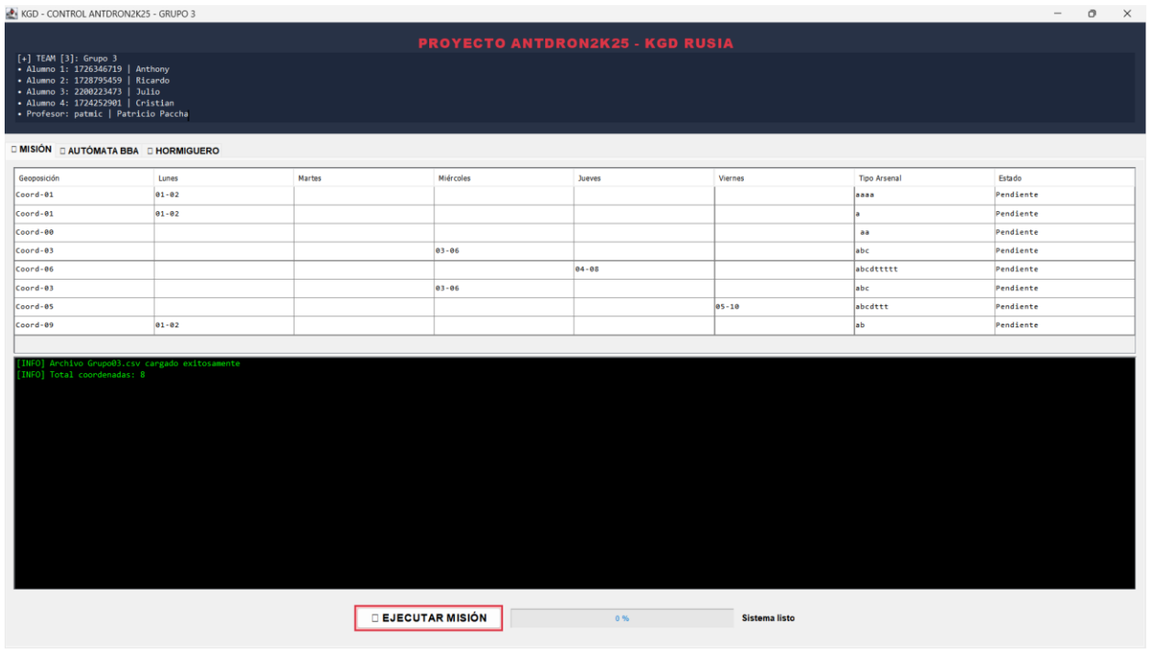

Figura 2. UAT-02 – Visualización correcta de los datos del equipo del Grupo 03 en el sistema AntCiberDron

