DOCUMENTACIÓN OFICIAL DEL SISTEMA DE MONITOREO Y PROTECCIÓN PARA UAVs

---

PORTADA

Nombre del proyecto: Diseño del proceso de protección de datos y comunicaciones en UAV usando la normativa PCI DSS, PCI PIN e ISO 27001
Versión del sistema: v1.0.1
Autores: Carventes Garduño Alan Daniel, Leal Sánchez Juan Marcos
Institución: Universidad Politécnica de Texcoco
Programa: Ingeniería en Sistemas Computacionales
Fecha: Abril 2025

ÍNDICE

---

1. INTRODUCCIÓN

El presente documento técnico describe de forma integral el desarrollo e implementación de un sistema de monitoreo y protección para vehículos aéreos no tripulados (UAVs), orientado a mejorar la seguridad de las comunicaciones, los datos y los accesos desde una perspectiva normativa. El sistema fue diseñado con base en los estándares PCI DSS v4.0, PCI PIN y la norma internacional ISO/IEC 27001, buscando simular un entorno funcional de alto nivel para prácticas académicas y profesionales.

La solución fue desarrollada mediante el uso de tecnologías de hardware como ESP32 y software web con lenguajes como PHP, JavaScript y CSS. Se construyó una plataforma visual que permite interpretar de forma accesible el comportamiento del dron en red, así

como evaluar su exposición ante riesgos de seguridad comunes. El resultado final incluye monitoreo en tiempo real, simulación de amenazas, gestión de eventos de seguridad, alertas visuales y controles de acceso, todo centralizado en una interfaz web intuitiva.

Este documento está dirigido a evaluadores, desarrolladores, docentes y autoridades institucionales que deseen conocer en profundidad el sistema, su diseño, justificación técnica y cumplimiento con marcos regulatorios de protección de datos y seguridad en redes aeronáuticas.

---

2. ALCANCE Y OBJETIVOS

2.1 Alcance del Proyecto

Este sistema está diseñado para funcionar en un entorno controlado, simulando la interacción de un dron con una red segura gestionada por un firewall intermedio basado en ESP32. El sistema es capaz de monitorear métricas de red, visualizar el estado de operación del UAV, registrar eventos de seguridad, y simular situaciones como escaneos, desconexiones e intrusiones.

El alcance funcional incluye:

- Conexión segura entre dron y estación de monitoreo.
- Simulación de comportamiento de red en tiempo real.
- Plataforma web con interfaz gráfica y notificaciones.
- Registro automático de eventos de seguridad.
- Control de conexiones y simulación de amenazas.

Limitaciones:

- El sistema no se conecta a redes externas ni realiza operaciones reales sobre drones en campo.
- Las amenazas detectadas son simuladas, no se ejecutan técnicas ofensivas reales.
- No incluye mecanismos avanzados como cifrado TLS, autenticación biométrica o integración con SIEM.

2.2 Objetivo General

Diseñar e implementar un sistema funcional de monitoreo y protección de datos en UAVs, alineado con las normativas PCI DSS, PCI PIN e ISO/IEC 27001, que permita simular un entorno de seguridad en tiempo real con funcionalidades visuales, alertas y controles operativos sobre la red de comunicación del dron.

2.3 Objetivos Específicos

- Construir una arquitectura técnica de bajo costo basada en ESP32 para monitoreo intermedio.
- Desarrollar un sistema web para visualizar métricas del dron y simular amenazas comunes.
- Implementar un registro de eventos y panel de alertas de seguridad.
- Alinear el desarrollo con normativas de ciberseguridad orientadas a protección de datos.
- Facilitar un entorno de pruebas para prácticas académicas en seguridad aplicada a UAVs.

3. ARQUITECTURA DEL SISTEMA

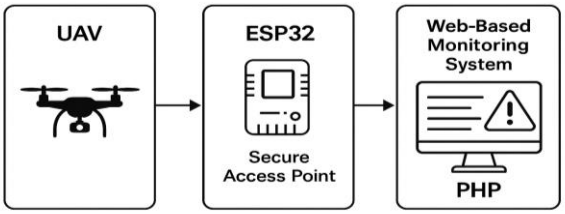
La arquitectura del sistema fue diseñada bajo un enfoque modular que combina la interacción entre hardware embebido, servicios web y componentes visuales del lado del cliente. El sistema simula una infraestructura de seguridad perimetral controlada localmente desde un ESP32, permitiendo actuar como intermediario entre el UAV y el usuario final.

