REVISTA DE
INVESTIGACIÓN ACADÉMICA SIN FRONTERA

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

REVISTAS UNISON
"El saber de mis hijos hará mi grandeza"

# Cultura de la Ciberseguridad en UABC

# Cybersecurity Culture at UABC

**Macias Aja Luz Karina[1] y Figueroa Villanueva Adelaida[2]**

[1]Universidad Autónoma de Baja California, Facultad de Ciencias Administrativas de Mexicali. Boulevard Rio Nuevo y Eje Central, CP 21330, Mexicali, Baja California, México.
karina.macias@uabc.edu.mx 0009-0002-0355-137X 686-280-16-83

[2]Universidad Autónoma de Baja California, Facultad de Ciencias Administrativas de Mexicali. Boulevard Rio Nuevo y Eje Central, CP 21330, Mexicali, Baja California, México.
afigueroa@uabc.edu.mx 0000-0003-2743-9948

DOI: https://doi.org/10.46589/riasf.v1i43.764

Recibido: 11 de abril de 2025.
Aceptado: 6 de junio 2025.
Publicado: 13 de junio de 2025.

Como citar
Macias Aja, L. K., & Figueroa Villanueva, A. (2025). Cultura de la Ciberseguridad en UABC. Revista De Investigación Académica Sin Frontera: Facultad Interdisciplinaria De Ciencias Económicas Administrativas - Departamento De Ciencias Económico Administrativas-Campus Navojoa, 1(43). https://doi.org/10.46589/riasf.v1i43.764

## Resumen

La creciente digitalización en las instituciones educativas ha intensificado la necesidad de fortalecer la ciberseguridad. En este contexto, la Universidad Autónoma de Baja California (UABC) enfrenta desafíos importantes ante la creciente cantidad de dispositivos conectados a su red. El presente trabajo propone el desarrollo de una cultura de ciberseguridad mediante una estrategia integral que incluye talleres, cursos, campañas informativas y el desarrollo de una plataforma digital llamada UABCiberSegura. Esta plataforma ofrece recursos educativos, reportes de incidentes, herramientas de protección y un sistema de alertas para la comunidad universitaria.



ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

Se adoptó una metodología ágil para su desarrollo, con tecnologías como JavaScript y el modelo MVC, además del uso de marcos de gestión como ITIL. Los resultados reflejan un aumento en la participación y concienciación sobre prácticas seguras. La investigación concluye que fomentar una cultura de ciberseguridad desde una perspectiva educativa y tecnológica es esencial para proteger los activos digitales institucionales y responder eficazmente ante las amenazas. El proyecto sienta las bases para futuras estrategias de resiliencia digital en la UABC.

**Palabras Clave:** ciberseguridad, universidad, cultura digital, educación, TICs

## Abstract

The increasing digitalization of educational institutions has intensified the need to strengthen cybersecurity. In this context, the Autonomous University of Baja California (UABC) faces significant challenges due to the growing number of devices connected to its network. This project proposes the development of a cybersecurity culture through a comprehensive strategy that includes workshops, courses, informational campaigns, and the development of a digital platform called UABCiberSegura. This platform provides educational resources, incident reporting tools, protection software, and a threat alert system for the university community. An agile methodology was adopted for its development, utilizing technologies such as JavaScript and the MVC model, along with IT service management frameworks like ITIL. The results show increased participation and awareness regarding safe digital practices. The research concludes that promoting a cybersecurity culture from both educational and technological perspectives is essential to protect institutional digital assets and respond effectively to cyber threats. The project establishes a solid foundation for future digital resilience strategies at UABC.

**Keywords:** cybersecurity, university, digital culture, education, ICTs

## Introducción

La ciberseguridad se ha convertido en una prioridad crítica para las instituciones de educación superior en todo el mundo, debido al incremento constante de los ataques cibernéticos y la



ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



creciente dependencia de las Tecnologías de la Información y la Comunicación (TIC). Diversas universidades de prestigio internacional, como Stanford en Estados Unidos y Cambridge en el Reino Unido, han desarrollado equipos especializados como los CSIRT (Computer Security Incident Response Team) o centros de operaciones de seguridad (SOC), como medida para fortalecer sus capacidades de prevención y respuesta ante incidentes de seguridad (Stanford, 2023; Cambridge, 2023).

En México, el gobierno y diversas instituciones educativas han adoptado marcos normativos como las series ISO y regulaciones nacionales para abordar la problemática. Universidades como la UNAM, la Universidad Autónoma de Chihuahua y la Universidad Veracruzana también han implementado sus propios CSIRT como respuesta proactiva (CSIRT, 2023).

Desde un enfoque teórico, este trabajo se apoya en el modelo socio-técnico y el cubo de McCumber para entender la interacción entre factores tecnológicos, humanos y organizacionales





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



en la construcción de una cultura de ciberseguridad. Asimismo, se consideran estudios como el de Chhetri y Motti (2020), que destacan las principales vulnerabilidades en redes educativas, y el de Morales-Paredes & Medina-Chicaiza (2021), que profundiza en las consecuencias del mal manejo de credenciales.

En el caso de la Universidad Autónoma de Baja California (UABC), la magnitud de su comunidad (69,358 estudiantes y un promedio de 3.6 dispositivos por persona) representa una superficie de ataque amplia. A pesar de acciones puntuales, como charlas con personal de la GESI, no existe una estrategia formal de cultura de ciberseguridad institucional, lo que expone a la universidad a riesgos críticos.