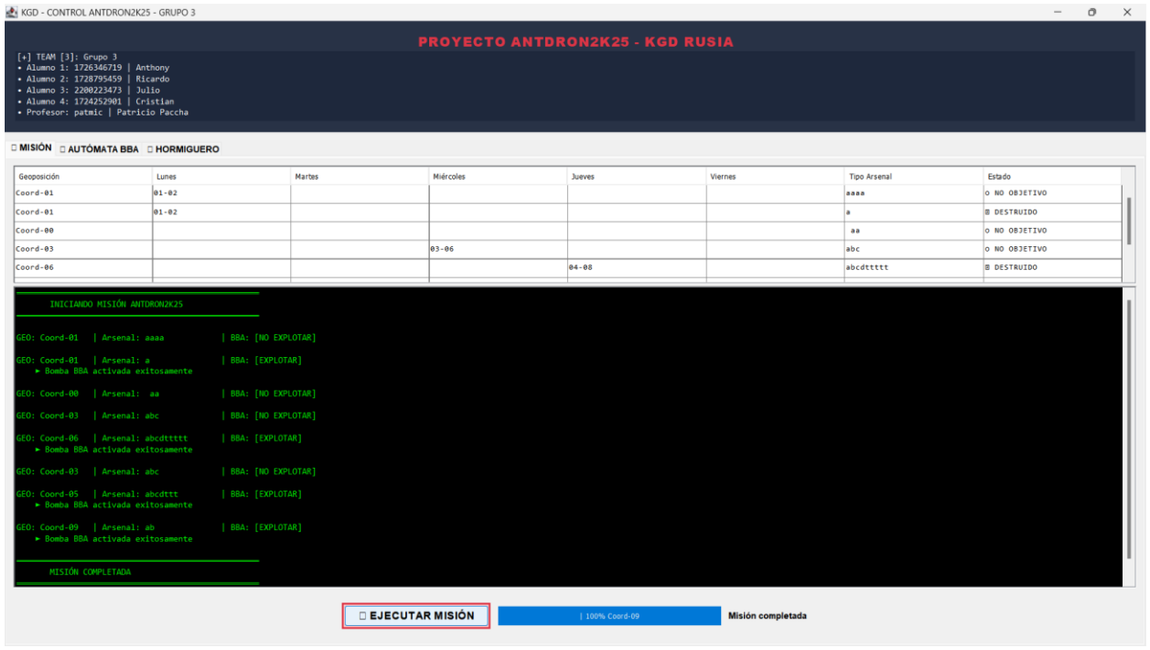

Figura 3. UAT-03 – Carga y lectura del archivo Grupo03.csv y visualización de coordenadas, horarios y tipo de arsenal en el sistema AntCiberDron

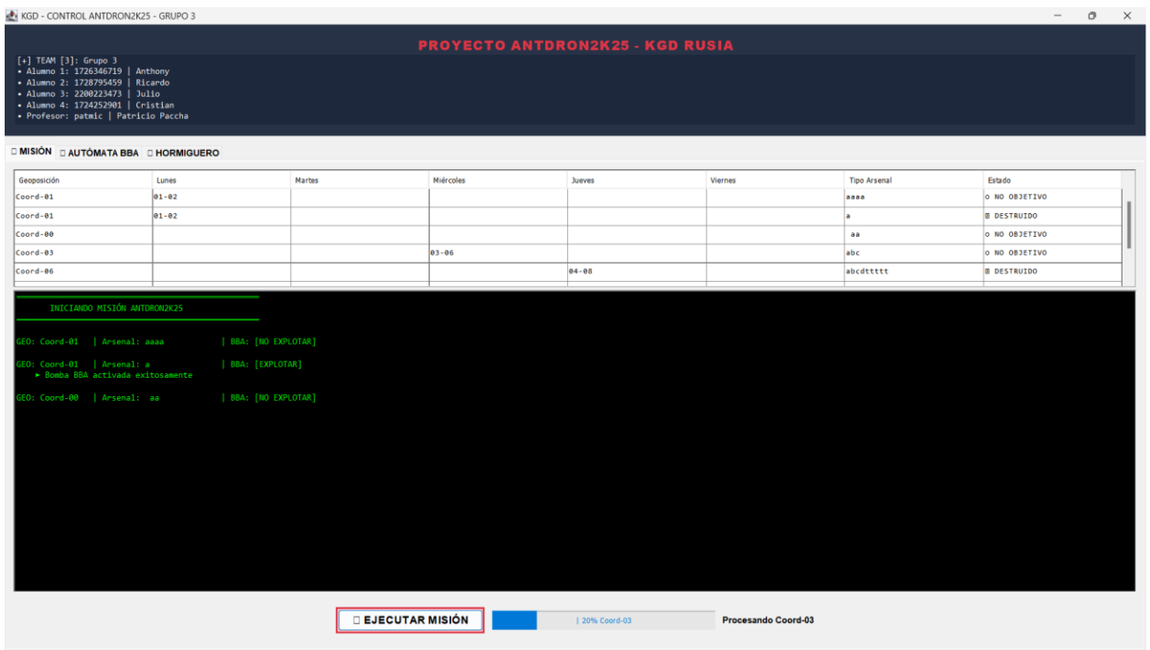

Figura 4. UAT-04 – Ejecución de la misión AntDron2K25 y visualización del progreso de procesamiento por coordenada en el sistema AntCiberDron