3.1 Arquitectura Lógica

- **Capa de Presentación:** Interfaz web desarrollada en HTML5, CSS y JavaScript para representar gráficamente métricas, alertas, eventos y simulaciones.
- **Capa de Aplicación:** Scripts en PHP y JS que gestionan las operaciones del sistema como la autenticación, registro de eventos, visualización dinámica de datos y lógica de control de estado.
- **Capa de Hardware/Red:** El ESP32 opera como punto de acceso y como firewall simulado, conectándose al dron vía WiFi y exponiendo un entorno seguro al usuario.

3.2 Diagrama de Flujo del Proceso de Monitoreo

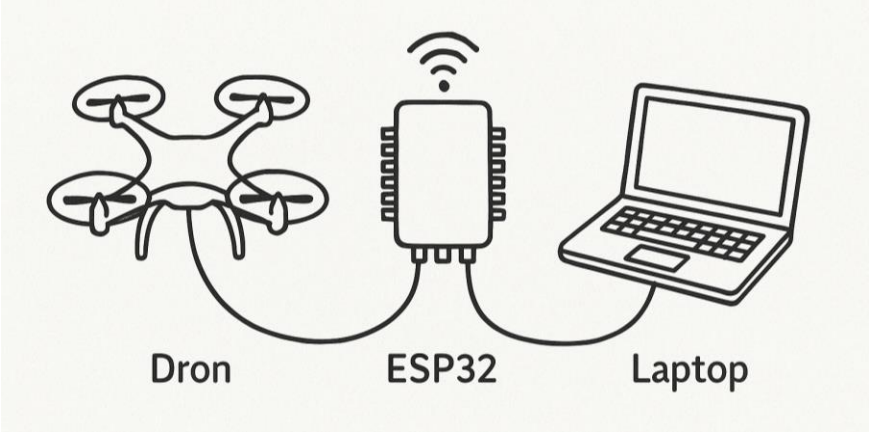
1. El ESP32 se conecta al dron y crea el AP "Dron_Seguro".
2. El usuario se conecta a ese AP y accede al sistema desde el navegador.
3. La sesión se valida mediante PHP (`login.php`).
4. Se cargan scripts y se inicializa la simulación.
5. Se visualizan eventos, se monitorea el tráfico, y se generan alertas dinámicas.



(Figura 1 – Diagrama lógico del proceso de monitoreo y visualización de eventos de seguridad en el sistema UAV.)

3.3 Diagrama de Conexión Física

- **ESP32:** Actúa como intermediario, conectado al dron por WiFi (modo STA) y al usuario mediante un AP seguro (modo AP).
- **Laptop:** Cliente que consume el servicio desde navegador web, monitoreando la actividad y accediendo al dashboard.
- **Dron:** Emisor de datos hacia el ESP32, sin conexión directa con el usuario final.



(Figura 2 – Esquema físico de conexión: ESP32 entre dron y laptop, simulando una red controlada de defensa en UAVs.)

Esta arquitectura permite replicar entornos de seguridad perimetral aplicados a redes aéreas sin poner en riesgo sistemas reales, facilitando prácticas educativas con soporte normativo y visualización avanzada de comportamiento de red.

4. COMPONENTES TÉCNICOS

Este apartado detalla los elementos clave a nivel de hardware, software y herramientas utilizadas durante el desarrollo del sistema de monitoreo y protección para UAVs. La integración coherente de estos componentes permite lograr un entorno funcional y seguro para la simulación de eventos de ciberseguridad.

4.1 Hardware Utilizado

- **ESP32 NodeMCU:** Microcontrolador con capacidad WiFi dual (AP/STA). Se encarga de establecer la red segura "Dron_Seguro" y de intermediar entre el dron y la laptop.
- **UAV LYZRC L900 Pro:** Dron simulado con doble cámara 8K y conectividad WiFi 5GHz. Utilizado como fuente emisora de tráfico hacia el sistema.
- **Laptop/PC de Monitoreo:** Terminal desde la cual se visualiza, analiza y controla el estado del sistema mediante un navegador web.
- **Sensores y cables auxiliares:** Fuente de alimentación, conectores USB, baterías, y sensores simulados integrados en el entorno.

