DESARROLLO DE UN PROTOTIPO DE EXTENSIÓN DE NAVEGADOR PARA LA PREVENCIÓN DE FRAUDE ACADÉMICO EN EVALUACIONES EN LÍNEA DENTRO DEL AULA

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

ANDRÉS CAMILO VÁSQUEZ RODRÍGUEZ

1003823278

ACAMILOVASQUEZ@UCUNDINAMARCA.EDU.CO

561221184

JUAN SEBASTIÁN ZABALA BENÍTEZ

JSEBASTIANZABALA@UCUNDINAMARCA.EDU.CO

561221289

FABIAN RODRIGO GUTIERREZ AREVALO

UNIVERSIDAD DE CUNDINAMARCA EXTENSIÓN CHÍA

FACULTAD DE INGENIERÍA

PROGRAMA INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

2025

DESARROLLO DE UN PROTOTIPO DE EXTENSIÓN DE NAVEGADOR PARA LA PREVENCIÓN DE FRAUDE ACADÉMICO EN EVALUACIONES EN LÍNEA

TRABAJO DE GRADO PARA OPTAR EL TÍTULO DE INGENIERO DE SISTEMAS Y COMPUTACIÓN

ANDRÉS CAMILO VÁSQUEZ RODRÍGUEZ

1003823278

ACAMILOVASQUEZ@UCUNDINAMARCA.EDU.CO

561221184

JUAN SEBASTIÁN ZABALA BENÍTEZ

JSEBASTIANZABALA@UCUNDINAMARCA.EDU.CO

561221289

FABIAN RODRIGO GUTIERREZ AREVALO

UNIVERSIDAD DE CUNDINAMARCA EXTENSIÓN CHÍA

FACULTAD DE INGENIERÍA

PROGRAMA INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

2025

AGRADECIMIENTOS

En primer lugar, agradecer a Dios por haber permitido llegar hasta esta etapa, a las familias que fueron el apoyo en el diario vivir, que comprendieron nuestros esfuerzos y dedicación en la meta que cultivamos en nuestro día a día, al semillero de investigación en seguridad informática y redes por el apoyo y orientación brindados a lo largo del desarrollo de este proyecto. Un agradecimiento especial al tutor de este proyecto, el ingeniero Fabian Rodrigo Gutiérrez Arévalo, que gracias a su empeño, dedicación y buena disposición para con nosotros permitió culminar esta etapa. Finalmente, agradecer a nuestros docentes, compañeros y a la universidad de Cundinamarca por sus valiosas contribuciones y sugerencias que enriquecieron el presente trabajo.

DEDICATORIA

A mis padres Rubén y Mary que con su ejemplo, amor y paciencia me han apoyado durante toda mi formación académica y fueron ellos mi impulso para culminar con éxito esta etapa de mi vida; también a mi hermano quien me ha brindado siempre su cariño.

A mis padres, Juan y Rosa, y a mi hermano, por su apoyo incondicional y la compañía en mi proceso académico. Gracias a ellos me dieron la fuerza y el impulso necesario para culminar con éxito esta etapa de mi vida, un logro reconfortante que les debo en gran parte a ellos, sobre todo. A mi abuelita, aunque ya no está físicamente conmigo, me brindó su apoyo mientras estuvo en vida. Sé que, desde donde esté, continúa acompañándome y guiándome.

RESUMEN

Este trabajo presenta el diseño y desarrollo de un prototipo de extensión para navegador web orientado a prevenir el fraude académico durante evaluaciones en línea. En el contexto actual de la educación virtual, mantener la integridad académica se ha convertido en un desafío importante para las instituciones educativas. El prototipo integra funciones de monitoreo de cambios de pestaña, detección de acciones de copiar y pegar y restricción de navegación durante los exámenes. Se utilizó una metodología de desarrollo incremental y pruebas piloto con estudiantes de pregrado, permitiendo crear una versión básica funcional capaz de supervisar actividades potencialmente fraudulentas sin afectar de manera significativa la privacidad de los

estudiantes. Las pruebas iniciales en un entorno controlado muestran resultados prometedores en la detección de conductas sospechosas durante evaluaciones simuladas. A partir de esta primera versión, el trabajo sienta las bases para el desarrollo futuro de una solución más completa, que podría incluir en el futuro funcionalidades adicionales como verificación de identidad y análisis de comportamiento, contribuyendo a la integridad académica en entornos virtuales.

Palabras clave

e-learning; evaluación en línea; extensión de navegador; fraude académico; integridad académica; prevención.

ABSTRACT

This work presents the design and development of a prototype web browser extension aimed at preventing academic fraud during online assessments. In the current context of virtual education, maintaining academic integrity has become a major challenge for educational institutions. The prototype integrates functions for monitoring tab changes, detecting copy and paste actions, and restricting navigation during exams. An incremental development methodology and pilot testing with undergraduate students were used, allowing for the creation of a basic functional version capable of monitoring potentially fraudulent activities without significantly affecting student privacy. Initial testing in a controlled environment shows promising results in detecting suspicious behavior during simulated assessments. Based on this first version, the work lays the foundation for the future development of a more comprehensive solution, which could include additional features such as identity verification and behavior analysis, contributing to academic integrity in virtual environments.

Keywords

academic integrity; browser extension; e-learning; fraud prevention; online assessment.