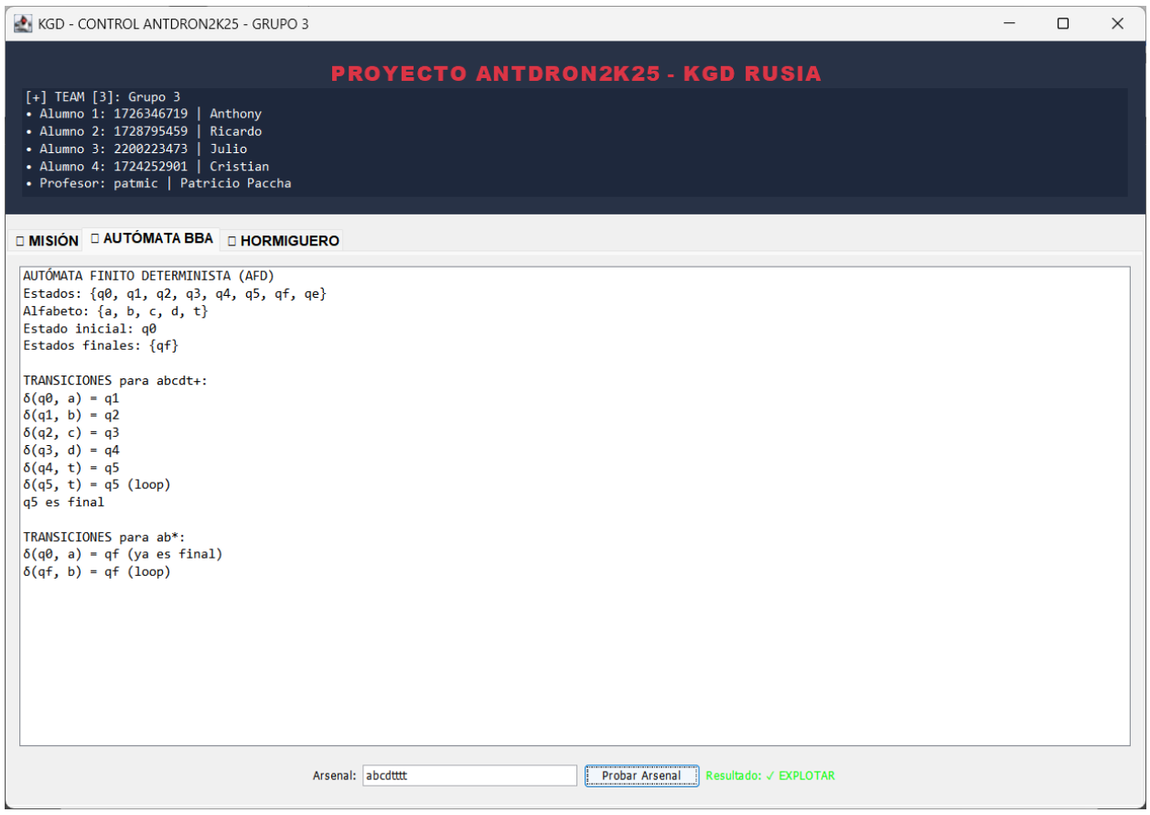

Figura 5. UAT-05 – Evaluación de cadena válida mediante el Autómata BBA con resultado positivo (EXPLOTAR) en el sistema AntCiberDron

