UNIVERSIDAD EAN

GUIA DIGITAL INTERACTIVA Y DE AUTODIAGNOSTICO PARA ASEGURAR DISPOSITIVOS IoT EN HOGARES DE LA COMUNIDAD EAN

GUIA 3

PRESENTADO POR:

JOSE MIGUEL GIRAL RODRIGUEZ

OSCAR EDGAR VARGAS NEIRA

JEAN CARLO RAMÍREZ VALBUENA

DIRECTOR:

LEON VELASQUEZ ELIZABETH

FACULTAD DE INGENIERIA

BOGOTÁ D.C NOVIEMBRE 09 DEL 2025

Tabla de contenido

RESUMEN EJECUTIVO

Este proyecto propone una guía digital interactiva, complementada con un autodiagnóstico breve, para fortalecer las prácticas de ciberseguridad en el uso de dispositivos IoT en hogares de la comunidad académica (estudiantes y docentes) de la Universidad EAN. A partir de la adopción creciente de IoT y la falta de configuraciones seguras, se presenta un recurso educativo práctico, de rápida implementación y bajo costo. La guía ofrece pasos accionables para asegurar router, cámaras IP, asistentes de voz, enchufes/focos y TVs/consolas, e incluye checklists descargables. El autodiagnóstico (12 ítems) genera un puntaje de madurez (bajo, medio, alto) con recomendaciones personalizadas. Se evaluará la utilidad y la adopción de medidas básicas (por ejemplo, cambio de contraseñas por defecto, desactivación de WPS/UPnP, uso de redes de invitados y actualizaciones de firmware) mediante un piloto con muestra representativa de la(s) cohorte(s) del curso de Sistemas, comparando percepciones y prácticas auto-reportadas antes y después del uso de la guía.

INTRODUCCIÓN

La expansión de dispositivos IoT en hogares colombianos ha mejorado la comodidad, pero también ha introducido nuevos vectores de riesgo cuando no se aplican prácticas básicas de ciberseguridad. En la comunidad académica de la Universidad EAN (estudiantes y docentes), estos riesgos pueden derivar en exposición de datos, intrusiones y afectaciones a su desempeño académico y profesional. Aunque existe literatura técnica, muchos usuarios no aplican configuraciones mínimas por desconocimiento, tiempo o complejidad percibida. Este proyecto presenta una guía digital interactiva con autodiagnóstico que traduce buenas prácticas en acciones concretas de 30 minutos y permite evaluar el nivel de madurez de seguridad en el hogar, cerrando la brecha entre conocimiento y práctica con un recurso práctico, atractivo y reutilizable.

OBJETIVOS

OBJETIVO GENERAL:

Diseñar una guía digital interactiva con autodiagnóstico para mejorar las prácticas de ciberseguridad en el uso de dispositivos IoT en hogares de la comunidad académica de la Universidad EAN.

OBJETIVOS ESPECÍFICOS:

- Identificar los dispositivos IoT más comunes en el entorno doméstico de la comunidad académica EAN y las prácticas básicas de seguridad aplicables.
- Desarrollar un autodiagnóstico de 12 ítems que clasifique el nivel de madurez de seguridad en tres niveles (bajo, medio, alto) y brinde recomendaciones personalizadas.
- Elaborar contenidos básicos paso a paso para asegurar router, cámaras IP, asistentes de voz, enchufes/focos y televisores/consolas, incluyendo checklists descargables.
- Validar la usabilidad y la claridad de la guía mediante un piloto con una muestra representativa del curso de Sistemas, midiendo percepción de utilidad y cambios auto reportados en prácticas.

DESCRIPCIÓN DEL PROBLEMA

- Durante 2024–2025, el crecimiento de dispositivos IoT en los hogares de la comunidad académica de la Universidad EAN (estudiantes y docentes) ha sido notable: desde routers avanzados hasta cámaras IP, asistentes de voz, enchufes inteligentes y televisores conectados. Sin embargo, este aumento no ha ido acompañado de una cultura sólida de ciberseguridad. Persisten prácticas inseguras recurrentes, como el uso de contraseñas por defecto, la activación innecesaria de funciones como WPS o UPnP, la falta de actualizaciones de firmware y la ausencia de segmentación de redes. Esta brecha expone a la comunidad a riesgos como intrusiones remotas, botnets y filtración de datos. La evidencia anecdótica y diagnósticos preliminares indican que las recomendaciones disponibles suelen ser demasiado técnicas, dispersas y poco adaptadas a contextos domésticos con recursos limitados. En consecuencia, muchas personas optan por ignorar la seguridad hasta que se presenta un incidente, lo que refleja un vacío crítico de conocimiento aplicado. Se requiere un recurso sencillo, guiado e interactivo que facilite la implementación de buenas prácticas mínimas viables sin demandar conocimientos avanzados ni inversión significativa.

JUSTIFICACIÓN

La investigación se justifica por la necesidad de fortalecer la cultura de ciberseguridad en la comunidad académica de la Universidad EAN, que, pese al creciente uso de dispositivos IoT en sus hogares, carece de recursos prácticos para implementar medidas de protección básicas. La propuesta de una guía digital interactiva con autodiagnóstico es factible y de alto impacto: puede desarrollarse rápidamente con herramientas no-code (Google Sites/Notion/Canva) y difundirse ampliamente. Los beneficios se reflejan a nivel:

- Académico: recurso pedagógico aplicable en cursos y proyectos prácticos
- Personal: reducción de riesgos de seguridad en el hogar.
- Institucional: material reutilizable para programas de formación y bienestar.

Además, el autodiagnóstico propuesto permitirá medir de forma inicial el nivel de madurez en ciberseguridad y evaluar cambios en las prácticas de los estudiantes, aportando para futuras investigaciones y mejoras. De este modo, el proyecto contribuye tanto al desarrollo académico como a la formación de competencias profesionales alineadas con los desafíos de la transformación digital.

La guía digital interactiva es la opción más factible y de mayor relación impacto/esfuerzo: puede desarrollarse en 1–2 semanas con herramientas no-code (Google Sites/Notion/Canva) y permite llegar rápidamente a la población objetivo. Ofrece beneficios académicos (formación práctica en ciberseguridad), personales (reducción del riesgo doméstico) y institucionales (material reutilizable para cursos o bienestar). Su enfoque en acciones concretas de corto tiempo favorece la adopción y compromiso. Complementar la guía con un autodiagnóstico variado, preciso y de fácil entendimiento incrementa el involucramiento y permite medir resultados básicos, aportando evidencia para futuras mejoras.

ANÁLISIS DE REQUERIMIENTOS

Para asegurar que el proyecto sea realmente útil y viable, se definieron los siguientes puntos:

Intención del producto

Requerimientos funcionales

La guía debe contar con un autodiagnóstico de 12 preguntas, el cual entregue un nivel de madurez en ciberseguridad (bajo, medio o alto) acompañado de recomendaciones acordes a cada resultado.