4.2 Software Desarrollado

- **PHP (backend):** Maneja la lógica de autenticación, conexión con la base de datos, registro de logs y visualización de eventos. Archivos clave:
  - `login.php`: Control de acceso al sistema.
  - `guardar_log.php`, `registrar_evento.php`: Registro automático de sucesos.
  - `dashboard.php`: Panel principal del sistema con carga de módulos.
- **JavaScript (frontend dinámico):** Controla eventos visuales, animaciones, simulación de tráfico, actualización de métricas y renderizado de gráficas.
  - `script.js`: Motor de simulación y generación de eventos.
  - `tabs_dinamicos.js`, `visualizacion_uav.js`, `monitoreo_uav.js`: Controlan visualización de pestañas, mapa de amenazas y gráfica de actividad.
- **CSS (diseño visual):**
  - `style.css`: Define el diseño oscuro del sistema, estilos de tarjetas, botones, animaciones, alertas visuales y efectos responsivos.
- **HTML (estructura base):**
  - `index.html`: Página de inicio institucional que presenta el sistema SecureDrone Firewall, con navegación, presentación, testimonios y contacto.
  - `menu.php`: Integración de navegación interna en el dashboard.

4.3 Herramientas y Librerías Adicionales

- **Servidor Apache (AppServ):** Entorno de ejecución local para los scripts PHP y la base de datos MySQL.
- **Base de datos MySQL:** Utilizada para almacenar credenciales de UAV, eventos registrados y sesiones activas.
- **Librería Chart.js:** Visualización gráfica de tráfico de red y uptime del sistema.
- **Editor Visual Studio Code:** IDE utilizado para desarrollar el sistema completo.
- **Arduino IDE:** Compilación y carga del firmware para el ESP32.

Este conjunto de componentes permitió construir un sistema modular, portátil y replicable, facilitando tanto la comprensión académica como la experimentación práctica en ciberseguridad aplicada a dispositivos UAV.

5. DESCRIPCIÓN DE FUNCIONALIDADES

El sistema implementado integra una serie de funcionalidades diseñadas para ofrecer una experiencia de monitoreo, control y simulación de seguridad sobre comunicaciones en UAVs. Estas funcionalidades están orientadas tanto a demostrar conceptos de ciberseguridad como a simular incidentes reales en un entorno controlado.

5.1 Panel de Monitoreo en Tiempo Real

- Visualiza continuamente el estado operativo del UAV simulado.
- Muestra métricas dinámicas como señal (RSSI), latencia, velocidad de transmisión y pérdidas de paquetes.
- El módulo `tabs_dinamicos.js` actualiza las métricas automáticamente cada 5 segundos.

5.2 Visualización Animada del Dron

- Representación gráfica del movimiento del UAV respecto a una antena base.
- Simulación de trayectoria, distancia, intensidad de señal y acciones de usuario.
- Interactúa con el archivo `visualizacion_uav.js` para generar animaciones precisas.

5.3 Simulaciones de Amenazas

- Escaneo de red: Simula búsqueda de vulnerabilidades sin efectos colaterales.
- Intrusión: Simula un ataque detectado con alerta visual y sonora.
- Desconexión: Representa una pérdida de señal o ataque de denegación de servicio.
- Controladas desde `script.js` y disparadas mediante botones del dashboard.

5.4 Registro de Eventos y Logs

- Todos los eventos generados (escaneo, intrusión, conexiones sospechosas) se almacenan automáticamente.
- Utiliza los scripts `guardar_log.php` y `registrar_evento.php`.
- Los registros pueden visualizarse en una tabla dentro de `dashboard.php`.

5.5 Gráfica de Tráfico y Actividad

- Integración con `Chart.js` para visualizar actividad de red.
- Distingue entre tráfico legítimo e intentos bloqueados.
- Se actualiza cada 30 segundos con nuevos datos simulados.

5.6 Control de Conexiones Activas

- El usuario puede observar las MACs conectadas al ESP32.
- Se pueden desconectar manualmente desde la interfaz con botones interactivos.
- Permite simular respuestas ante accesos no autorizados.