TABLA DE CONTENIDO

AGRADECIMIENTOS....3
DEDICATORIA....3
RESUMEN....3
Palabras clave....4
ABSTRACT....4
Keywords....4
TABLA DE CONTENIDO....5
LISTA DE FIGURAS....8
LISTA DE TABLAS....9
CAPÍTULO 1....9
INTRODUCCIÓN....9
1. PROBLEMA....10
1.1 Planteamiento del problema....10
1.2 Formulación del problema....11
2. OBJETIVOS....11
2.1 Objetivo general....11
2.2 Objetivos específicos....12
3. ALCANCES Y LIMITACIONES....12
3.1 Alcances....12
3.2 Limitaciones....12
4. JUSTIFICACIÓN....13
5. LÍNEAS DE INVESTIGACIÓN....14
CAPÍTULO 2....15
6. MARCO TEÓRICO....15
6.1 Marco referencial....15
6.1.1 Integridad académica en entornos virtuales....15
6.1.2 Métodos comunes de fraude académico en línea....16
6.1.3 Tecnología de supervisión de exámenes....17
6.1.4 Marco legal y ético....18
6.1.5 Revisión de casos reales....18
6.1.6 Antecedentes Nacionales e internacionales....19
6.1.6.1 Antecedentes nacionales....19
6.1.6.2 Antecedentes Internacionales....20
6.2 Marco conceptual....21
6.2.1 Fraude académico....21
6.2.2 Integridad académica....21
6.2.3 Proctoring....21
6.2.4 Extensiones de navegador....22
6.2.5 Privacidad y protección de datos....22
6.3 Marco ingenieril....22

6.3.1 Arquitectura y metodología....22
6.3.2 Herramientas y modelos aplicados....23
6.3.3 Estándares de buenas prácticas....23
6.3.4 Compromiso social e innovación....24
CAPÍTULO 3....24
7. METODOLOGÍA....24
7.1 Enfoque metodológico....25
7.2 Fases del proceso de desarrollo....25
7.2.1 Análisis de requisitos....25
7.2.2 Historias de usuario....25
7.2.3 Definición de Done(DoD)....26
7.2.4 Product backlog....27
7.2.5 Priorización y asignación de sprints....28
7.2.6 Diseño técnico....28
7.2.7 Desarrollo del prototipo....29
7.2.8 Pruebas piloto y validación....29
7.2.9 Análisis de resultados y documentación....29
7.3 Población y muestra....29
7.4 Técnicas y muestra....29
7.5 Procedimientos....30
7.6 Análisis de datos....30
7.7 Alineación con los objetivos....30
7.8 Fases del ciclo de vida del desarrollo....30
7.8.1 Análisis....31
7.8.2 Planeación....31
7.8.3 Desarrollo....31
7.8.4 Despliegue y validación....31
8. DESARROLLO DEL PROYECTO....31
8.1 Prototipo y arquitectura del sistema....32
8.1.2 Descripción del prototipo....32
8.1.2 Arquitectura....33
8.1.2.1 Arquitectura de componentes del sistema....34
8.1.2.2 Arquitectura logica detallada....36
8.1.3 Artefactos de diseño....37
Actores del sistema....37
8.1.3.1 Diagramas de flujo de procesos....37
8.1.4 Casos de uso....41
8.1.4.1 Activar extensión....42
8.1.4.2 Monitorear cambio de pestaña....42
8.1.4.2 Bloquear copiar/pegar....42
8.1.4.3 Restringir navegación externa....42

8.1.4.5 Generar reportes de eventos....42
8.1.4.6 Consultar reportes....42
Diagrama UML....42
8.2 Implementación del sistema....43
8.3 Pruebas pilotos y validación....44
8.3.1 Evidencia de funcionalidad mediante capturas....44
8.3.2 Pruebas piloto y validación....47
8.3.3 Procedimiento de prueba....48
8.4 Resultados encuestas y análisis de las respuestas....49
8.4.1 Resultados de la encuesta a estudiantes....49
8.4.2 Resultados obtenidos....49
8.4.3 Resultados de la encuesta a estudiantes....50
8.4.3.1 Exámenes virtuales....50
8.4.3.2 Conocimiento sobre el fraude académico....51
8.4.3.3 Métodos de fraude....51
8.4.3.4 Uso de herramientas para evitar el fraude....51
8.4.3.5 Extensiones de navegador....52
8.4.3.6 Preocupación sobre privacidad y seguridad....53
8.4.3.7 Aceptación de una extensión nueva....54
8.5 Resultados de pruebas de la extensión....54
8.5.1 Facilidad de uso....54
8.5.2 Efectividad....54
8.5.3 Experiencia con la extensión....55
8.5.4 Entrevista sobre la prueba....55
8.5.5 Análisis de los reportes de cada usuario....56
8.5.6 Evidencias....57
8.6 Discusión....59
8.6.1 Análisis de resultados durante el desarrollo y la prueba piloto....59
8.6.2 Comparación con soluciones existentes....61
8.6.3 Limitaciones del prototipo....63
8.6.4 Hoja de ruta para versiones futuras....63
8.7 Conclusión del desarrollo....64
CAPÍTULO 4....64
1. CONSIDERACIONES DE PRIVACIDAD Y SEGURIDAD....64
1.2 Declaración de privacidad....65
1.3 Medidas de seguridad implementadas....65
1.4 Cumplimiento normativo....65
2. CONCLUSIONES....66
2.2 Logros alcanzados....66
3. RECOMENDACIONES....66
3.1 Para desarrolladores....66

3.2 Para instituciones educativas..... 67
3.3 Para investigadores..... 67
3.4 Para el diseño de evaluaciones..... 67
3.5 Consideraciones finales..... 67
4. PROYECCIONES..... 69
REFERENCIAS BIBLIOGRÁFICAS..... 69
ANEXOS..... 75
Anexo 1. Instrumento de encuesta aplicado a estudiantes..... 75
Anexo 2. Resultados de las encuestas..... 76
Anexo 3. Extractos del código fuente de la extensión..... 78
Anexo 4. Manual para docentes..... 80
Anexo 5. Manual para estudiantes..... 81
Anexo 6. Guia de instalacion técnica (para administradores de sistemas)..... 82

LISTA DE FIGURAS

Figura 1..... 33
Flujo entre la extensión, el usuario y en este caso Moodle..... 33
Figura 2..... 33
Flujo de funcionamiento de la extensión..... 33
Figura 3..... 34
Arquitectura de componentes de ProctorGuard..... 34
Figura 4..... 38
Flujo de activación de la extensión..... 38
Figura 5..... 39
Flujo de detección de evento sospechoso..... 39
Figura 6..... 40
Flujo de generación y consulta de reportes..... 40
Flujo de Manejo de Errores y Excepciones..... 41
Figura 7..... 42
Modelo casos de uso..... 42
Figura 8..... 45
Pantallazo en Moodle de la extensión..... 45
Figura 9..... 45
Pantallazo en Moodle de la extensión..... 45
Figura 10..... 46
Pantallazo en Moodle de la extensión..... 46
Figura 11..... 47
Pantallazo en Moodle de la extensión..... 47
Figura 12..... 50