Es necesario que ofrezca instrucciones prácticas y claras, paso a paso, para proteger al menos cinco dispositivos IoT de uso común en los hogares de la comunidad académica: router, cámaras IP, asistentes de voz, enchufes o bombillos inteligentes, televisores y consolas.

Además, debe permitir la descarga de listas de verificación sencillas que faciliten a los usuarios comprobar las configuraciones aplicadas.

Verificación de parámetros de diseño

Requerimientos no funcionales

La propuesta se debe realizar con herramientas digitales que hagan en lo posible una implementación rápida y eficiente, sin perder calidad técnica.

El tiempo total de aplicación no debe de superar los 40 minutos lo ideal es (10 para el autodiagnóstico y 30 para las configuraciones).

El lenguaje debe ser claro, pedagógico y pensado para personas que no tengan conocimientos avanzados en tecnología, pero aun así mantener una precisión técnica.

Se busca que el proyecto sea de bajo costo, fácil de actualizar y que sea escalable en el futuro, garantizando su sostenibilidad.

Estimación de características y especificaciones

Restricciones iniciales

El desarrollo estará enfocado en plataformas que tengan un despliegue sencillo, para de esta manera reducir la complejidad operativa y cumplir con los plazos.

El alcance se limitará únicamente a dispositivos IoT que sean de uso doméstico, dejando por fuera los entornos empresariales e industriales.

El piloto será aplicado en un grupo de estudiantes y docentes de la Universidad EAN.

Recursos necesarios

Un equipo de trabajo conformado por 3 estudiantes autores del proyecto y el acompañamiento del tutor del proyecto.

Acceso a la base de datos académica y algunas guías sobre buenas prácticas en ciberseguridad para IoT.

Herramientas digitales de diseño y publicación en línea por ejemplo: Google Sites, Canva y formularios web.

Retroalimentación por parte de la comunidad académica, con el fin de comprobar la claridad y utilidad de la propuesta.

MARCO DE REFERENCIA

En este apartado presentamos los conceptos, referentes y evidencias que sustentan el diseño de una guía digital interactiva con autodiagnóstico para mejorar la ciberseguridad de dispositivos IoT en hogares de la comunidad EAN. El propósito es conectar lo que ya se

conoce sobre el tema con la solución propuesta, para que el proyecto no parta de cero y mantenga coherencia con estándares reconocidos.

Conceptos básicos

- **Superficie de ataque en el hogar**
  puntos por donde un atacante podría acceder a la red o a los equipos. En IoT doméstico se relaciona con contraseñas por defecto, WPS/UPnP activos, puertos expuestos, firmware sin actualizar y redes sin segmentación.
- **Madurez de ciberseguridad**
  nivel en que un hogar aplica prácticas básicas de protección. En el proyecto se mide con 12 ítems que clasifican el estado en bajo, medio o alto.
- **Principios guía**
  mínimo privilegio (solo lo necesario), reducción de exposición (desactivar servicios que no se usan) y privacidad por diseño (configurar para recolectar y exponer la menor cantidad de datos).
- **Internet de las Cosas (IoT)**
  Conjunto de dispositivos físicos interconectados que recopilan, procesan y transmiten datos a través de Internet.
  Villa Crespo, E., & Morales Alonso, I. (2023). Ciberseguridad IoT y su aplicación en ciudades inteligentes. Ediciones de la U.
- **Protocolos IoT**
  Protocolos ligeros diseñados para dispositivos con recursos limitados.
  Universitat Oberta de Catalunya. (2022). Protocolos de comunicación de nueva generación. UOC. https://openaccess.uoc.edu/server/api/core/bitstreams/51d0f4b4-ce25-4282-a833-86fae171d2ab/content

  https://openaccess.uoc.edu/server/api/core/bitstreams/51d0f4b4-ce25-4282-a833-86fae171d2ab/content
- **Crecimiento del IoT en hogares**

El estudio analiza las tecnologías que conforman la base del Internet del Futuro, destacando el papel del IoT en la interconexión de sistemas y servicios.

García, J. (2021). Internet del futuro: Estudio de tecnologías IoT. Revista Iberoamericana de Ingeniería, 7(2), 45-60. Dialnet

- **Ingeniería social**

  Técnica que explota la falta de conocimiento del usuario para acceder a sistemas.

  Mitnick, K. (2011). Ghost in the Wires. Little, Brown and Company.

- **Recolección de datos**
- Asistentes de voz y cámaras que recogen datos sensibles del hogar.
- Red principal y de invitados, separar dispositivos IoT en subredes limita los riesgos de intrusión.
- Checklists, herramientas pedagógicas que facilitan la aplicación de prácticas seguras.

  Zeng, E., Mare, S., & Roesner, F. (2017). End User Security & Privacy Concerns with Smart Homes. SOUPS.

  Cisco Systems. (2020). IoT Security Best Practices.

- **Cultura de ciberseguridad**

  La concientización es clave para reducir vulnerabilidades humanas.

  ENISA. (2021). Cybersecurity Culture in Organizations.

- **Futuro regulatorio**

  Normativas emergentes para la protección de usuarios en IoT.

  European Union. (2018). *General Data Protection Regulation (GDPR)*.

- **Políticas en Colombia**

  Directrices locales para la protección digital.

  Ministerio TIC (2022). *Estrategia Nacional de Ciberseguridad*.

Marcos y estándares que orientan la solución

Para evitar recomendaciones aisladas o basadas solo en experiencia, se consultaron referencias técnicas ampliamente aceptadas:

- NISTIR 8228 (NIST): sugiere gestionar riesgos de IoT a lo largo del ciclo de vida. Para el hogar, esto se traduce en inventariar dispositivos, configurar de forma segura desde el inicio, mantener actualizaciones y no exponer servicios innecesarios.
- OWASP IoT Top 10: lista riesgos frecuentes (credenciales débiles, falta de actualizaciones, servicios inseguros, configuraciones por defecto, privacidad insuficiente) y controles para mitigarlos.
- ENISA – Buenas prácticas para IoT: refuerza autenticación robusta, gestión de firmware, hardening de servicios y separación de redes.
- Guías de fabricantes y material de divulgación (por ejemplo Microsoft Security): ayudan a "aterrizar" los pasos prácticos para usuarios finales.
- Normativa colombiana de protección de datos (Ley 1581/2012) y políticas institucionales: relevantes para el manejo del autodiagnóstico y del piloto (consentimiento, minimización de datos, almacenamiento seguro).
- ISO/IEC 27001 Norma internacional sobre gestión de seguridad de la información.

Con estos insumos, la guía no solo explica "qué hacer", sino también "por qué" esas acciones reducen el riesgo.

¿Qué dice la evidencia y dónde está la brecha?