El objetivo de esta investigación es fortalecer la cultura de la ciberseguridad en la UABC mediante la implementación de una estrategia integral basada en acciones educativas, la creación de una plataforma digital institucional, y un sistema informático para la gestión de incidentes de seguridad.

## Método

En consideración del trabajo de investigación, análisis, desarrollo e implementación tecnológica realizado para el presente proyecto, se adoptaron tres metodologías complementarias: Stage-Gate, ITIL y el enfoque de desarrollo ágil de software. La elección de estas metodologías se fundamentó en la revisión de experiencias previas en la gestión de servicios digitales dentro de instituciones educativas, así como en la necesidad de estructurar el proceso de manera ordenada, flexible y centrada en las necesidades reales de los usuarios.

Para lograr una visión integral del entorno universitario, se convocó a un grupo interdisciplinario de participantes con experiencia en áreas clave como tecnologías de la información, comunicación, seguridad informática y docencia. Entre los perfiles involucrados se encuentran el Coordinador Informática y Bibliotecas, personal del área de seguridad informática, responsables de infraestructura TI, personal de desarrollo y soporte técnico. La comunidad universitaria de la UABC está compuesta por 69,358 estudiantes (CGSEGE, 2023), y





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



considerando un promedio de 3.6 dispositivos por persona (Cisco, 2020), se estimó una gran superficie de exposición tecnológica. El muestreo fue no probabilístico por conveniencia, enfocado en individuos con acceso regular a plataformas institucionales. Desde una perspectiva sociodemográfica, los participantes incluyeron estudiantes de entre 18 y 30 años y personal docente y administrativo entre 30 y 55 años, con niveles de educación media superior y superior, y competencias digitales





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870


básicas o intermedias.

La metodología Stage-Gate se utilizó para estructurar las etapas del proyecto tecnológico, estableciendo puntos de control o "gates" que facilitaron la toma de decisiones informadas, permitiendo además evaluar el cumplimiento de objetivos, la viabilidad de las entregas y los riesgos potenciales en cada fase (Rangel, 2017). Paralelamente, se adoptó la metodología ITIL (Axelos, 2019), la cual proporcionó un marco para la gestión eficiente de los servicios de TI relacionados con la plataforma, asegurando disponibilidad, confiabilidad y calidad en cada uno de sus componentes. Estas metodologías fueron complementadas con el enfoque ágil (Beck, 2004; Schwaber & Sutherland, 2020) aplicado al desarrollo de la plataforma UABCiberSegura, lo que permitió integrar entregas incrementales, recibir retroalimentación constante de los usuarios y adaptar funcionalidades de forma flexible y continua.

El desarrollo técnico se realizó utilizando el lenguaje de programación JavaScript, aprovechando su compatibilidad multiplataforma y capacidad de respuesta dinámica (Mozilla Developer Network, s.f.; Flanagan, 2020). La arquitectura implementada se basó en el modelo Cliente/Servidor con el patrón de diseño Modelo-Vista-Controlador (MVC), lo que facilitó la organización del código, su mantenibilidad y la separación de responsabilidades (Coulouris et al., 2011). Entre los materiales utilizados se encuentran herramientas de diseño como Canva para la creación de flyers educativos, documentación oficial del CSIRT México y el Instituto Nacional de Ciberseguridad (INCIBE), así como lineamientos internacionales en materia de ciberseguridad recogidos en la Estrategia Nacional de Ciberseguridad del Gobierno de México (2017) y los marcos operativos del proyecto TheHive (Strange Bee, 2022).

El diseño metodológico general fue de tipo descriptivo, aplicado y no experimental. La investigación se enfocó en resolver una necesidad institucional concreta, integrando componentes educativos, tecnológicos y operativos en una solución funcional. La estructura conceptual se basó en el modelo socio-técnico (Sittig & Singh, 2016), el cual permitió analizar la interacción entre usuarios, procesos y tecnología, y en el modelo del cubo de McCumber (Musich, 2020), el cual proporcionó una perspectiva tridimensional para abordar la seguridad de la información desde las dimensiones de confidencialidad, integridad y disponibilidad.





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



**Descubrimiento:** El proyecto surgió como respuesta a la necesidad institucional de fortalecer la ciberseguridad en la Universidad Autónoma de Baja California (UABC), en un contexto donde las instituciones educativas se han convertido en blanco frecuente de ataques cibernéticos (Check

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870


Point Research, 2023; NCSC, 2023). Para definir el enfoque, se organizaron reuniones colaborativas con personal de tecnologías de información, seguridad informática, docentes y estudiantes. A través de una lluvia de ideas se identificaron necesidades clave como la falta de concienciación, la ausencia de canales para reportar incidentes, y la necesidad de herramientas educativas accesibles (INCIBE, s.f.; Morales, 2014). Estas aportaciones permitieron definir la estructura y funcionalidad inicial de la plataforma UABCiberSegura, orientada a brindar formación, alertas y soporte en ciberseguridad para toda la comunidad universitaria.