Experiencia y percepción....50
Figura 13....52
Uso y conocimiento de extensiones....52
Figura 14....53
Supervisión y confianza....53
Figura 15....55
Resultados percepción de usuarios....55
Figura 16....57
Diagramas de los reportes de fraude....57
Figura 17....57
Evidencia extensión en uso....57
Figura 18....58
Evidencia extensión en uso....58
Figura 19....58
Evidencia extensión en uso....58
Figura 20....59
Evidencia extensión en uso....59
Figura 21....59
Evidencia extensión en uso....59

LISTA DE TABLAS

Tabla 1....16
Métodos comunes de fraude académico en línea....16
Tabla 2....26
Historias de usuario del prototipo ProctorGuard....26
Tabla 3....27
Product backlog....27
Tabla 4....36
Descripción detallada de capas de arquitectura....36
Tabla 5....49
Resultados esperados....49
Tabla 6....61
Comparación entre ProctorGuard con herramientas anti fraude....61
Tabla 7....77
Resumen de respuestas....77
Tabla 8....82
Solución de problemas....82

CAPÍTULO 1

INTRODUCCIÓN

La evolución de la educación en los últimos años ha estado marcada por la incorporación de las tecnologías de la información y la comunicación. Este proceso se intensificó durante la pandemia del COVID-19, donde las instituciones educativas debieron migrar de forma rápida hacia modalidades virtuales. Esta modalidad amplió el acceso y flexibiliza procesos de enseñanza pero también emergieron nuevos retos relacionados con la evaluación académica y la garantía de la integridad en los procesos de aprendizaje.

En ese contexto el fraude académico en entornos virtuales se ha convertido en una de las principales preocupaciones de las instituciones. La facilidad de acceso a la información en línea junto con el uso de herramientas de inteligencia artificial, han incrementado los intentos de fraude académico, lo cual pone en riesgo la validez de los procesos educativos y la formación ética de los estudiantes.

Ante esta problemática surge la necesidad de desarrollar herramientas tecnológicas que ayuden a fortalecer la confianza en las evaluaciones en línea. Entre las soluciones actuales se encuentran el proctoring basado en cámaras y sistemas de bloqueo de navegadores que ofrecen cierto nivel de seguridad pero que muchas veces resultan intrusivos y generan preocupación en cuanto a privacidad de datos.

Por ello, este proyecto propone el diseño y desarrollo de un prototipo de extensión de navegador orientado a prevenir conductas fraudulentas durante los exámenes en línea, mediante la detección de acciones sospechosas y la restricción de comportamientos que comprometan la integridad académica.

El desarrollo de este prototipo se realizó aplicando una metodología incremental, validada con pruebas piloto que permiten comprobar su viabilidad y efectividad. Con el proyecto presentado se busca aportar una alternativa innovadora, menos invasiva y más aceptable para estudiantes y docentes, contribuyendo así al fortalecimiento de la educación con calidad y transparencia.

1. PROBLEMA

1.1 Planteamiento del problema

La pandemia del COVID-19 irrumpió en las vidas de las personas, forzando una transformación en la educación. De un día para otro, las aulas se vaciaron y las escuelas y universidades se vieron obligadas a dar un giro masivo hacia los exámenes y estudios a distancia. Este cambio, si bien hizo la educación más accesible, también desencadenó una serie de presiones emocionales, sociales y económicas que han cambiado la dinámica de enseñanza y aprendizaje (Melo-Becerra et al., 2021).

En este contexto de educación virtual, el fraude académico se ha consolidado como uno de los principales desafíos éticos y tecnológicos. La facilidad de acceso a información, el uso de dispositivos múltiples y las nuevas herramientas de inteligencia artificial (IA) generativa, como Chat GPT o Copilot, han facilitado la copia, suplantación y colaboración no autorizada durante los exámenes (Guerrero-Dib, Portales & Heredia-Escorza, 2020; Bulut & Beiting-Parrish, 2024). Estudios realizados por International Center for Academic Integrity (ICAI) respaldan esta preocupación, evidenciando que el 64% de los estudiantes reconocen haber cometido algún tipo de trampa, siendo esta práctica más frecuente en entornos en línea que en evaluaciones presenciales (McCabe et al., 2012).

Aunque existen varias herramientas como los sistemas de proctoring (supervisión remota) o los navegadores bloqueados, estas suelen ser intrusivas, costosas y generan desconfianza por su impacto en la privacidad del estudiante (Terpstra et al., 2025). Además la integración de herramientas robustas de detección de IA en plataformas educativas como Moodle es un proceso complicado (Saha & Mondal, 2024). Por ello, el vacío identificado se centra en la falta de herramientas ligeras y adaptables que puedan integrarse a entornos educativos existentes y que midan su impacto no solo en la reducción del fraude sino también en la mejora de la confianza docente en el proceso de evaluación digital.

1.2 Formulación del problema

¿Cómo puede una extensión de navegador contribuir a prevenir el fraude académico en evaluaciones en línea dentro del aula y aumentar la confianza de los docentes en la integridad del proceso evaluativo, mediante un prototipo validado en entorno controlado?

2. OBJETIVOS

2.1 Objetivo general

Validar la viabilidad de un prototipo de extensión de navegador orientado a prevenir el fraude académico en evaluaciones en línea dentro del aula y fortalecer la confianza docente en la integridad del proceso evaluativo.