La literatura reciente sobre IoT doméstico muestra patrones que se repiten: muchas personas mantienen contraseñas por defecto, dejan WPS/UPnP activados, no actualizan firmware y no separan los dispositivos IoT de los equipos personales. Esto facilita intrusiones, el uso de los equipos como parte de botnets y la fuga de datos. Un punto importante es que varias de las medidas más efectivas son rápidas y baratas (cambiar credenciales, desactivar WPS/UPnP, crear una red de invitados, actualizar firmware), pero no se aplican por barreras comunes: desconocimiento, complejidad percibida, miedo a "dañar" la configuración y falta de guías claras pensadas para no expertos. Ahí se ubica el aporte del proyecto.

Fuentes clave RAES

- Gálvez Cisneros & Robayo Jácome (2025)
  Propósito y alcance: revisión sistemática sobre ciberseguridad en dispositivos IoT de uso doméstico. Metodológicamente mapea literatura reciente para identificar amenazas, vulnerabilidades y controles aplicables en hogares. Hallazgos clave: persisten configuraciones inseguras por defecto (credenciales, WPS/UPnP activos), firmware desactualizado y ausencia de segmentación de red, lo que habilita intrusiones, botnets y filtración de datos. Recomiendan medidas de bajo costo con alto impacto: cambio de contraseñas por defecto, actualización periódica de firmware, desactivación de servicios innecesarios (WPS/UPnP), y uso de redes de invitados para aislar IoT. Aporte al proyecto: fundamenta el enfoque práctico de la guía y las dimensiones del autodiagnóstico (contraseñas, actualizaciones, servicios, segmentación). Limita-ciones: heterogeneidad de fuentes y escasez de estudios experimentales en contextos latinoamericanos, lo que motiva la validación piloto propuesta.

Gálvez Cisneros, X. A., & Robayo Jácome, D. J. (2025). Ciberseguridad en los dispositivos IoT de uso doméstico: Una revisión sistemática de la literatura. Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS, 7(1), 140–170. https://doi-org.bdbiblioteca.universidadean.edu.co/10.59169/pentaciencias.v7i1.1371

- NISTIR 8228 (2019)
  Propósito y alcance: documento de referencia del NIST que presenta consideraciones para gestionar riesgos de ciberseguridad y privacidad en IoT. Estructura riesgos por ciclo de vida y roles (fabricantes, integradores, usuarios) y sugiere prácticas de gestión proporcionales al impacto. Hallazgos clave: necesidad de inventariar activos IoT, aplicar configuración segura por defecto, actualizar software/firmware oportunamente y minimizar exposición a Internet/servicios innecesarios. Relevancia para hogares: aunque pensado para organizaciones, sus principios se adaptan a

contextos domésticos mediante controles básicos en routers y dispositivos (autenticación fuerte, deshabilitar UPnP/WPS, segmentación/red de invitados). Aporte al proyecto: sirve de marco para priorizar controles del checklist y como respaldo técnico de las recomendaciones, sus limitaciones constan de lenguaje y enfoque organizacional, por lo que se requiere traducción pedagógica para usuarios no expertos, tarea que asume la guía.

National Institute of Standards and Technology. (2019). Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (NISTIR 8228). NIST.

OWASP IoT Top 10 (2024)

Propósito y alcance: compendio de los principales riesgos de seguridad en IoT publicado por OWASP, con enfoque en vulnerabilidades frecuentes y controles mitigadores. Riesgos relevantes para el hogar: contraseñas débiles o reutilizadas, servicios inseguros expuestos, actualizaciones inexistentes o no verificadas, configuraciones por defecto y privacidad insuficiente. Recomendaciones prácticas: gestión de credenciales únicas, desactivar servicios innecesarios (telnet/UPnP), aplicar actualizaciones firmadas, restringir exposición de puertos y aislar IoT de dispositivos de trabajo/estudio. Aporte al proyecto: ofrece una taxonomía de riesgos que guía el diseño del autodiagnóstico (12 ítems) y el contenido paso a paso por dispositivo. Refuerza la priorización de quick wins (cambiar credenciales admin, desactivar WPS/UPnP, crear red invitada, actualizar firmware). Limitaciones: nivel de abstracción alto; se complementa con guías de fabricantes y pruebas de usabilidad en el piloto.

OWASP Foundation. (2024). OWASP IoT Top 10. OWASP.

Enfoque pedagógico del proyecto

Para cerrar la brecha entre teoría y práctica, la guía se diseña con criterios de uso real:

- Tareas cortas (máximo 30 minutos) y checklists descargables.
- Lenguaje claro, pasos numerados y advertencias para evitar errores (por ejemplo, respaldar la configuración del router antes de cambiarla).
- Quick wins primero (acciones de alto impacto con poco esfuerzo).
- Autodiagnóstico de 12 preguntas que da retroalimentación inmediata y recomendaciones personalizadas.
- Contenidos accesibles desde celular y con apoyos visuales sencillos.

Cómo se refleja el marco en la guía y el autodiagnóstico

- Cada categoría de dispositivo (router, cámaras IP, asistentes de voz, enchufes/bombillos, TV/consolas) incluye acciones clave: cambio de credenciales administrativas, desactivar WPS/UPnP y otros servicios que no se usen, asegurar el Wi-Fi con WPA2/WPA3 y una clave fuerte, crear red de invitados para aislar IoT, mantener firmware actualizado y revisar accesos remotos/privacidad.
- El autodiagnóstico evalúa precisamente estos puntos y clasifica el nivel de madurez. Según el resultado, la guía sugiere qué hacer primero.
- En el piloto se medirá si las personas perciben utilidad y si reportan cambios en prácticas básicas después de usar la guía.

Este marco de referencia combina estándares técnicos (NIST, OWASP, ENISA), resultados de la literatura y un enfoque pedagógico orientado a la acción. Con eso, el proyecto busca que la comunidad EAN cuente con una guía práctica, sustentada y viable para reducir riesgos de ciberseguridad en sus hogares.

Análisis de restricciones

El desarrollo de la guía digital interactiva para fortalecer las buenas prácticas de ciberseguridad en dispositivos IoT en hogares de la comunidad debe considerar un conjunto de restricciones que pueden influir en su diseño, alcance y aplicación. A continuación, se detallan las principales limitaciones identificadas desde las diferentes perspectivas.

Restricciones ambientales

Dado que el proyecto se centra en una guía digital, su impacto ambiental directo es mínimo. No obstante, se busca fomentar la sostenibilidad mediante el uso de herramientas en línea que no requieran impresión física ni consumo adicional de recursos materiales. La propuesta contribuye de manera indirecta a la protección ambiental al promover configuraciones seguras que evitan el uso ineficiente de energía y la exposición de dispositivos IoT que puedan verse comprometidos por ciberataques que incrementen el consumo energético.