5.7 Notificaciones y Alertas Visuales

- El sistema emite mensajes flotantes ante eventos importantes: intrusión, desconexión, escaneo, configuración.
- Las notificaciones incluyen íconos, colores por nivel de riesgo y cierre automático.

5.8 Configuración de Seguridad y Emergencia

- Módulo de cambio de nivel de seguridad: bajo, medio, alto.
- Modo emergencia: bloquea todo el tráfico simulado y cambia la interfaz a color rojo.
- Reactiva operación normal tras cierto tiempo o por acción del usuario.

Estas funcionalidades permiten no solo simular un entorno de monitoreo robusto para UAVs, sino también interactuar de manera práctica con conceptos clave de ciberseguridad: control de accesos, visibilidad del tráfico, respuesta a incidentes, y protección de datos en redes inalámbricas.

6. INTERFAZ DE USUARIO

El sistema cuenta con una interfaz gráfica intuitiva, diseñada con enfoque en la experiencia del usuario (UX) y la eficiencia visual, basada en principios de diseño responsivo. Su objetivo es facilitar la navegación, la interpretación de métricas y la gestión de eventos de seguridad.

6.1 Estructura General

La interfaz principal del sistema está dividida en módulos claramente identificables:

- **Encabezado:** Contiene el título del sistema y botones de navegación general.
- **Panel de métricas:** Presenta información clave como señal, velocidad, latencia y pérdida de paquetes.
- **Mapa de amenazas:** Espacio donde se muestran puntos rojos animados que simulan intentos de intrusión.
- **Gráfica de tráfico:** Visualiza de forma comparativa el tráfico legítimo y los intentos bloqueados.
- **Historial de eventos:** Lista de incidentes registrados, con opción de análisis o bloqueo.
- **Controles:** Botones de escaneo, modo emergencia, nivel de seguridad y cerrar sesión.

6.2 Navegación y Accesibilidad

- Menú principal implementado en `menu.php`, con pestañas que permiten acceder a las diferentes secciones del sistema sin recargar la página.
- La navegación es fluida gracias al uso de AJAX y actualización en tiempo real de los módulos.

6.3 Diseño Visual (style.css)

- Paleta de colores oscuros con acentos en verde, rojo y azul, adaptada para reducir la fatiga visual.
- Elementos interactivos (botones, tarjetas, alertas) con efectos de transición, sombreado y animaciones.

- Notificaciones flotantes aparecen en la parte inferior derecha y desaparecen automáticamente.
- Interfaz totalmente responsiva, optimizada para pantallas de laptops y dispositivos móviles.

6.4 Elementos Interactivos

- **Botón de Escaneo:** Simula búsqueda de vulnerabilidades.
- **Botón de Modo Emergencia:** Cambia el fondo y simula bloqueo total del sistema.
- **Selector de Nivel de Seguridad:** Permite al usuario establecer nivel bajo, medio o alto.
- **Botón de Cerrar Sesión:** Regresa al menú inicial y reinicia el entorno.
- **Log interactivo:** Cada evento registrado permite realizar acciones de análisis o bloqueo (🔍 / 🚫).

6.5 Representación Visual del UAV

- Animación que simula el movimiento del dron.
- Cambios de color en línea de conexión y barra de señal según la intensidad.
- Interfaz desarrollada en `visualizacion_uav.js` y reforzada con estilos personalizados desde `style.css`.

La interfaz de usuario constituye una parte esencial del sistema, no solo por su funcionalidad, sino por su capacidad para comunicar visualmente los riesgos, alertar sobre incidentes y brindar al usuario control sobre el entorno de prueb

7. PRUEBAS Y RESULTADOS

El sistema fue sometido a diversas pruebas con el objetivo de validar su funcionalidad, robustez y alineación con los estándares de seguridad definidos. Las pruebas abarcaron desde validaciones técnicas hasta simulaciones operativas, incluyendo evaluaciones previas y posteriores a la implementación.

7.1 Pruebas de Penetración Iniciales

Antes del desarrollo del sistema, se realizaron pruebas de penetración sobre el dron sin protección:

- **Observaciones:**
  - La red WiFi del dron no utilizaba cifrado.
  - No existía autenticación entre el control y el UAV.
  - Era posible interceptar comandos y video en tiempo real.
- **Conclusión:** Estas vulnerabilidades justificaron el diseño de un sistema de protección y monitoreo centralizado.