2.2 Objetivos específicos

- Analizar las principales prácticas de fraude académico en entornos virtuales y las limitaciones de las tecnologías actuales de supervisión.
- Diseñar la arquitectura técnica y funcional de una extensión de navegador enfocada en la detección y prevención de comportamientos fraudulentos.
- Desarrollar un prototipo funcional basado en metodologías de ingeniería de software y estándares internacionales.
- Implementar pruebas piloto controladas para medir la efectividad del prototipo y su impacto en la percepción de confianza.
- Evaluar los resultados obtenidos y definir una hoja de ruta para la evolución del sistema hacia una versión institucional escalable.

3. ALCANCES Y LIMITACIONES

3.1 Alcances

El proyecto comprende el diseño, desarrollo y validación de un prototipo funcional inicial de extensión para el navegador Google Chrome capaz de detectar y restringir acciones como el cambio de pestaña y el uso de copiar y pegar durante exámenes en línea.

Las pruebas se realizan en un entorno controlado con participación de estudiantes y docentes evaluando su efectividad técnica y percepción de uso.

El trabajo establece los fundamentos conceptuales, técnicos y metodológicos para futuras versiones de la herramienta.

3.2 Limitaciones

El prototipo desarrollado presenta unas limitaciones debido a que la versión inicial es compatible con el navegador de Google Chrome debido a la dependencia de las WebExtensions APIs y del estándar Manifest V3, sin abordar compatibilidad con otros navegadores esta limitación tecnológica restringe la interoperabilidad de la solución y condiciona su adopción en entornos educativos con políticas de software heterogéneas, en segundo lugar el desarrollo inicial se hace con funcionalidades básicas correspondiente a la versión base del sistema , con la detección de cambios de ésta , restricción en copiar/pegar y bloqueo de navegación externa.

Respecto a la validación funcional se implementa en un entorno controlado con un grupo reducido, por lo cual estos resultados son interpretados como una evidencia inicial de viabilidad en contextos institucionales más amplios. La falta de replicación en escenarios reales con diversidad de plataformas y usuarios limita la robustez de las conclusiones y destaca la necesidad de futuras pruebas en ambientes de producción. Por último, debido a motivos de alcance y recursos, no se desarrolla un panel de administración completo para docentes, sino una interfaz básica para demostrar el funcionamiento de supervisión académica (monitoreo de pestañas, bloqueo de copiar y pegar y restricción de URLs), sin implementar mecanismos avanzados como autenticación biométrica, integración profunda con sistemas de gestión del aprendizaje (LMS) o administración detallada de reportes eso debido a priorizar las funciones para la entrega de una versión mínima viable dentro de los límites de tiempo y personal asignado

4. JUSTIFICACIÓN

La educación en entornos virtuales ha tenido un crecimiento importante en los últimos años, especialmente desde la pandemia del COVID-19, que obligó a las instituciones a estructurar sus métodos de enseñanza y evaluaciones en línea. Sin embargo, este cambio trajo algunos inconvenientes como lo es el aumento de casos de fraude académico, lo que presenta un desafío para la integridad de los procesos formativos y la credibilidad de los títulos otorgados.

Este proyecto encuentra su justificación, en primer lugar en el ámbito académico ya que propone una herramienta innovadora que busca salvaguardar la transparencia de las evaluaciones, garantizando que los resultados reflejen el desempeño de los estudiantes, así mismo contribuye a generar confianza en la validez de los procesos educativos.

En el ámbito tecnológico el diseño y desarrollo de un prototipo de extensión para navegador contribuye un aporte en el campo del software aplicado a la seguridad educativa. A diferencia de soluciones como proctoring con cámaras, la extensión ofrece un enfoque menos invasivo, centrado en la detección y prevención de trampa, sin comprometer de manera directa la privacidad de los usuarios.

Desde una perspectiva social, la implementación de esta herramienta aporta a la formación ética de los estudiantes, promoviendo valores como la honestidad y la responsabilidad académica. Por otra parte, fortalece la confianza de la comunidad educativa y de la sociedad en general en torno a la calidad de la educación.

En consecuencia el estudio realizado no solo responde a una necesidad inmediata de las instituciones educativas frente a la evaluación en línea sino que también constituye un punto de partida para futuros desarrollos tecnológicos orientados a garantizar la integridad académica.

5. LÍNEAS DE INVESTIGACIÓN

La extensión para evitar el plagio en exámenes en línea se presenta con las líneas de investigaciones de la universidad de cundinamarca , principalmente es Aprendizaje, conocimiento, tecnologías, comunicación y digitalización, siendo que la propuesta integra el uso de herramientas tecnológicas innovadores que fortalezcan los procesos de enseñanza o aprendizaje, para garantizar la integridad académica y poder promover un uso ético de la información en entornos virtuales de la evaluación.

Por su parte se complementan con la facultad de ingeniería con la línea de investigación de software y sistemas emergentes , debido a que se realiza una solución tecnológica planteada con fundamentos en el desarrollo y aplicación de un sistema de software que permite prevenir prácticas deshonestas como el copiado y el acceso a otras ventanas de fraude académico en plataformas digitales.

Siendo así la extensión para evitar el plagio marca el enfoque multidisciplinar que vincula la innovación tecnológica con la ética académica para poder contribuir en los objetivos institucionales de la investigación como a mejorar la calidad educativa.

CAPÍTULO 2

6. MARCO TEÓRICO

6.1 Marco referencial

6.1.1 Integridad académica en entornos virtuales

La integridad académica se refiere al compromiso de ser honesto, confiable y justo en la formación académica, es algo que siempre se tiene en cuenta para la educación superior (ICAI | Committees, s. f.). Pero, la verdad, desde que la educación pasó a una virtualización, las cosas se han puesto más complicadas. Imaginar que antes se estaba en un salón con un profesor vigilando, y ahora se está solo en casa frente a una pantalla. Todo cambió, especialmente cómo se enfrenta los exámenes.

De acuerdo McCabe en 2010 nos informa que la deshonestidad no es ninguna novedad en las universidades, durante el entorno digital se tiene un nivel de complejidad más alto, además de que se tiene el mundo entero, Google, notas, lo que sea a un clic de distancia (McCabe et al., 2010). Debido a que falta alguien que esté de manera presencial todo se siente más fácil como dice Walsh en 2021 que casi el 81% de los estudiantes piensan que hacer trampa en un examen virtual es más sencillo que en uno presencial (Walsh et al., 2021).