Restricciones económicas

El proyecto debe ajustarse a un presupuesto limitado, por lo que se priorizan herramientas gratuitas o de bajo costo como Google Sites, Canva y formularios web. Se descarta el uso de plataformas comerciales que pidan licencias pagas o algún tipo infraestructura tecnológica adicional. Además, la guía debe ser viable económicamente para los usuarios finales, asegurando tener acceso gratuito y sin requerir algún tipo software especializado.

Restricciones legales

La guía y el autodiagnóstico deben cumplir con la legislación colombiana sobre protección de datos personales que es la (Ley 1581 de 2012 y el Decreto 1377 de 2013), así como con también los lineamientos institucionales de la Universidad EAN. Cualquier recolección de información mediante el autodiagnóstico requerirá consentimiento el uso es exclusivo con fines académicos. También se considera las normativas internacionales relevantes, como lo es el reglamento General de Protección de Datos en lo referente a buenas prácticas.

Restricciones de salud y seguridad

Aunque el proyecto no involucra riesgos físicos o químicos, se contemplan aspectos de seguridad, las recomendaciones de la guía deben evitar que los usuarios realicen configuraciones que puedan ser peligrosas o que puedan afectar la estabilidad de su red doméstica. Por ello, se agregarán advertencias antes de cualquier cambio técnico y se recomendará siempre realizar algún tipo de copia de seguridad de las configuraciones de los dispositivos antes de modificarlos.

Restricciones socioculturales

La comunidad académica de la Universidad EAN es muy diversa en edad, también en nivel de conocimiento tecnológico y hábitos digitales. Esto nos genera una restricción de cierta manera sociocultural, ya que la guía debe adaptarse a varios perfiles de usuario. Se empleará un lenguaje claro y educativo, evitando conceptos mu técnicos o innecesarios. Además, se intentará fomentar una cultura de ciberseguridad como parte del bienestar y la responsabilidad digital, alineada con los valores institucionales

Metodología para la selección y desarrollo de la solución

Comenzamos desde el análisis de requerimientos y de las restricciones técnicas, legales, económicas y socioculturales identificadas previamente. El objetivo es garantizar que la guía digital interactiva y su autodiagnóstico se diseñen de manera segura, eficiente y viable para la comunidad académica de la Universidad EAN.

1. Generación de alternativas

Durante la fase inicial, se plantearon diversas alternativas para materializar la guía, considerando herramientas digitales disponibles y los criterios de bajo costo, accesibilidad y facilidad de actualización. Entre las opciones se evaluaron plataformas como Google Sites, Notion, Canva y la integración de formularios web interactivos. Se priorizó la combinación Google Sites + Formularios de Google por su simplicidad de implementación, su integración con cuentas institucionales y su compatibilidad con diversos dispositivos.

Asimismo, se exploraron alternativas de presentación (página estática, app móvil, documento descargable) y se seleccionó el formato web interactivo, ya que permite una experiencia dinámica, segura y fácilmente actualizable sin requerir instalación de software adicional.

2. Evaluación y descarte de soluciones ilógicas

Cada propuesta fue revisada con base en su factibilidad técnica y operativa. Se descartaron las soluciones que implicaban costos elevados de hosting, el uso de software propietario o requerimientos técnicos complejos que excedieran el alcance académico del proyecto. También se evitó incluir funcionalidades que comprometieran la protección de datos personales de los usuarios, en cumplimiento con la Ley 1581 de 2012 y la Estrategia Nacional de Ciberseguridad (MinTIC, 2022). De igual forma, se excluyeron ideas que pudieran

contradecir principios técnicos o de seguridad, como almacenar contraseñas o información sensible en servidores no controlados institucionalmente.

3. Comparación con hechos y experiencias conocidas

Para asegurar la validez de la solución, se revisaron experiencias previas y buenas prácticas documentadas en guías internacionales como NISTIR 8228 (2019), OWASP IoT Top 10 (2024) y ENISA (2021). Estas fuentes sirvieron como referencia para estructurar los contenidos y definir el alcance del autodiagnóstico.

4. Evaluación y refinamiento de alternativas

A partir de los criterios, se seleccionó la alternativa más viable:

- Plataforma: Google Sites como contenedor principal.
- Contenido visual: Canva, para el diseño de checklists descargables.
- Evaluación del usuario: Formulario web con retroalimentación automática, basado en los 12 ítems del autodiagnóstico.

Esta solución fue refinada de acuerdo con los riesgos identificados en el análisis previo:

- **Riesgo de baja comprensión técnica**: uso de lenguaje pedagógico y ejemplos visuales.
- **Riesgo de error en configuración de dispositivos**: incorporación de advertencias previas y pasos reversibles.
- **Riesgo de desactualización tecnológica**: estructura modular que permite actualizar contenidos fácilmente.

5. Criterios de selección final

La selección definitiva de la solución se basó en tres dimensiones:

- Económica: mínimo costo de desarrollo y mantenimiento.

- Ambiental: uso exclusivo de medios digitales, evitando materiales físicos.
- Social y educativa: accesibilidad para usuarios con distintos niveles de conocimiento tecnológico y fomento de la cultura de ciberseguridad.

La guía final responde al equilibrio entre impacto, factibilidad y sostenibilidad, integrando la función pedagógica con la validación técnica y la protección de datos.

6. Desarrollo de la solución

El desarrollo se llevará a cabo siguiendo las etapas:

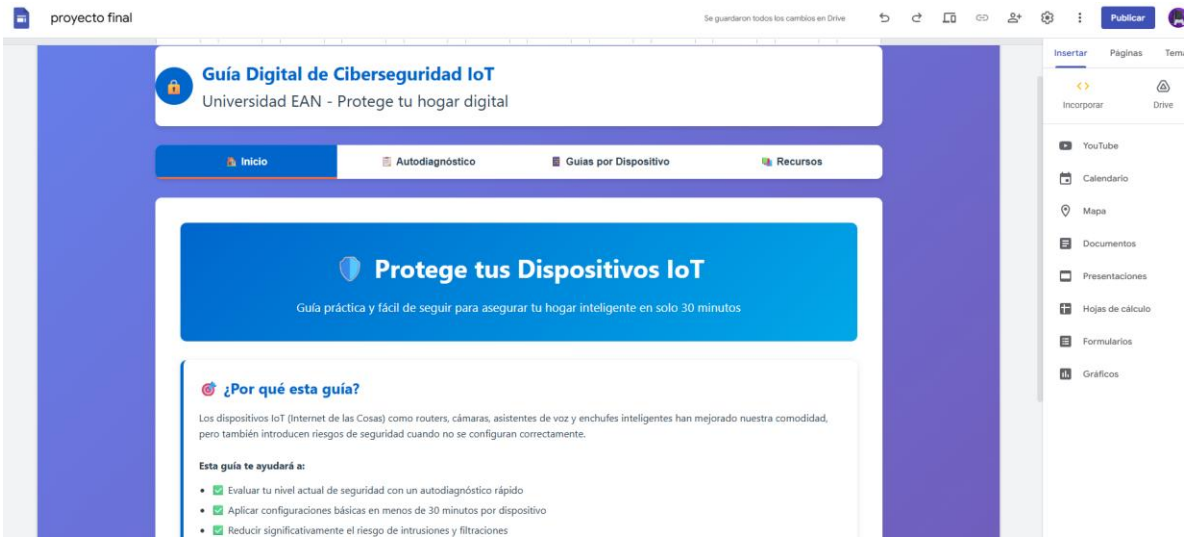
1. Diseño estructural del sitio web (mapa de contenidos y navegación).
2. Redacción y adaptación de los contenidos técnicos según los estándares NIST y OWASP.
3. Diseño visual de checklists descargables y banners educativos.
4. Implementación del formulario de autodiagnóstico con cálculo automático de nivel de madurez.
5. Validación piloto con grupo de estudiantes y docentes, midiendo claridad, utilidad y cambios en las prácticas.
6. Ajustes finales según retroalimentación y preparación del informe de evaluación.