7.2 Pruebas Funcionales del Sistema

Tras la implementación del sistema, se realizaron pruebas funcionales para validar cada módulo:

- **Conectividad:** El ESP32 establece el punto de acceso y redirecciona correctamente al dashboard.
- **Autenticación:** El login filtra accesos no autorizados y protege rutas internas.
- **Visualización:** Las métricas y simulaciones se muestran correctamente en tiempo real.
- **Eventos:** Los registros se almacenan de forma confiable y son visualizables.
- **Alertas:** El sistema emite notificaciones visuales y sonoras ante eventos críticos.

7.3 Pruebas de Integración

Se validó el flujo completo desde la conexión del usuario al AP, hasta la visualización del UAV, el control de amenazas y la desconexión de dispositivos:

- La interacción entre módulos `visualizacion_uav.js`, `monitoreo_uav.js`, `script.js` y `dashboard.php` se comportó de forma estable.
- La base de datos almacenó correctamente cada sesión, evento y acción tomada por el usuario.

7.4 Simulación de Escenarios Críticos

- **Modo Emergencia:** Al activarse, bloquea funciones críticas y emite alertas visuales.
- **Intrusión Simulada:** Aparece en el mapa, genera logs y aumenta el nivel de amenaza.
- **Ataques Secuenciales:** La gráfica de tráfico representa el aumento progresivo de conexiones sospechosas.

7.5 Resultados Generales

- El sistema operó correctamente durante sesiones extendidas de prueba (>30 min).
- No se detectaron cuelgues, errores de renderizado ni pérdida de datos en los módulos visuales.
- Se logró demostrar que una arquitectura con ESP32 puede actuar como cortafuegos intermedio efectivo, con visualización educativa en tiempo real.

Estas pruebas permiten afirmar que el sistema cumple satisfactoriamente con los objetivos propuestos, demostrando ser una herramienta útil tanto para evaluación académica como para prácticas en ciberseguridad UAV.

8. CUMPLIMIENTO NORMATIVO

El sistema fue diseñado desde sus bases con un enfoque normativo, tomando como referencia tres marcos principales de seguridad: PCI DSS v4.0, PCI PIN y la norma

ISO/IEC 27001. A continuación, se describe cómo el sistema simula y respeta los lineamientos de dichas normativas en su estructura, funciones y controles.

8.1 PCI DSS v4.0 (Payment Card Industry Data Security Standard)

- **Control de Accesos (Requisito 7):** El sistema implementa autenticación por ID y contraseña para acceder a la interfaz de monitoreo.
- **Registro de Actividades (Requisito 10):** Se lleva un log detallado de cada evento relevante: escaneos, desconexiones, intrusiones, accesos.
- **Protección en Comunicaciones (Requisito 4):** Aunque se simula en entorno local, el sistema aplica restricciones de conexión directa y expone una red controlada vía ESP32.
- **Segmentación de Red (Requisito 1.2):** Se simula un entorno donde el ESP32 aísla al UAV de la red del usuario, actuando como perímetro lógico.

8.2 PCI PIN (PIN Transaction Security Requirements)

- **Protección contra acceso físico y lógico:** El ESP32 se utiliza como elemento intermedio que controla el acceso a las comunicaciones.
- **Simulación de PIN Transport Layer:** Aunque no se transmiten PINs reales, se emulan escenarios donde el tráfico sensible se monitorea y puede ser protegido.
- **Alertamiento ante anomalías:** El sistema detecta patrones de tráfico inusuales, múltiples accesos o simulaciones de fuerza bruta e inyecciones (SQLi).

8.3 ISO/IEC 27001:2022 (Sistema de Gestión de Seguridad de la Información)

- **A.9 Control de accesos:** El acceso al sistema está restringido mediante inicio de sesión.
- **A.12 Seguridad de operaciones:** El sistema monitorea constantemente la operación del dron y emite alertas sobre eventos sospechosos.
- **A.13 Seguridad en las comunicaciones:** Toda comunicación entre usuario y sistema pasa por el entorno seguro generado por el ESP32.
- **A.16 Gestión de incidentes:** El registro automático de eventos permite una trazabilidad útil para responder a posibles incidentes de seguridad.