La literatura académica tiene algunas ideas claras que contribuyen a ese comportamiento, en primer lugar, la presión por sacar buenas notas, combinado con la imaginación de que los demás estudiantes lo hacen; son unos de los factores para recurrir a conductas deshonestas y sin sanciones claras incrementando el fraude académico (Ramberg & Modin, 2019).

En segundo lugar, la tecnología de fácil acceso permitiendo acciones de copiar y pegar la información es una acción bastante fácil sabiendo que internet está al alcance durante un examen, y vigilar lo que se hace detrás de la pantalla es un reto enorme (Watson & Sottile, 2010). Además, las políticas del sistema no están claras, o nadie se toma el tiempo de explicar de qué se trata el fraude y hay exámenes tan mal diseñados que pueden incluir a los estudiantes a buscar atajos en la evaluación digital (Maleki, 2025).

Este acontecimiento no es solo un problema de la educación. Guerrero-Dib, Portales y Heredia-Escorza en 2020 destacan que los estudiantes que reportan haber cometido actos contra

la integridad académica también reportan estar involucrados en actividades deshonestas en otros contextos, es decir que si los estudiantes al hacer trampa en un aula, por qué no lo haría en el ámbito laboral, además, cada vez que alguien hace trampa, se pierden las credenciales de las instituciones (Guerrero-Dib et al., 2020).

6.1.2 Métodos comunes de fraude académico en línea

Algunos estudios han publicado cómo los estudiantes utilizan herramientas para saltarse las reglas en los exámenes virtuales, estas herramientas o conductas se pueden dividir en diferentes categorías como recursos prohibidos, trabajo en equipo (no autorizado), trucos tecnológicos, suplantación de identidad. Para una descripción más completa de cada recurso, se presenta una tabla a continuación.

Tabla 1

Métodos comunes de fraude académico en línea

Categoría	Descripción	Referencia
Recursos prohibidos	Buscar respuestas en Google durante el examen, consultar notas abiertas en otras pestañas, usar aplicaciones de traducción o calculadoras avanzadas, y pedir respuestas en grupos de WhatsApp o foros.	Melo-Becerra et al., 2021
Trabajo en equipo (no autorizado)	Enviar mensajes a compañeros, compartir pantalla o pagar a alguien para que realice el examen en su lugar.	Lancaster & Clarke, 2016
Trucos tecnológicos	Usar programas para eludir restricciones del sistema, aprovechar fallos en plataformas de evaluación, tener dispositivos adicionales para consultar información o tomar capturas de pantalla.	Garg & Goel, 2023

Suplantación de identidad	Permitir que otra persona se haga pasar por el estudiante durante el examen o engañar verificaciones de identidad.	Holden et al., 2021b

Nota. Descripción sobre algunos métodos de fraude

Holden en 2021 dice que el 74% de los casos de trampa en línea vienen de buscar en internet o charlar con otros durante el examen (Holden et al., 2021b). Garg & Goel en 2023 notaron que si los estudiantes abandonan con frecuencia la ventana de evaluación para cambiar a otras pestañas del navegador posiblemente se esté incurriendo en fraude (Garg & Goel, 2023).

6.1.3 Tecnología de supervisión de exámenes

Para poner frente al fraude académico, las universidades han implementado algunas tecnologías que vigilan los exámenes en línea. Llamadas proctoring o supervisión remota, en donde las herramientas tienen diferentes enfoques:

IA que observa: Sistemas como ProctorU o Proctorio usan inteligencia artificial para detectar trampa, Movimientos inusuales, mirar fuera de la cámara o algún sonido que se escuche (sonido ambiental. Susurros); La IA lo detecta analizando video y audio en tiempo real (Giller et al., 2019).

Navegadores protegidos: Programas como Respondus LockDown Browser o Safe Exam Browser convierten la computadora en un punto seguro, debido a que no se pueden abrir otras pestañas o aplicaciones, técnicamente dejando visible únicamente el examen (LockDown Browser - Respondus, 2024).

Monitoreo digital: Existen herramientas que registran cada tecla que se toca o cada ventana que cambia. Siendo una herramienta menos invasiva que la supervisión por medio de la cámara. (Noorbehbahani et al., 2022).

Extensiones discretas: Son pequeños programas añadidos al navegador que vigilan cosas específicas del examen, siendo programas más livianos que otras herramientas, aunque se pueden presentar problemas con respecto a la seguridad (Leyden, 2021).

Pero no todo es perfecto. Estas tecnologías pueden impedir a los tramposos hacer fraude en los exámenes, pero puede traer problemas entre algunos estudiantes que sienten que están

siendo observados por lo que su privacidad se siente comprometida; Otros no tienen el equipo o internet para que la herramienta funcione adecuadamente, esta vigilancia podría ver afectada la relación profesor-estudiante ya que los estudiantes sienten mayor desconfianza frente a estas tecnologías (Calderwood, 2025).

Por eso, se propone una extensión de navegador. Es como un punto medio donde se busca un nivel razonable de supervisión durante los exámenes en línea, pero sin que se genere una supervisión excesiva sobre los estudiantes.

6.1.4 Marco legal y ético

En el desarrollo de una extensión de extensión de navegador para la prevención del fraude académico, se debe garantizar la privacidad y seguridad de los datos personales de los estudiantes, según el estudio de Análisis de seguridad de las extensiones para navegadores de las extensiones para navegadores Web (Arturo, 2023). La extensión puede tener acceso a información sensible, lo que exige un manejo responsable y transparente de los datos que se puedan recolectar.

Antes de una instalación los usuarios en este caso los estudiantes deben ser informados de manera clara que los permisos solicitados, el uso que se dará a la información y las medidas de seguridad se implementa dentro de la extensión. Esto en la relación con la ley 1581 de 2012 que nos informa la regulación sobre la protección de datos personales, que tiene como objetivo principal garantizar los derechos constitucionales de todas personas a conocer, actualizar y rectificar la información que se encuentre en bases de datos o archivos, en entidades públicas o privadas (Congreso de la República de Colombia, 2012).