Es la opción más coherente con los objetivos del proyecto. Integra criterios técnicos, pedagógicos y éticos, garantizando un impacto real en la mejora de prácticas seguras dentro de los hogares de la comunidad EAN.

ALTERNATIVA DE SOLUCIÓN

El diseño completo de la guía digital, descrita.

La guía tiene un diseño limpio, moderno y pensado para que cualquier persona la use sin complicaciones. Visualmente busca transmitir confianza: predominan fondos claros y espacios abiertos, con acentos en azul para las acciones importantes y toques de verde cuando algo es positivo o está bien configurado. Hay también colores de aviso (amarillo) y error (rojo) usados con moderación para llamar la atención sólo cuando hace falta.



Nota: elaboración propia de guía

Los botones son claros y fáciles de identificar. El botón principal, en azul, destaca las acciones clave como “Realiza el Autodiagnóstico”; al pasar el cursor o tocarlo cambia ligeramente para indicar que está activo. Los botones secundarios tienen borde y fondo transparente para acciones menos urgentes, como descargar un PDF. Los enlaces y pequeñas acciones usan un verde amable que refuerza la sensación de

avance y seguridad.

Nota: elaboración propia de guía

El autodiagnóstico está presentado de forma amigable: preguntas directas con opciones grandes y fáciles de seleccionar, y una barra de progreso que muestra cuánto falta. Al terminar, los resultados aparecen de forma clara: un nivel (Bajo/Medio/Alto) y recomendaciones priorizadas para que sepas qué hacer primero. Todo está pensado para que la interacción no sea estresante y puedas completar el proceso en pocos minutos.

Nota: elaboración propia de guía

La estructura (secciones, menús, navegación).

la guía es como un libro interactivo o una aplicación sencilla. Está organizada de forma lógica para que siempre sepas dónde estás y cómo llegar a la información que necesitas. No hay laberintos ni páginas ocultas; todo está a la vista y es fácil de encontrar.

El menú principal: Tu brújula

Nota: elaboración propia de guía

En la parte superior de la guía, siempre visible, encontrarás un **menú principal** que funciona como tu brújula. Tiene cuatro puntos clave, como los capítulos de un libro:

- **Inicio:** Es la portada de la guía. Aquí te damos la bienvenida, te explicamos rápidamente de qué va todo y te invitamos a empezar tu viaje por la ciberseguridad. Es el punto de partida.

- **Autodiagnóstico:** Este es el corazón interactivo de la guía. Es donde puedes evaluar qué tan seguro está tu hogar digital. Piensa en ello como un pequeño cuestionario que te ayuda a entender tu situación actual.

- **Guías por Dispositivo:** Aquí es donde está la acción. Si ya sabes qué dispositivo quieres proteger (tu router, una cámara, el asistente de voz), esta sección te lleva directamente a las instrucciones paso a paso para cada uno. Es como tener un manual específico para cada aparato.

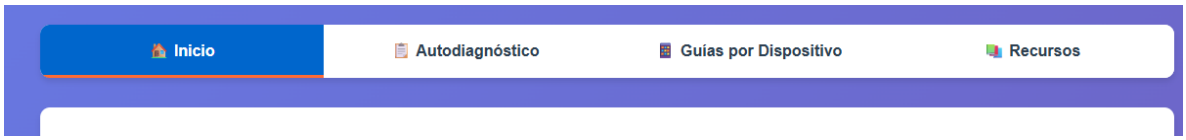
- **Recursos:** Esta sección es tu biblioteca de apoyo. Si quieres profundizar, entender algún término técnico o buscar más información, aquí encontrarás un glosario, enlaces útiles y las referencias que sustentan la guía.

Navegación: Siempre sabes dónde ir

La forma en que te mueves por la guía es muy intuitiva. Puedes ir de un punto a otro usando el menú principal, o seguir el "flujo" natural que te proponemos:

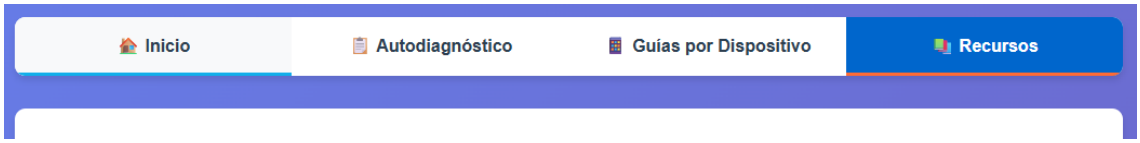
- **Empezar por el principio:** Lo ideal es ir a "Inicio", luego hacer el "Autodiagnóstico" para saber dónde estás parado, y después ir a las "Guías por Dispositivo" para aplicar las recomendaciones.
- **Ir directo al grano:** Si ya sabes que quieres configurar tu router, puedes ir directamente a "Guías por Dispositivo" y buscar la sección del router.

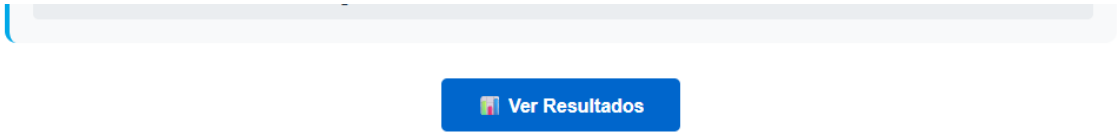
- **Botones que te guían:** Dentro de cada sección, hay botones claros que te invitan a la siguiente acción lógica (por ejemplo, "Ver Resultados" después del autodiagnóstico, o "Descargar Checklist PDF" en las guías de dispositivos).