**Alcance:** La estrategia contempla el diseño, desarrollo e implementación de una plataforma digital denominada UABCiberSegura, orientada a fortalecer la cultura de la ciberseguridad dentro de la Universidad Autónoma de Baja California (UABC), en concordancia con las recomendaciones de organismos especializados como el INCIBE (s.f.) y la Estrategia Nacional de Ciberseguridad (Gobierno de México, 2017). Esta plataforma integra contenidos educativos, herramientas prácticas, alertas de seguridad y un sistema para el reporte de incidentes, buscando impactar directamente en estudiantes, docentes y personal administrativo (ENISA, 2018; Foro Nacional de Ciberseguridad, 2021).

También se incluye la creación de materiales visuales, campañas de concienciación y recursos de capacitación que promuevan el uso seguro de tecnologías en el entorno académico (IFT, 2018; Romero Galicia, 2018). Además, se plantea la incorporación de un sistema básico para la gestión de incidentes y lineamientos institucionales que fortalezcan el acompañamiento en temas de seguridad digital.

La implementación inicial se realizará en modalidad piloto, con el objetivo de evaluar su efectividad, recopilar retroalimentación de los usuarios y realizar mejoras antes de su expansión progresiva a nivel institucional.

**Concepto:** Previo al desarrollo de la plataforma UABCiberSegura, se realizó una etapa de planeación estratégica en la que se definió el valor que esta solución aportaría a la comunidad universitaria. Se identificaron beneficios como el fortalecimiento de la cultura de la ciberseguridad, la accesibilidad a contenidos formativos, el establecimiento de canales para el





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870


reporte de incidentes y el aumento de la conciencia sobre el uso responsable de tecnologías digitales.

A partir de este análisis, se elaboró un plan de proyecto que integró tareas específicas, tiempos estimados y responsables por área, con base en metodologías como Stage-Gate para la gestión por etapas y ITIL para la alineación de servicios tecnológicos con las necesidades institucionales. Este plan sirvió como guía operativa durante el desarrollo e implementación de la plataforma.

Finalmente, se realizó una revisión de viabilidad para evaluar los recursos disponibles en la universidad y la pertinencia del proyecto. Se concluyó que la propuesta era factible, alineada con los objetivos de transformación digital institucional y con potencial para ser escalada a toda la comunidad universitaria.

**Desarrollo:** Para asegurar la calidad de los entregables y el cumplimiento de los tiempos establecidos, se adoptó una metodología ágil que permitió un desarrollo flexible, iterativo y funcional de la plataforma UABCiberSegura. Esta etapa se enfocó en transformar los objetivos estratégicos definidos en productos tecnológicos concretos, adaptados a las necesidades detectadas durante las fases de diagnóstico y planificación institucional.

Si bien no se aplicó formalmente un marco específico como **Scrum**, se tomaron como referencia algunos de sus principios y prácticas con el fin de estructurar el trabajo por etapas, integrar retroalimentación continua y entregar versiones incrementales del sistema. Esta adaptación del enfoque ágil facilitó el desarrollo gradual de funcionalidades clave y permitió ajustar el rumbo del proyecto conforme surgían nuevas necesidades institucionales (Beck, 2004; Schwaber & Sutherland, 2020).

La autora del proyecto asumió el liderazgo funcional, definiendo la visión general del producto, priorizando las funcionalidades y validando requerimientos con base en las necesidades de los usuarios finales, principalmente estudiantes, docentes y personal administrativo. El área de soporte técnico contribuyó como equipo de desarrollo, integrando conocimientos en programación, diseño web, ciberseguridad y pruebas funcionales. Juntos, trabajaron en la





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870


implementación de módulos como reportes de incidentes, cursos, alertas, noticias, herramientas de protección digital y un canal de asistencia.

Durante el proceso se utilizaron herramientas de gestión digital como tableros de tareas, documentos colaborativos y registros de seguimiento para organizar el flujo de trabajo, dar seguimiento a las decisiones y facilitar la documentación de observaciones.

El desarrollo se organizó en ciclos de trabajo mensuales, inspirados en la estructura de los sprints del enfoque ágil. En cada ciclo se definieron objetivos específicos, se asignaron tareas clave y al concluir se presentaron avances funcionales para su validación y mejora. Este enfoque permitió mantener un proceso adaptable, centrado en la experiencia del usuario y orientado a resultados incrementales.

El proceso de desarrollo se estructuró en torno a cinco eventos principales, tomados como referencia de la metodología Scrum, los cuales fueron adaptados a las condiciones y necesidades del entorno universitario:

1. **Planificación:** Al inicio de cada ciclo de trabajo, se realizó una reunión de planificación para definir las metas del periodo, establecer prioridades y organizar tareas. Estas reuniones permitieron traducir los objetivos generales del proyecto en entregables alcanzables y calendarizados (DoneTonic, 2023).
2. **Ejecución o Iteración:** Durante cada ciclo, el equipo se enfocó en la implementación de las funcionalidades previstas. A lo largo del proceso surgieron cambios, sugerencias y ajustes, los cuales fueron documentados para atenderse dentro del mismo ciclo o en el siguiente. La metodología ágil permitió responder de forma oportuna a estos requerimientos, manteniendo el enfoque en el valor entregado al usuario.
3. **Comunicación continua:** Aunque no se realizaron reuniones diarias formales, se mantuvo una comunicación constante mediante canales digitales, lo cual permitió resolver dudas técnicas, ajustar tareas en curso y coordinar avances. Esta dinámica informal, pero efectiva, resultó clave para sostener la colaboración y la alineación entre los miembros del equipo (Schwaber & Sutherland, 2020).