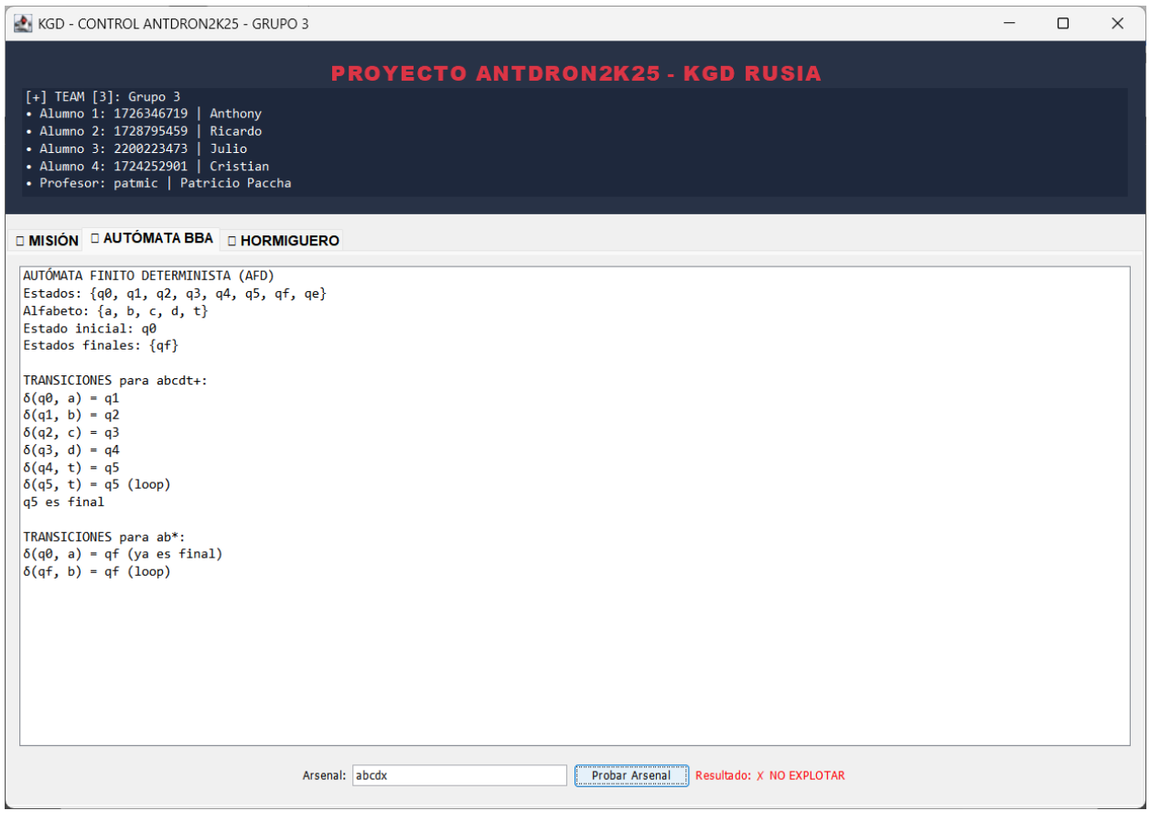

Figura 6. UAT-06 – Evaluación de cadena inválida mediante el Autómata BBA con resultado negativo (NO EXPLOTAR) en el sistema AntCiberDron