En la base ética es necesario que el sistema no sea invasivo y se respete la autonomía del estudiante, es decir, que se debe evitar las prácticas de vigilancia excesivas que puedan vulnerar los derechos de la intimidad o genera una desconfianza para el proceso educativo (Hillman et al., 2025). De esta manera, se promueve un equilibrio entre la seguridad académica e informática.

6.1.5 Revisión de casos reales

En el estudio de Análisis de Seguridad de las Extensiones para Navegadores Arturo en 2023 documenta de qué riesgos potenciales que pueden tener las extensiones en parte de las seguridades y privacidad, uno de lo más relevante es como una extensión maliciosa que parecía

una herramienta legítima logra obtener datos de los usuarios sin un consentimiento explícito, logrando obtener historial de navegación y credenciales almacenadas; Este tipo de incidente demuestra que si no se implementan controles en algunas extensiones legítimas como traductores o complementos, estos solicitan permisos excesos que manipulan el contenido de páginas (DMO) lo que facilita la inyección de código o alteración de información sensible (Arturo, 2023).

Por otro lado, está el caso positivo de cómo la implementación segura de la Universidad Externado de Colombia con Safe Exam Browser (SEB) esta institución usa la plataforma Moodle donde se realizan los exámenes en un entorno controlado logró impedir el acceso a otras páginas, funciones del sistema (copiar y pegar, imprimir pantalla), además la configuración además la configuración adopta garantiza que no se recolectan datos sensibles del dispositivo. Permitiendo mantener una integridad durante la evaluación así respetando la privacidad (Cev, 2020).

A partir de la revisión de casos reales, se identificó que la mayoría de las soluciones existentes, como Safe Exam Browser, Respondus LockDown Browser o los sistemas de proctoring basados en inteligencia artificial, presentan altos niveles de intrusividad y dependencia de hardware adicional, lo cual puede generar desconfianza por parte de los estudiantes. En contraste, la propuesta desarrollada en este proyecto se diferencia por su enfoque preventivo y no punitivo, orientado a mitigar las oportunidades de fraude sin invadir la privacidad del usuario. Este factor diferencial radica en el desarrollo de un prototipo de una extensión ligera, adaptable y de bajo consumo de recursos, que opera directamente sobre navegadores convencionales y prioriza la experiencia del usuario. De esta manera, se promueve una alternativa tecnológicamente viable, pedagógicamente respetuosa y éticamente responsable frente a los modelos de supervisión tradicionales.

6.1.6 Antecedentes Nacionales e internacionales

6.1.6.1 Antecedentes nacionales

En diversos estudios han abordado los desafíos de una integridad académica en la educación virtual en Colombia. Oyague en 2023 señalan que la masificación de los entornos digitales durante la educación superior trajo consigo un incremento en los riesgos de fraudes académicos, obligando a las instituciones a realizar diseños estratégicos innovadores que logren

salvaguardar la calidad educativa y fortalecer la confianza en procesos de evaluaciones (Oyague et al., 2024).

En cambio, Martínez-Garcés y Garcés-Fuenmayor en 2020 explican que los principales retos en el país se constituyen en la ausencia de una cultura institucional sólida durante la integridad académica, lo que traduce en prácticas de copia, suplantación y mal uso de los recursos digitales en la presentación de exámenes en línea. Estos autores resaltan la implementación de las herramientas tecnológicas, que no solo previene el fraude también generan una experiencia del estudiante sin poder vulnerar sus derechos (Martínez-Garcés & Garcés-Fuenmayor, 2020).

Finalmente, desde el Congreso de la República de Colombia nos constituye la ley 1581 de 2012 la cual nos da el marco fundamental al establecer principios y disposiciones generales para proteger datos personales. Con esta ley sobre la importancia del diseño de soluciones tecnológicas, pues asegura que está supervisión de evaluaciones debe salvaguardar la privacidad y seguridad de la información para los estudiantes (Congreso de la República de Colombia, 2012).

6.1.6.2 Antecedentes Internacionales

En el plano internacional Guerrero-Dib en 2020 documentan la integridad académica genera un impacto de procesos educativos, además generan un comportamiento ético en el ámbito laboral. Ellos sostienen que al tener esas prácticas deshonestas en el ámbito académico generan repercusiones al reproducirse posteriormente en la vida profesional, lo que da refuerzo de la importancia de medidas preventivas en la institución educativa (Guerrero-Dib et al., 2020b).

Igualmente, Stone en 2022 realiza el análisis de las percepciones de los estudiantes frente a su integridad académica en los entornos virtuales, reconociendo las consecuencias de cometer fraude, por considerar que es más sencillo en escenarios en línea por la falta de vigilancia presencial. Con esto se constituye un reto significativo para las Universidades a nivel global que buscan un entorno virtual (Stone, 2022).

Por último, Noorbehbahani en 2022 realizó una revisión sistemática de investigaciones durante 2010 y 2021 sobre fraudes académicas en exámenes en línea, sus hallazgos mostraron los métodos más comunes usadas incluyendo el uso de dispositivos externos, haciendo consultas de recursos digitales no autorizados, Además, se evidencia que el desarrollo de las tecnologías de supervisión y detección han tenido un crecimiento exponencial, pero con varios debates a su efectividad y respecto a la privacidad que generan estas tecnologías (Noorbehbahani et al., 2022).

6.2 Marco conceptual

Este marco conceptual define los términos y categorías centrales para el desarrollo del proyecto, asegurando el uso de conceptos clave relacionados con la integridad académica, el fraude en entornos virtuales y una de las tecnologías usada para el control en exámenes en línea.