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870


4. **Revisión:** Al finalizar cada ciclo, se realizó una presentación de los avances y entregables desarrollados. Se validaron módulos como el sistema de alertas, la sección de cursos, reportes de incidentes y herramientas de ciberseguridad. Las observaciones recibidas se utilizaron como base para retroalimentar el siguiente ciclo de trabajo (Martínez Sánchez, 2025).
5. **Retrospectiva:** Luego de cada revisión, se realizó una reflexión sobre los aciertos, desafíos y oportunidades de mejora del ciclo. Se evaluaron aspectos como la claridad de los objetivos, la carga de trabajo y la comunicación entre roles, buscando siempre optimizar el proceso y fortalecer la colaboración del equipo.

El desarrollo de la plataforma se extendió por un periodo aproximado de ocho meses, distribuidos en ocho ciclos de trabajo, cada uno con entregables específicos e incrementales. Esta estructura permitió construir una solución tecnológica sólida, alineada con los principios de ciberseguridad, accesibilidad y usabilidad, y adaptada al contexto institucional de la Universidad Autónoma de Baja California.

**Pruebas:** Finalizada cada etapa de desarrollo, se realizaron pruebas funcionales internas con el objetivo de validar el correcto funcionamiento de cada uno de los módulos implementados en la plataforma UABCiberSegura. Estas pruebas se llevaron a cabo de forma iterativa al término de cada ciclo de trabajo, permitiendo detectar errores, evaluar la experiencia de usuario y realizar ajustes oportunos antes de integrar nuevas funcionalidades.

Las pruebas incluyeron la verificación de la interfaz de usuario, la funcionalidad de formularios, la carga de contenidos educativos, la visualización de alertas, la navegación entre secciones, y el funcionamiento del módulo de reportes. También se realizaron validaciones cruzadas sobre la conexión entre componentes, la consistencia visual, el acceso multiplataforma y el rendimiento general.

Los escenarios de prueba fueron diseñados tomando en cuenta los casos de uso más comunes de los usuarios finales (estudiantes, docentes y personal administrativo). Se utilizaron criterios de aceptación definidos durante la fase de planificación de cada ciclo, alineados con los





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870


objetivos del proyecto. Las observaciones obtenidas durante las pruebas fueron documentadas y sirvieron de insumo para la mejora continua dentro de los siguientes ciclos de desarrollo (Beck, 2004).

El enfoque ágil permitió que los procesos de validación no se limitaran a una fase única al final del desarrollo, sino que se integraran como parte natural de cada iteración. Este enfoque incremental facilitó la identificación temprana de errores y aseguró la calidad de los entregables a lo largo del proceso.

**Lanzamiento:** Una vez finalizadas las pruebas y obtenida la validación funcional de los módulos principales, se procedió al lanzamiento de la versión piloto de la plataforma UABCiberSegura. Esta versión se presentó a un grupo reducido de usuarios dentro de la comunidad universitaria, con el fin de recopilar retroalimentación real en un entorno controlado.

El lanzamiento se acompañó de una estrategia de comunicación institucional que incluyó la





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



difusión a través de canales internos de UABC como el correo institucional y redes sociales oficiales. Se diseñaron materiales informativos (flyers y publicaciones digitales) para guiar a los usuarios en el uso de la plataforma y promover la participación activa en la adopción de prácticas seguras en el entorno digital.

Durante esta fase, se habilitó también el canal de soporte y asistencia, permitiendo a los usuarios registrar comentarios, dudas o sugerencias relacionadas con el funcionamiento del sistema. Esta interacción directa con los usuarios permitió detectar oportunidades de mejora y ajustar ciertos elementos visuales y de navegación antes de su futura expansión a mayor escala.

## Resultados

Como resultado de este proyecto, se diseñó, desarrolló e implementó la plataforma web institucional UABCiberSegura, con el objetivo de fortalecer la cultura de la ciberseguridad en la Universidad Autónoma de Baja California. Esta solución tecnológica agrupa recursos educativos, módulos de atención, herramientas digitales y contenidos de alerta diseñados para informar, prevenir y acompañar a la comunidad universitaria ante incidentes de seguridad digital.

La plataforma inicia con una pantalla de bienvenida en la que se muestran las secciones disponibles para los usuarios. En la *Figura 1* se aprecia la interfaz principal, que da acceso a todos los módulos del sistema.





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



**Figura 1.**

*UABCiberSegura - Interfaz principal*


*Nota.* Imagen obtenida de la *plataforma UABCiberSegura* por Luz Macias, 2025, (https://cibersegura.uabc.mx/)

Una de las secciones más relevantes es el módulo de Reporte de Incidentes, mostrado en la Figura 2. Este apartado permite a los usuarios registrar eventos sospechosos o ataques cibernéticos que afecten sus cuentas institucionales, adjuntando detalles clave como tipo de





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



incidente, fecha, descripción y evidencia.

**Figura 2.**

*Reporte de incidente*


*Nota.* Imagen obtenida de la *plataforma UABCiberSegura* por Luz Macias, 2025, (https://cibersegura.uabc.mx/)

Pantalla de reporte de incidentes de seguridad digital dentro de la plataforma UABCiberSegura. En esta sección, los usuarios pueden registrar eventos sospechosos o ataques cibernéticos, proporcionando detalles clave para su análisis y seguimiento.En la figura 2 se muestra





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

el formulario utilizado para este proceso.