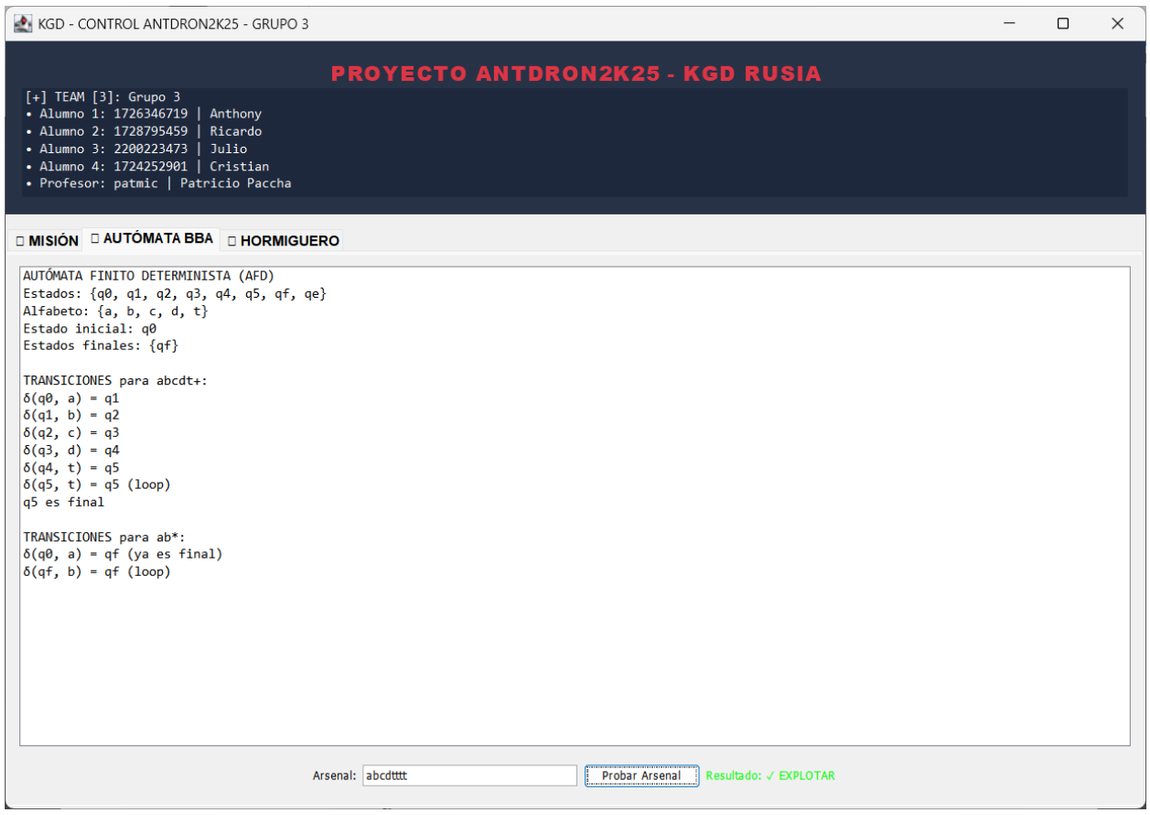

Figura 7. UAT-07 – Visualización de la coordenada asociada a la explosión BBA tras evaluación positiva del Autómata en el sistema AntCiberDron