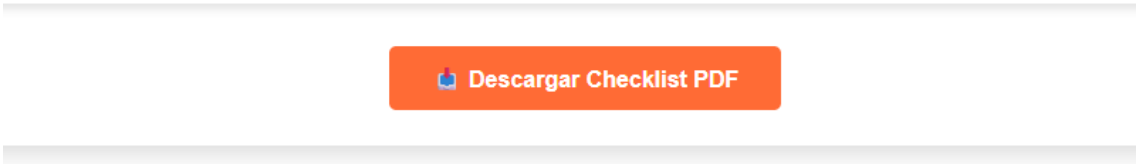
- 

- 

- 

- 

- 



Nota: elaboración propia de guía

Secciones de contenido: Organizadas para ti

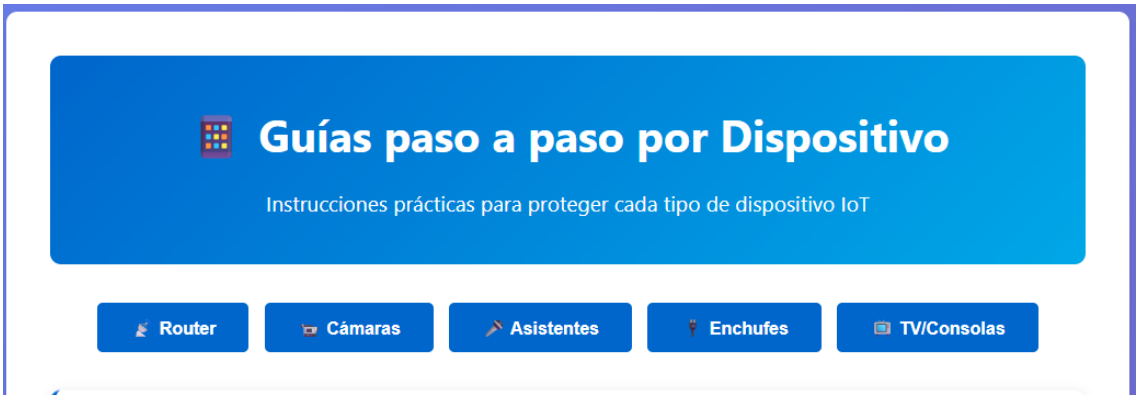
Cada "capítulo" de la guía está bien estructurado:

- **En el Autodiagnóstico:** Verás una pregunta a la vez o un grupo pequeño, con opciones de respuesta claras. Una barra de progreso te indica cuánto te falta. Al final, un resumen de tus resultados y las recomendaciones personalizadas.

Nota: elaboración propia de guía

Nota: elaboración propia de guía

- **En las Guías por Dispositivo:** Cada dispositivo (router, cámaras, asistentes de voz, etc.) tiene su propia página o subsección. Dentro de cada una, encontrarás:
    - Un título claro y un tiempo estimado para completar la configuración.
    - Advertencias importantes (por ejemplo, "haz una copia de seguridad antes de cambiar esto").
    - Una lista numerada de **pasos sencillos y concretos** que debes seguir.
    - Un **checklist** al final, para que puedas verificar que no se te olvidó nada.
    - Un botón para descargar ese checklist en formato PDF.



Nota: elaboración propia de guía

En Recursos: Verás listas de términos con sus explicaciones (el glosario) y enlaces a otras páginas web o documentos que te pueden ser útiles si quieres saber más.

Nota: elaboración propia de guía

El **contenido**: autodiagnóstico, recomendaciones IoT, checklists.

El contenido de la guía es el corazón de su utilidad, diseñado para ser directo, práctico y accionable. Se estructura en tres pilares fundamentales: el autodiagnóstico, las recomendaciones específicas para dispositivos IoT y los checklists de verificación.

El **autodiagnóstico** funciona como un "chequeo" inicial para el hogar digital. Consiste en 12 preguntas clave que evalúan las prácticas de ciberseguridad del usuario, abordando temas como el cambio de contraseñas por defecto, la configuración de la red Wi-Fi, la gestión de actualizaciones y el uso de funciones de seguridad. Las opciones de respuesta son intuitivas, permitiendo al usuario reflejar su situación de manera precisa. Al finalizar, la guía proporciona un nivel de madurez en ciberseguridad (Bajo, Medio o Alto) y, crucialmente, ofrece recomendaciones personalizadas y priorizadas, indicando al usuario las acciones más urgentes y de mayor impacto para mejorar su seguridad.

Las **recomendaciones IoT** constituyen el manual de instrucciones detallado para proteger los dispositivos. La guía ofrece pasos específicos para los aparatos más comunes en un hogar inteligente: routers Wi-Fi, cámaras IP, asistentes de voz, enchufes y focos inteligentes, y televisores y consolas. Para cada categoría, se detallan acciones concretas como cambiar credenciales predeterminadas, configurar cifrados de red robustos (WPA2/WPA3), desactivar funciones vulnerables (WPS, UPnP), mantener el firmware actualizado, crear redes de invitados para aislar dispositivos IoT, y revisar permisos o accesos remotos. La explicación es sencilla, evitando tecnicismos y enfatizando la importancia de cada paso con advertencias claras cuando es necesario.

Finalmente, los **checklists** actúan como listas de verificación para asegurar que no se omita ningún paso importante. Después de cada sección de recomendaciones por dispositivo, se presenta una lista concisa de los puntos clave que el usuario debe

haber configurado o revisado. Estos checklists son una herramienta práctica para confirmar la implementación de las medidas de seguridad y pueden descargarse en formato PDF o imprimirse, facilitando su uso durante el proceso de configuración y para futuras revisiones periódicas.

Las herramientas que usaríano usaron (Google Sites, Canva, Google Forms).

Usaron herramientas no-code al inicio (Google Sites para publicar la guía, Google Forms para el autodiagnóstico y Canva para los checklists y recursos visuales). Esa combinación funciona rápido y sin invertir mucho, pero al probarla detectaron limitaciones: Google Sites/Forms no permitía lógica condicional avanzada, la experiencia móvil/visual no se pudo pulir como se quería, y la integración para calcular puntajes, mostrar recomendaciones personalizadas en la misma página y generar PDFs dinámicos quedó limitada.

- Por eso se propuso pasar a una solución con programación: construir la web como un proyecto estático dinámico (HTML/CSS/JS) o con un framework ligero (React/Vue) y desplegarlo en Netlify o GitHub Pages. La idea es mantener la facilidad de despliegue pero ganar control: implementar el autodiagnóstico con lógica propia (cálculo de puntaje y recomendaciones en tiempo real), mostrar resultados en la misma página, habilitar descargas de checklists generadas al vuelo (PDFs) y agregar tracking/analítica personalizada

Ventajas de programarlo:

UX más fluida: preguntas dinámicas, barra de progreso más interactiva y recomendaciones priorizadas según las respuestas.

Integración directa: almacenar resultados, enviar correos opcionales, mostrar gráficas de madurez al instante.

Checklists y PDFs personalizados al momento, sin depender de descargas manuales o plantillas estáticas.

Mejor control de diseño, accesibilidad y rendimiento (optimizar para móvil).