Otra funcionalidad clave es la sección de Flyers Informativos (Figura 3), en donde se presentan materiales gráficos con recomendaciones sobre contraseñas, ingeniería social, phishing, y buenas prácticas digitales. Estos recursos están diseñados con lenguaje accesible y están dirigidos a toda la comunidad universitaria.

**Figura 3.**

*Sección de Flyers informativos*


*Nota.* Imagen obtenida de la *plataforma UABCiberSegura* por Luz Macias, 2025,

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



(https://cibersegura.uabc.mx/)

En el apartado de Herramientas de Seguridad (Figura 4) se ofrecen accesos a software de protección digital como administradores de contraseñas, antivirus recomendados, y extensiones para la navegación segura. Esta sección incluye enlaces verificados para su descarga.

**Figura 4.**

*Herramientas de Seguridad*


*Nota.* Imagen obtenida de la *plataforma UABCiberSegura* por Luz Macias, 2025,





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

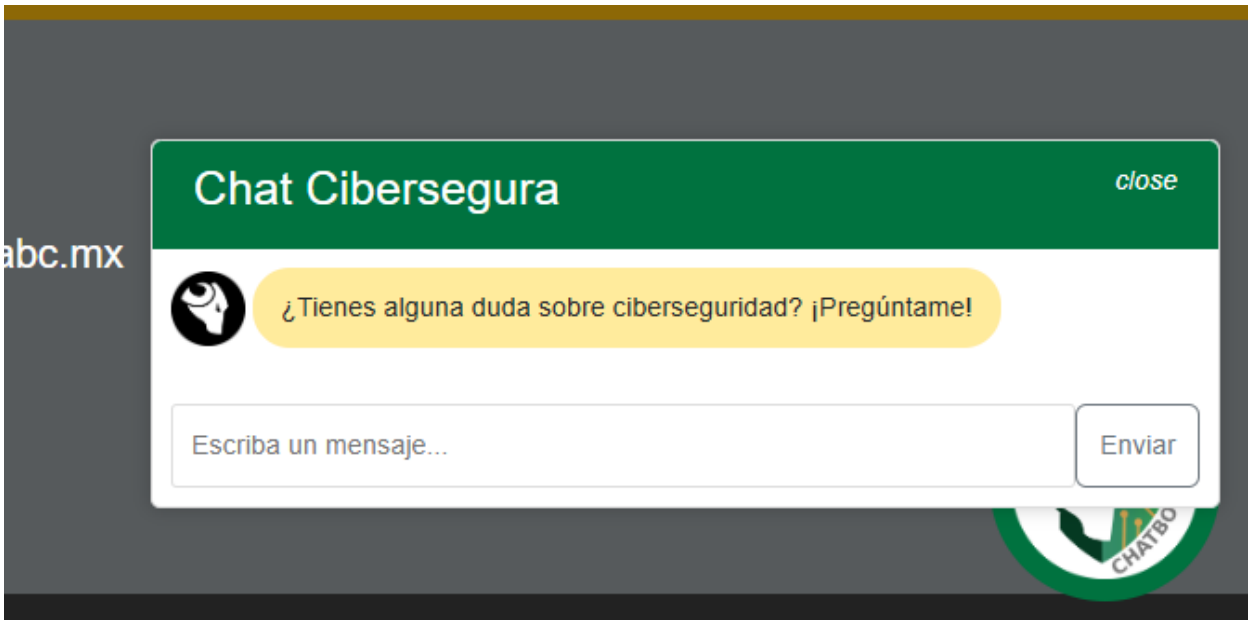
Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870


(https://cibersegura.uabc.mx/)

La plataforma incluye también un chat de asistencia en tiempo real (Figura 5), funcionalidad que permite atender dudas relacionadas con seguridad digital. Este canal fue diseñado para resolver inquietudes sobre incidentes, recuperación de cuentas, o uso de herramientas institucionales.

**Figura 5.**

*Interfaz del chat de asistencia*




*Nota.* Imagen obtenida de la *plataforma UABCiberSegura* por Luz Macias, 2025, (https://cibersegura.uabc.mx/)

En cuanto a la formación continua, la sección de CiberCursos (Figura 6) contiene materiales educativos clasificados por nivel: básico, intermedio y avanzado. Los contenidos se componen de cápsulas informativas, actividades interactivas y evaluaciones diagnósticas.