6.2.1 Fraude académico

El fraude académico comprende las acciones deshonestas en las cuales un estudiante podría obtener ventajas indebidas en procesos de evaluación. Esas prácticas afectan la validez de los resultados de aprendizaje y debilitan la credibilidad institucional. En el artículo Análisis de seguridad informática en entornos virtuales de la Universidad Regional Autónoma de los Andes extensión Quevedo en tiempos de COVID-19 destacan que, en los entornos virtuales, estas conductas aprovechan vulnerabilidades técnicas y su falta de supervisión directa (Zuñiga Paredes et al., 2021).

6.2.2 Integridad académica

La integridad académica se entiende como el compromiso con los valores de honestidad, confianza, justicia, respeto y responsabilidad en la parte educativa (ICAI | Valores, s. f.). Este concepto nos da la base para un diseño de las políticas o herramientas que estén destinadas para el fraude académico.

6.2.3 Proctoring

Hace referencia al conjunto de las tecnologías de supervisión digital que busca la autenticidad e integridad de los exámenes en línea, según LEE y Fanguy en 2022, las

herramientas permiten una reducción de las ocurrencias de fraude y generar debates éticos sobre el impacto en la confianza y la experiencia del estudiante (Lee & Fanguy, 2022).

6.2.4 Extensiones de navegador

Las extensiones son pequeños programas los cuales dan funcionalidades de un navegador web, teniendo acceso a información del navegador web y poder modificar la información del usuario. En el contexto académico, las extensiones se configuran para poder hacer limitaciones en las funciones de copiar, pegar o abrir nuevas pestañas, con el fin de poder prevenir el fraude en las evaluaciones (Arturo, 2023).

6.2.5 Privacidad y protección de datos

La privacidad de los datos es un derecho fundamental el cual los individuos a controlar recolección, uso y divulgación de los datos en dado caso que sea información personal. En Colombia, el derecho se regula con la ley 1581 de 2012, la cual establece disposiciones generales para tener la protección de datos personales y hace una exigencia de prácticas responsables de esta información (Congreso de la República de Colombia, 2012).

6.3 Marco ingenieril

El proyecto se enmarca en la ingeniería de sistemas y computación como se construyó la solución orientada a la integridad académica en entornos virtuales. Se propone el desarrollo de una extensión de navegador la cual previene las prácticas de fraude durante evaluaciones en línea; Integrando la usabilidad, seguridad informática y cumplir con la normativa.

El marco ingenieril se fundamenta en arquitectura de software modernas, metodología ágiles, estándares internacionales y herramientas, lo cual garantiza la rigurosidad técnica y la pertinencia en un ámbito educativo.

6.3.1 Arquitectura y metodología

La extensión se diseñó bajo la arquitectura cliente-navegador, la cual el procesamiento principal ocurre dentro del navegador del estudiante. El enfoque se apoya en la evolución de las WebExtensions Apis de Google. particularmente con la transacción de manifest V3, permitiendo la seguridad de la misma para poder tener los controles de los permisos que solicitados y reducir vulnerabilidades potenciales (Cómo Migrar A Manifest V3, 2024).

Durante el desarrollo se aplicó la metodología ágil Scrum, que asegura ciclos iterativos e incrementales, como se facilita las pruebas piloto y garantiza que se haga entrega en funciones parciales, está metodologías permite la validación temprana de resultados y adaptación al cambio en los requisitos (Scrum Guides, 2025). Por lo tanto ayuda a la definición y documentación de los requisitos que se alinearon a las buenas prácticas de la ingeniería donde se da como recomendación de la claridad, verificabilidad, trazabilidad en las especificaciones (Pacheco et al., 2022).

6.3.2 Herramientas y modelos aplicados

La seguridad académica, se destaca una herramienta como safe Exam Browser (SEB), siendo usada por instituciones de educación superior para crear entornos controlados que genere los bloqueos de accesos no autorizados y limitan atajos o funciones externas (Safe Exam Browser – About, s. f.; Safe Exam Browser – Windows User Manual, s. f.). Este navegador sirve para hacer referencias que evalúan los alcances y las limitaciones de la propuesta en desarrollo.

Por otro lado se analiza el riesgo de la seguridad informática presentes en los entornos virtuales de universidades en Latinoamérica, donde la extensión de navegador señala como pueden ser vectores de vulnerabilidades y acceso indebido de datos sensibles (Paredes, 2021), Frente a ello, el desarrollo de la extensión busca mitigar dichos riesgos mediante la implementación de controles preventivos dentro del propio entorno de evaluación.

En la fase de analizar y ver los resultados, se dará uso a Power BI que permite transformar los datos en tableros interactivos y una visualización dinámica, lo que facilita poder tomar decisiones académicas y administrativas (JulCsc, 2025).

6.3.3 Estándares de buenas prácticas

El prototipo se diseña y se valida con estándares internacionales.

- ISO/IEC 25010:2011: Establece un modelo de calidad del software, como se incluye atributos como seguridad, usabilidad, eficiencia y mantenibilidad (ISO/IEC 25010:2011, s. f.).

- OWASP Top 10: Marco de referencia para prevenir riesgos críticos de aplicaciones web además de la inyección de código, control en acceso o gestión de seguridad en los permisos (OWASP, 2021).

- HTML Y CSS estándares del W3C, aseguran interoperabilidad y cumplen con prácticas reconocidas en el desarrollo web (W3C, 2022).

En este contexto las normas colombianas, la solución se ajusta con la ley de 1581 de 2012, que hace regulación del tratamiento de datos personales y establecer garantías de transparencias y consentimientos en uso de la información sensible (Congreso de la República de Colombia, 2012).

6.3.4 Compromiso social e innovación

La herramienta desarrollada representa una contribución tecnológica para la transformación de la educación virtual. Además de responder a retos técnicos de integridad académica, con soluciones menos invasivas y más aceptables para docentes y estudiantes. De este modo, se sienta un precedente de innovación responsable, éticamente comprometida y socialmente pertinente orientada a fortalecer los procesos de formación en la era digital.

CAPÍTULO 3

7. METODOLOGÍA

La investigación se enmarca dentro de un enfoque mixto cualitativo y cuantitativo, ya que combina la descripción de fenómenos sociales y educativos con la recolección y análisis de datos numéricos obtenidos a través de pruebas y encuestas.