ANÁLISIS DE COSTOS

El presente análisis de costos tiene como propósito establecer y documentar los recursos económicos, técnicos y humanos necesarios para el desarrollo del proyecto de grado (Guía Digital Interactiva y Autodiagnóstico para la Ciberseguridad IoT) en la Comunidad Académica de la Universidad EAN.

Aunque la ejecución del proyecto se realizó sin inversión financiera directa gracias al uso de herramientas gratuitas y recursos institucionales, resulta fundamental estimar el costo equivalente del trabajo, del tiempo invertido y de los materiales utilizados. Esto permite evaluar la viabilidad real del proyecto, así como su sostenibilidad en caso de replicarse o escalarse en un entorno profesional.

El análisis se estructura en cuatro categorías:

1. Costos directos, asociados al desarrollo técnico, la mano de obra y las herramientas utilizadas.
2. Costos indirectos, relacionados con servicios, infraestructura y recursos complementarios.

3. Gastos administrativos, necesarios para la organización y gestión del proyecto.
4. Inversión inicial y valoración equivalente, que reflejan el costo total si el proyecto se desarrollara en un entorno comercial.

1. COSTOS DIRECTOS

Los costos directos comprenden aquellos elementos estrictamente necesarios para la producción de la guía digital, incluyendo mano de obra, herramientas tecnológicas y recursos para pruebas.

1.1 Mano de obra (valor equivalente profesional)

Aunque la elaboración del proyecto se realizó sin ninguna compensación económica, se presenta un cálculo equivalente basado en estándares del sector para dimensionar el esfuerzo involucrado.

Rol	Cantidad de horas	Tarifa estimada	Costo estimado
Estudiantes desarrolladores (3)	72 horas c/u	$15.000 COP / hora	$3.240.000 COP
Tutor académico	12 horas	$40.000 COP / hora	$480.000 COP
Total equivalente del trabajo	—	—	**$3.720.000 COP**

Este valor refleja el esfuerzo técnico, investigativo, metodológico y operativo realizado durante varias semanas de trabajo continuo.

Costo real asumido por el proyecto: $0 COP.

1.2 Herramientas digitales utilizadas

El desarrollo de la guía digital se apoyó en plataformas de diseño, creación de formularios y publicación en línea. Se seleccionaron herramientas gratuitas para garantizar accesibilidad y eficiencia.

Herramienta / Plataforma	Uso específico en el proyecto	Costo
Plataforma digital de publicación	Estructuración, maquetación y despliegue de la guía	$0
Herramientas de diseño (Canva u similares)	Creación de iconografía, encabezados y material visual	$0
Formularios digitales	Desarrollo del autodiagnóstico interactivo	$0
Sistemas de almacenamiento en la nube	Almacenamiento de documentos, versiones y material base	$0
Total herramientas digitales	—	**$0 COP**

Todas las plataformas utilizadas cuentan con versiones gratuitas que ofrecen las funcionalidades necesarias para el alcance del proyecto.

1.3 Equipos y material de prueba

Para validar las recomendaciones de configuración, se realizaron pruebas con dispositivos IoT reales, pertenecientes a los integrantes del proyecto o disponibles en entornos domésticos cercanos.

Recurso	Uso en el proyecto	Costo
Router doméstico	Pruebas de configuración y seguridad	$0
Cámara IP	Validación de seguridad y accesos	$0
Asistente de voz inteligente	Comprobación de ajustes de privacidad	$0
Televisor inteligente (Smart TV)	Verificación de configuraciones	$0
Computadores personales	Documentación, análisis y diseño	$0
Total	—	**$0 COP**

No se incurrió en costos adicionales, puesto que los dispositivos utilizados eran personales o de uso común.

2. COSTOS INDIRECTOS

Los costos indirectos comprenden servicios, recursos institucionales y consumos generales necesarios para la ejecución del proyecto.

Recurso	Responsable / Fuente	Costo
Internet	Hogares de los integrantes	$0
Energía eléctrica	Hogares y Universidad	$0
Espacios de estudio institucionales	Universidad EAN	$0
Servicios digitales de comunicación	Plataformas de videollamadas	$0
Total costos indirectos	—	**$0 COP**

Estos costos se consideran cubiertos por los estudiantes.

3. GASTOS ADMINISTRATIVOS

Incluyen actividades de coordinación, seguimiento, análisis de resultados y documentación final.

Actividad	Descripción	Costo
Coordinación del proyecto	Reuniones, planificación y control de entregables	$0
Aplicación del piloto	Evaluación con estudiantes y docentes	$0
Recolección y análisis de datos	Procesamiento de resultados del autodiagnóstico	$0
Elaboración del informe final	Redacción, edición, correcciones y ajustes finales	$0
Total gastos administrativos	—	**$0 COP**

Toda la gestión administrativa fue realizada por los integrantes del proyecto bajo supervisión académica.

4. INVERSIÓN INICIAL Y COSTO TOTAL

A continuación se presenta el costo equivalente total del proyecto si se hubiese contratado en un entorno profesional.

Concepto	Costo estimado
Desarrollo completo de la guía digital	$3.720.000 COP
Material de apoyo y diseño visual	$0
Publicación digital (servicios gratuitos utilizados)	$0
Total equivalente del proyecto	$3.720.000 COP
Total real invertido (como proyecto académico)	**$0 COP**

La diferencia entre costo equivalente y costo real demuestra el alto valor generado por el trabajo académico colaborativo.

5. Conclusión del Análisis de Costos

El proyecto demuestra ser altamente viable y sostenible desde el punto de vista económico. La totalidad de su ejecución se apoyó en herramientas gratuitas, recursos propios y acompañamiento institucional, lo que permitió que el costo real fuera de $0 COP.

Sin embargo, el valor equivalente del trabajo realizado asciende a más de $3.720.000 millones de pesos, cifra que refleja el esfuerzo técnico, metodológico y profesional que implicó el desarrollo de la guía digital.

El proyecto es económicamente accesible, escalable, replicable y sostenible dentro de la Universidad EAN. Asimismo, su bajo costo operativo hace viable su ampliación futura hacia cursos, facultades u otros programas académicos.

PLAN DE IMPLEMENTACIÓN

1. **Cómo se haría el piloto**

El piloto se realizará con un grupo controlado de participantes de la comunidad académica de la Universidad EAN, con el fin de validar la claridad, usabilidad y efectividad de la guía digital.La implementación se llevará a cabo en modalidad virtual, utilizando la versión funcional de la guía, junto con el autodiagnóstico en Google Forms.
El procedimiento incluirá tres fases dividas en:

- **Pretest:** aplicación del autodiagnóstico inicial para conocer el nivel de madurez en ciberseguridad del hogar antes del uso de la guía.
- **Intervención:** uso libre de la guía durante una semana, aplicando las configuraciones y checklists sugeridos.
- **Postest:** nuevo autodiagnóstico y encuesta de retroalimentación sobre claridad, utilidad y experiencia de uso y que tanto cambio sobre el autodiagnóstico inicial.