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



**Figura 6.**

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



*CiberCursos*






ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

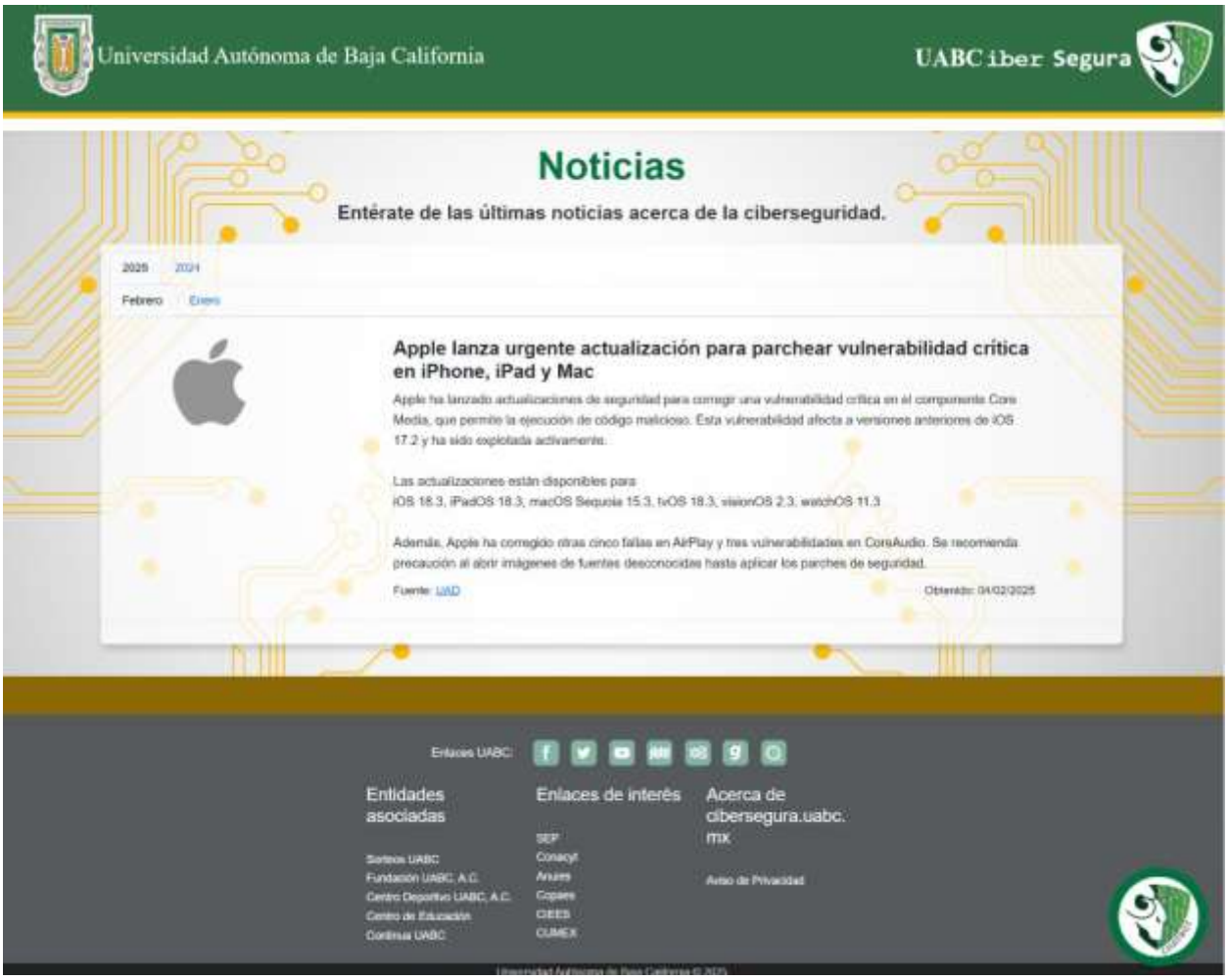


*Nota.* Imagen obtenida de la *plataforma UABCiberSegura* por Luz Macias, 2025, (https://cibersegura.uabc.mx/)

La sección de Noticias (Figura 7) recopila información actualizada sobre vulnerabilidades recientes, recomendaciones de organismos especializados y campañas institucionales. Su objetivo es mantener informada a la comunidad sobre el panorama cambiante de la ciberseguridad.

**Figura 7.**

*Sección de noticias en ciberseguridad*



Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



*Nota.* Imagen obtenida de la *plataforma UABCiberSegura* por Luz Macias, 2025, (https://cibersegura.uabc.mx/)

En la sección de Descargas Seguras (Figura 8), los usuarios pueden acceder a programas verificados para la protección de sus dispositivos. Esta área está organizada por categoría de herramienta y sistema operativo, con enlaces auditados.

**Figura 8.**

*Pantalla de descargas verificadas*






ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



*Nota.* Imagen obtenida de la *plataforma UABCiberSegura* por Luz Macias, 2025, (https://cibersegura.uabc.mx/)