8.4 Conclusión de Cumplimiento

Si bien el sistema es una simulación académica y no tiene interacción con datos financieros reales, sus módulos y funciones se alinean conceptualmente con las exigencias de los marcos normativos seleccionados. Esto permite reforzar la formación práctica en ciberseguridad aplicada a dispositivos IoT/UAV y facilitar el aprendizaje de estándares de cumplimiento industrial.

9. MANUAL DE USUARIO (RESUMEN)

A continuación, se presenta una guía breve para el uso correcto del sistema de monitoreo y protección de UAVs. Este resumen está diseñado para facilitar la comprensión operativa del sistema, especialmente para nuevos usuarios o personal técnico en formación.

9.1 Acceso Inicial

1. Encender el dron y el ESP32.
2. Desde la laptop, conectarse a la red WiFi "Dron_Seguro".
3. Abrir el navegador y acceder a `http://192.168.4.1/index.html` o `monitoreo.php`.
4. Ingresar ID y contraseña del UAV registrados en la base de datos.

9.2 Panel Principal

Una vez dentro, el usuario podrá visualizar:

- Estado del firewall.
- Métricas en tiempo real (señal, latencia, pérdida de paquetes).
- Mapa animado con puntos de amenaza.
- Gráfica de tráfico legítimo vs intentos bloqueados.
- Historial de eventos registrados.

9.3 Funciones Disponibles

- **Simular Escaneo:** Ejecuta búsqueda de vulnerabilidades.
- **Simular Intrusión:** Lanza una alerta de intento de acceso no autorizado.
- **Modo Emergencia:** Simula un bloqueo general del sistema.
- **Cambiar Nivel de Seguridad:** Ajuste visual y de advertencias por riesgo.
- **Desconectar Cliente:** Finaliza la conexión de una dirección MAC sospechosa.

9.4 Notificaciones

- El sistema genera alertas visuales emergentes ante eventos críticos o acciones del usuario.
- Los colores indican gravedad: verde (normal), amarillo (advertencia), rojo (crítico).

9.5 Recomendaciones de Uso

- No apagar el ESP32 durante simulaciones activas.
- Consultar regularmente el historial de eventos.
- Usar una sesión única por UAV para evitar conflictos.
- Verificar la intensidad de señal antes de iniciar una prueba.

Este manual resume los pasos clave para operar el sistema de manera efectiva, reforzando el enfoque práctico de la plataforma como herramienta de aprendizaje en ciberseguridad UAV.

10. CONCLUSIONES

El desarrollo del sistema de monitoreo y protección de UAVs con enfoque en normas PCI DSS, PCI PIN e ISO/IEC 27001 permitió demostrar la viabilidad de aplicar conceptos avanzados de ciberseguridad en entornos educativos y simulados.

Se logró construir un entorno técnico funcional, capaz de representar visualmente el estado de una red UAV, identificar anomalías y registrar eventos de seguridad en tiempo real. Gracias a su diseño modular, el sistema no solo permite observar el comportamiento de la red, sino también simular ataques e incidentes para evaluar respuestas y reforzar el aprendizaje.

La integración de hardware accesible (ESP32) con software web personalizado demostró que es posible construir plataformas de simulación de bajo costo pero alto valor académico, ofreciendo herramientas de visualización y control que replican prácticas industriales.

Además, el proyecto sirvió como medio de formación y concientización sobre el cumplimiento de normativas internacionales, aportando valor tanto a la formación universitaria como a la práctica profesional.

---

11. ANEXOS

Anexo A. Capturas del Sistema

- Inicio de sesión
- Panel de monitoreo
- Simulación de amenaza
- Modo emergencia activo
- Gráfica de tráfico

Anexo B. Manual de Usuario Completo

- Instrucciones detalladas de cada módulo
- Explicación de scripts y su funcionamiento

Anexo C. Código Fuente Principal

- `monitoreo.php`, `login.php`, `dashboard.php`
- `script.js`, `visualizacion_uav.js`, `monitoreo_uav.js`
- `style.css`, `tabs_dinamicos.js`, `menu.php`

Anexo D. Base de Datos

- Estructura de las tablas: `usuarios`, `eventos`, `logs`

- Sentencias SQL de creación y ejemplos de registros

Anexo E. Bitácora de Desarrollo

- Actividades por semana
- Entregables por sprint (Scrum)
- Lecciones aprendidas y obstáculos superados