2. **Con quiénes (estudiantes y docentes EAN)**

El piloto se aplicará a una muestra de 15 a 20 participantes, divididos entre:

- **Estudiantes de pregrado en Ingeniería de Sistemas y afines (90%)**, que representan usuarios jóvenes familiarizados con tecnología, pero con prácticas de seguridad variables.

- **Docentes del área de tecnología e innovación (10%)**, que aportan una visión más crítica y metodológica sobre la aplicabilidad y claridad del contenido.

(Todos los participantes deberán otorgar consentimiento informado, garantizando el cumplimiento de la Ley 1581 de 2012 sobre protección de datos personales).

3. En qué tiempo

El piloto tendrá una duración total de tres semanas, distribuidas así:

- **Semana 1:** Aplicación del autodiagnóstico inicial y entrega del enlace a la guía.
- **Semana 2:** Uso de la guía, implementación de configuraciones y aplicación del postest con encuesta de usabilidad.
- **Semana 3**: Se reservará para analizar resultados y ajustar el contenido antes de la versión final.

4. Cómo se evaluará la usabilidad y claridad

La evaluación se basará en tres criterios principales:

- **Usabilidad:** Facilidad de navegación, comprensión de instrucciones, percepción de utilidad.
- **Claridad:** Nivel de comprensión del lenguaje técnico, coherencia visual y facilidad para seguir los pasos propuestos.
- **Impacto percibido:** Cambios auto-reportados en las prácticas de ciberseguridad después del uso de la guía.

Cada dimensión se medirá con indicadores como:

- Porcentaje de usuarios que completan el autodiagnóstico.
- Puntuaciones promedio de satisfacción (escala Likert de 1 a 5).
- Evolución del nivel de madurez (bajo → medio → alto) entre el pretest y el postest.

Escala de Likert – ¿Qué es? ¿Cómo se usa? ¿Dónde se utiliza?, Yi Min Shum,2020 MAYO 27, Escala de Likert – ¿Qué es? ¿Cómo se usa? ¿Dónde se utiliza?

5. **Qué instrumentos se usarán**

Se emplearán instrumentos mixtos (cuantitativos y cualitativos):

- **Encuesta digital de percepción y usabilidad**, para medir facilidad de uso, claridad y utilidad percibida.
- **Observación indirecta** mediante el seguimiento de métricas de Google Forms (tiempo de respuesta, tasa de completado).
- **Análisis comparativo de resultados** del autodiagnóstico antes y después del uso de la guía, identificando mejoras en la madurez de ciberseguridad.
- **Comentarios abiertos** para recoger sugerencias y detectar puntos de mejora en la redacción o diseño visual.

ENLACE DE LA GUIA

https://guia-digital-interactiva.netlify.app/

CONCLUSIONES

El proyecto de la guía digital interactiva ha logrado crear un recurso práctico y bien fundamentado para mejorar la ciberseguridad en los hogares de la comunidad EAN. La reflexión final del proyecto destaca que se ha construido una herramienta accesible que traduce conceptos técnicos complejos en acciones sencillas, basándose en estándares como NIST y OWASP. La versión web actual demuestra su viabilidad, pero también señala oportunidades para una mayor personalización y una experiencia de usuario más fluida.

El impacto esperado es significativo: se anticipa una mejora tangible en las prácticas de seguridad básicas de estudiantes y docentes, como el cambio de contraseñas por defecto y el uso de redes de invitados, lo que a su vez elevará la conciencia general sobre ciberseguridad. Este impacto se medirá a través de indicadores clave de rendimiento (KPIs) como la tasa de completado del autodiagnóstico y la evolución de los niveles de madurez de seguridad.

La guía mejora la ciberseguridad en la comunidad EAN al ofrecer una herramienta que desmitifica la seguridad IoT, prioriza acciones de alto impacto y proporciona un autodiagnóstico personalizado que dirige al usuario hacia las intervenciones más relevantes. Esto no solo reduce la superficie de ataque en los hogares, sino que también fomenta una cultura de seguridad proactiva. De cara al futuro, las líneas de desarrollo se centran en una "versión 2.0" que priorice la implementación de un piloto controlado para validar el impacto,

seguido de una migración del autodiagnóstico a una plataforma programada que permita una lógica de puntuación y recomendaciones más dinámica y personalizada, así como la generación de PDFs y checklists adaptados al usuario. A mediano plazo, se buscará enriquecer las guías con capturas de pantalla y tutoriales específicos para modelos de dispositivos comunes, y asegurar la accesibilidad universal de la plataforma.

A largo plazo, se explorarán innovaciones como la integración opcional con la red local para la detección de dispositivos (siempre con consentimiento y respetando la privacidad) y la integración curricular de la guía en los programas académicos de la Universidad EAN, asegurando su sostenibilidad y relevancia continua. Es crucial, en todas estas fases, mantener un estricto apego a las consideraciones éticas y legales, especialmente en lo referente a la privacidad y el manejo de datos personales, conforme a la normativa vigente.

REFERENCIAS

Gálvez Cisneros, X. A., & Robayo Jacome, D. J. (2025). Ciberseguridad en Los Dispositivos Iot De Uso Doméstico: Una Revisión Sistemática De La Literatura. *Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS*, *7*(1), 140–170. https://doi-org.bdbiblioteca.universidadean.edu.co/10.59169/pentaciencias.v7i1.1371

Villa Crespo, E., Morales Alonso, I.(2023). *Ciberseguridad IoT y su aplicación en ciudades inteligentes*. Ediciones de la U. https://www-ebooks7-24-com.bdbiblioteca.universidadean.edu.co/?il=35416

¿Qué es un ciberataque? | Seguridad de Microsoft. (2017). Microsoft.com. https://www.microsoft.com/es-mx/security/business/security-101/what-is-a-cyberattack

National Institute of Standards and Technology. (2019). Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks (NISTIR 8228). NIST.

OWASP Foundation. (2024). OWASP IoT Top 10. OWASP. https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project

Mitnick, K. (2011). *Ghost in the Wires*. Little, Brown and Company.

Universitat Oberta de Catalunya. (2022). Protocolos de comunicación de nueva generación. UOC. https://openaccess.uoc.edu/server/api/core/bitstreams/51d0f4b4-ce25-4282-a833-86fae171d2ab/content

Villa Crespo, E., & Morales Alonso, I. (2023). Ciberseguridad IoT y su aplicación en ciudades inteligentes. Ediciones de la U.

Zeng, E., Mare, S., & Roesner, F. (2017). *End User Security & Privacy Concerns with Smart Homes*. SOUPS.

Cisco Systems. (2020). *IoT Security Best Practices*.

ENISA. (2021). *Cybersecurity Culture in Organizations*.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013*.

European Union. (2018). *General Data Protection Regulation (GDPR)*.

Ministerio TIC (2022). *Estrategia Nacional de Ciberseguridad*.