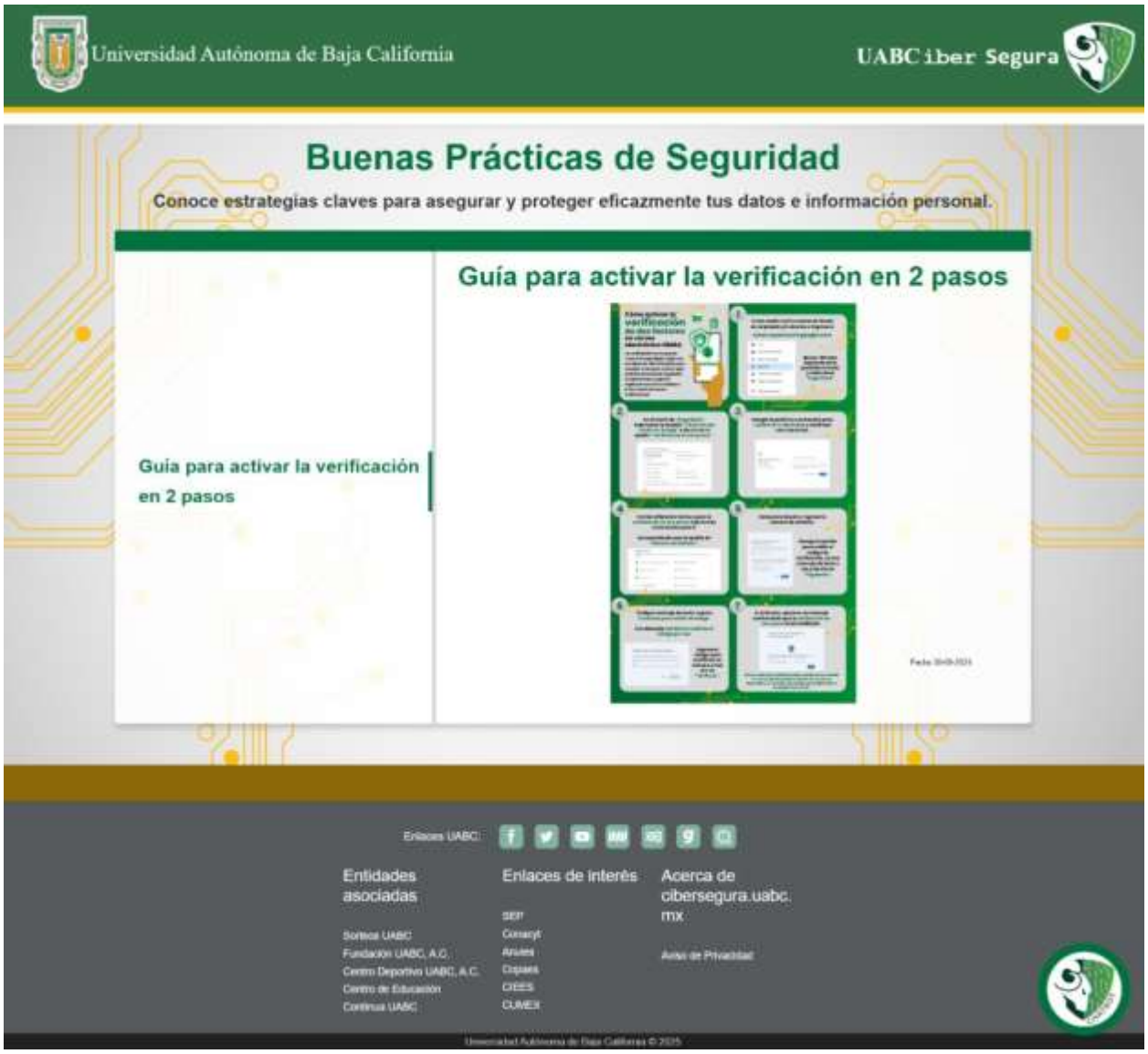
El módulo de Buenas Prácticas (Figura 9) recopila guías, checklists y recomendaciones para el resguardo de contraseñas, gestión de identidades y uso de redes públicas. Esta sección busca fomentar hábitos digitales responsables en el día a día universitario.

**Figura 9.**

*Guías de buenas prácticas digitales*

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870






*Nota.* Imagen obtenida de la *plataforma UABCiberSegura* por Luz Macias, 2025, (https://cibersegura.uabc.mx/)

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



Finalmente, en la sección de Alertas de Amenazas (Figura 10) se despliegan advertencias sobre campañas de phishing, malware en circulación, suplantación de identidad y otras vulnerabilidades emergentes. Cada alerta incluye medidas preventivas concretas y rutas de atención institucional.

**Figura 10.**

*Sistema de alertas emergentes*

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



*Nota.* Imagen obtenida de la *plataforma UABCiberSegura* por Luz Macias, 2025, (https://cibersegura.uabc.mx/)





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



## Discusión

El desarrollo e implementación de la plataforma UABCiberSegura evidencia la importancia de adoptar un enfoque integral en la promoción de la cultura de la ciberseguridad dentro del entorno universitario. A lo largo del proyecto, fue posible identificar que las amenazas digitales no solo representan un riesgo técnico, sino también una oportunidad para fortalecer competencias digitales en la comunidad académica, administrativa y estudiantil.

Diversas investigaciones y organismos especializados en ciberseguridad han señalado que el factor humano es una de las principales vulnerabilidades en la gestión de la seguridad digital (INCIBE, s.f.; Chhetri & Motti, 2020). En este sentido, la plataforma desarrollada actúa como un recurso educativo que busca minimizar esos riesgos a través de la concienciación continua, el acceso a contenidos formativos y el acompañamiento directo en la gestión de incidentes.

Los resultados obtenidos concuerdan con experiencias previas documentadas por instituciones que han incorporado estrategias socio-técnicas para fortalecer su resiliencia digital (Leiva, 2015; Morales, 2014). Al igual que en esos casos, en la UABC se comprobó que una estrategia basada en formación, participación activa y herramientas tecnológicas accesibles puede contribuir significativamente a mejorar las prácticas de seguridad en el uso cotidiano de las tecnologías de la información y la comunicación (TIC).

Otro hallazgo relevante fue el valor de adoptar metodologías ágiles durante el proceso de desarrollo, lo cual permitió ajustes rápidos, una validación constante por parte de los usuarios, y una mayor alineación entre los entregables y las necesidades reales del entorno universitario (Beck, 2004; Schwaber & Sutherland, 2020). La adaptabilidad del enfoque también resultó fundamental frente a los cambios de prioridades institucionales o solicitudes emergentes.