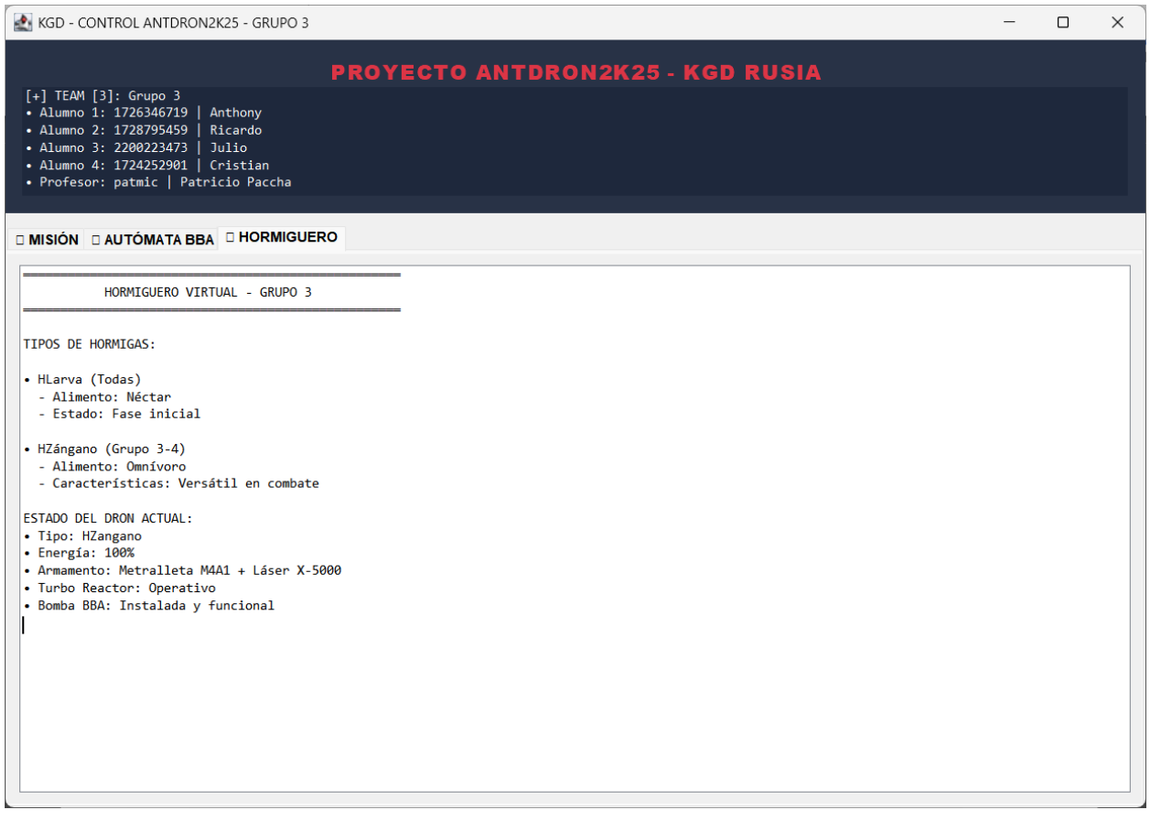

Figura 8. UAT-08 – Visualización del estado del Hormiguero Virtual y del dron del Grupo 03 en el sistema AntCiberDron

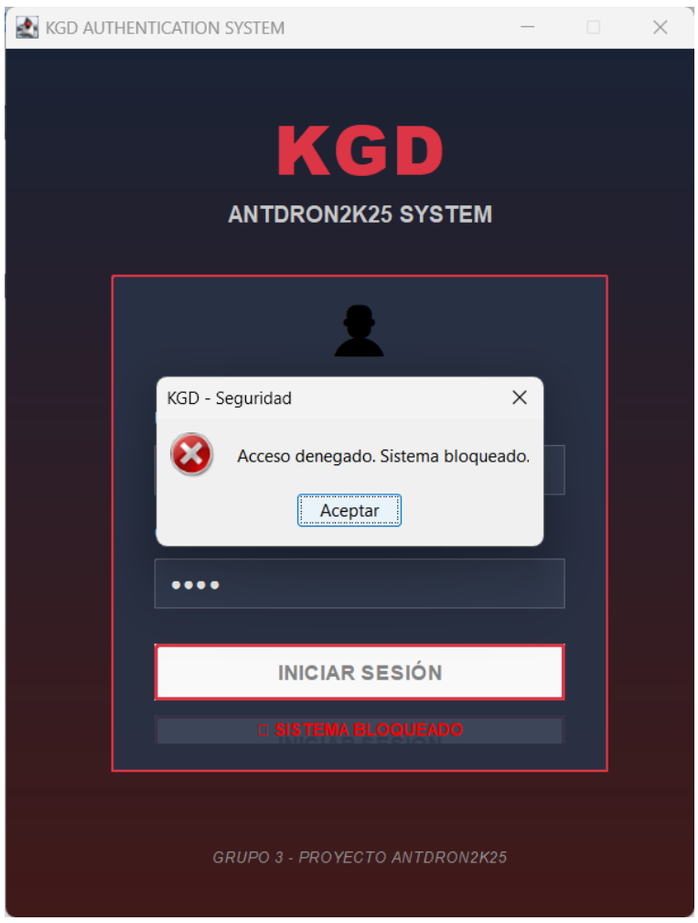

Figura 9. UAT-09 – Bloqueo del sistema tras tres intentos fallidos de autenticación en el sistema AntCiberDron