La experiencia de este proyecto sugiere que, más allá de la solución tecnológica en sí, es necesario establecer mecanismos permanentes de actualización, seguimiento y evaluación que permitan sostener los avances logrados y anticipar nuevas amenazas digitales, especialmente en contextos como el universitario, donde la diversidad de perfiles y niveles de competencia digital es alta.





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



## Conclusiones

El proyecto Cultura de la Ciberseguridad en UABC permitió desarrollar una estrategia institucional centrada en la prevención, educación y atención de incidentes digitales mediante la plataforma UABCiberSegura, logrando así fortalecer la resiliencia digital de la comunidad universitaria.

Se concluye que la implementación de acciones formativas, como cursos, campañas y guías, junto con herramientas digitales accesibles, puede tener un impacto positivo en la adopción de buenas prácticas de seguridad informática. La plataforma consolidó en un solo espacio recursos educativos, canales de reporte y módulos de atención, facilitando la gestión de incidentes y promoviendo una mayor conciencia institucional sobre la importancia de la ciberseguridad.

El enfoque metodológico ágil adoptado para el desarrollo de la plataforma fue clave para lograr entregas incrementales, mejorar funcionalidades con base en la retroalimentación y mantener alineado el proyecto a las necesidades institucionales.

Finalmente, se reconoce la necesidad de continuar ampliando la estrategia de ciberseguridad en la universidad, integrando indicadores de seguimiento, simulacros regulares (como los de phishing), y alianzas con organismos especializados para asegurar la sostenibilidad de la cultura de la ciberseguridad en el largo plazo.





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870



## Referencias

Axelos. (2019). ITIL Foundation: ITIL 4 Edition. TSO.

Beck, K. (2004). Extreme Programming Explained: Embrace Change. Addison-Wesley. Cambridge.

(2023). Cyber Security Centre. https://www.cam.ac.uk/

Check Point Research. (2023). Threat Intelligence Reports. https://research.checkpoint.com/

Chhetri, N., & Motti, V. G. (2020). Vulnerabilities in educational networks: A study of cyber threats in academia. Journal of Cybersecurity and Education, 5(2), 45–62.

Cisco. (2020). Annual Internet Report (2018–2023). Cisco Systems.

CSIRT México. (2023). Reportes de Incidentes y Alertas. https://www.csirt.gob.mx/

Coulouris, G., Dollimore, J., Kindberg, T., & Blair, G. (2011). Sistemas distribuidos: Conceptos y diseño. Addison-Wesley.

DoneTonic. (2023, 26 septiembre). ¿Qué es el Sprint Planning? https://donetonic.com/es/que-es-el-sprint-planning/

ENISA. (2018). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. https://www.enisa.europa.eu/

Flanagan, D. (2020). JavaScript: The Definitive Guide. O'Reilly Media.

Foro Nacional de Ciberseguridad. (2021). Estrategias nacionales y desafíos en ciberseguridad.

Gobierno de México. (2017). Estrategia Nacional de Ciberseguridad. Secretaría de

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

Comunicaciones y Transportes.

INCIBE. (s.f.). Instituto Nacional de Ciberseguridad. https://www.incibe.es/

IFT. (2018). Recomendaciones para el uso seguro de internet. Instituto Federal de Telecomunicaciones.

Leiva, J. (2015). Cultura de la Ciberseguridad en entornos educativos. Revista Iberoamericana de Tecnología Educativa, 10(1), 15–22.

Martínez Sánchez, Á. L. (2025, 25 marzo). Lo que necesitas saber sobre la Sprint Review para mejorar cada proyecto ágil. Ineaf. https://www.ineaf.es/tribuna/sprint-review-en-scrum/

Morales, D. (2014). Gestión de riesgos en instituciones educativas frente a ciberamenazas. Editorial Académica Española.

Mozilla Developer Network. (s.f.). JavaScript Guide. https://developer.mozilla.org/

Musich, M. (2020). Information Security Foundations: The McCumber Cube Model. Infosec Institute.

NCSC. (2023). UK National Cyber Security Centre Reports. https://www.ncsc.gov.uk/

Rangel, R. (2017, 11 julio). Utiliza la metodología Stage-Gate para crear innovaciones. IDESAA.

https://idesaa.edu.mx/blog/utiliza-la-metodologia-stage-gate-para-crear-innovaciones/

Romero Galicia, A. (2018). Seguridad digital en el entorno universitario. Revista Mexicana de Educación Superior, 7(2), 35–50.





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.

Año 18 / Núm. 43 / - Enero - junio 25
Revista de Investigación Académica sin Frontera
ISSN 2007-8870

Schwaber, K., & Sutherland, J. (2020). Guía Scrum: La guía definitiva para Scrum. Scrum.org.

Sittig, D. F., & Singh, H. (2016). A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. Journal of the American Medical Informatics Association, 23(5), 1073–1079.

Stanford. (2023). Information Security Office. https://uit.stanford.edu/security Strange Bee. (2022). TheHive Project. https://thehive-project.org/





ISSN 2007-8870 RIASF Universidad de Sonora
Facultad Interdisciplinaria de Ciencias Económicas Administrativas
Departamento de Ciencias Económico Administrativas-Campus Navojoa.