Desde el punto de vista investigativo, la metodología es de tipo exploratoria y descriptiva, permite analizar el fenómeno del fraude académico en entornos virtuales, comprender las percepciones de estudiantes y docentes, y describir el funcionamiento de la solución tecnológica propuesta: una extensión de navegador orientada a prevenir prácticas de fraude en evaluaciones en línea.

Desde el punto de vista investigativo, la metodología es de tipo exploratoria y descriptiva, pues permite analizar el fenómeno del fraude académico en entornos virtuales, comprender las percepciones de estudiantes y docentes, y describir el funcionamiento de la solución tecnológica propuesta: una extensión de navegador orientada a prevenir prácticas de fraude en evaluaciones en línea.

7.1 Enfoque metodológico

El proyecto se estructura en dos niveles complementarios:

Nivel investigativo: Permite identificar, describir y analizar las principales formas de fraude académico en entornos virtuales, así como evaluar la percepción y efectividad de la herramienta propuesta.

Nivel técnico: Corresponde al proceso de diseño, desarrollo, prueba y validación del prototipo de software, siguiendo las fases del ciclo de vida de ingeniería de software.

7.2 Fases del proceso de desarrollo

El desarrollo del proyecto se implementó siguiendo las fases del marco Scrum, adaptadas al contexto académico

7.2.1 Análisis de requisitos

Se identificaron las necesidades del sistema y los riesgos asociados al fraude académico. Se revisaron antecedentes teóricos y herramientas similares, definiendo los requerimientos funcionales y no funcionales de la extensión.

7.2.2 Historias de usuario

Como parte del análisis de requisitos y siguiendo la metodología ágil Scrum, se definieron historias de usuario que representan las necesidades funcionales del sistema desde la perspectiva de los actores principales: estudiantes, docentes y administradores del sistema. Cada historia sigue el formato estándar: "Como [rol], quiero [funcionalidad], para [beneficio]".

Tabla 2

Historias de usuario del prototipo ProctorGuard

Actor	Historia de usuario	Criterios de aceptación

Docente	Como docente, quiero configurar la extensión para un examen específico, para habilitar el monitoreo solo durante ese periodo.	Dado que estoy en Moodle/LMS, cuando creo un examen, entonces debe haber una opción para enlazar la extensión y establecer la duración del monitoreo.
Estudiante	Como estudiante, quiero activar la extensión al iniciar mi examen, para demostrar mi honestidad y poder comenzar la evaluación.	Dado que inicio el examen, cuando la extensión solicita activación, entonces al aceptar, el estado de monitoreo debe cambiar a "Activo" y el examen debe desbloquearse.
Estudiante	Como estudiante, quiero recibir una notificación si detecta una acción no permitida (ej. cambio de pestaña), para tener la oportunidad de corregir mi comportamiento y evitar una alerta mayor.	Dado que realizó una acción prohibida, cuando la extensión la registra, entonces aparece una ventana emergente no obstructiva que indica la infracción y el tiempo restante de examen.
Sistema(LMS)	Como LMS, quiero recibir y almacenar los registros de eventos de la extensión, para que el docente pueda consultar la evidencia detallada de las alertas generadas.	Dado que la extensión registra un evento (ej. copia de texto), cuando el evento se envía al servidor, entonces se guarda el timestamp, el tipo de evento y el identificador del estudiante en la base de datos.

Nota. Descripción historias de usuarios

7.2.3 Definición de Done(DoD)

Esta es una lista de verificación que se aplica a cada historia de usuario o elemento del *Product Backlog* (PBI) antes de que pueda ser considerado terminado.

- Código: El código cumple con las guías de estilo, está integrado en la rama principal.
- Pruebas Unitarias: Se han creado y superado el 100% de las pruebas unitarias para el componente funcional.
- Pruebas de Integración: La funcionalidad ha sido probada con el LMS (Moodle) y el reporteador.
- Criterios de Aceptación: Todos los Criterios de Aceptación de la Historia de Usuario han sido verificados.
- Documentación: La documentación técnica (API, comentarios en código) está actualizada y la documentación de usuario ha sido creada.
- Rendimiento/Seguridad: La funcionalidad no introduce vulnerabilidades de seguridad ni degrada el rendimiento del navegador o el LMS.

7.2.4 Product backlog

Es una lista priorizada de todos los requerimientos y funcionalidades del proyecto. Se presenta como una tabla.

Tabla 3

Product backlog

ID	Historia de usuario	Estimación	Prioridad	Modulo/ Componente
HU01	(Docente) Configurar la extensión para un examen.	8	Must Have	Panel Docente/Integración LMS
HU02	(Estudiante) Activar la extensión al iniciar el examen.	5	Must Have	Interfaz de Extensión
HU03	(Estudiante) Recibir notificación	5	Should Have	Interfaz de Extensión

	por acción no permitida.			
HU04	(Sistema) Registrar eventos de cambio de pestaña.	3	Must Have	Lógica de Monitoreo

Nota. Descripción los requerimientos y funcionalidades del proyecto

7.2.5 Priorización y asignación de sprints

La codificación del desarrollo con JavaScript (ES6), HTML5 y CSS3, utilizando Visual Studio Code y control de versiones en GitHub.

Cada iteración del desarrollo (sprint) tuvo una duración de dos semanas, implementando las funcionalidades planificadas, seguido de pruebas internas y ajustes.

Los entregables principales por sprint fueron:

- Sprint 1: diseño de estructura base y permisos.
- Sprint 2: implementación de detección de pestañas.
- Sprint 3: bloqueo de copiar/pegar.
- Sprint 4: alertas y registro de eventos.
- Sprint 5: pruebas piloto y documentación técnica

7.2.6 Diseño técnico

Se definió la arquitectura cliente-navegador, se diseñaron los diagramas de flujo y se seleccionaron las tecnologías base: HTML5, CSS3, JavaScript y Manifest V3. Esta etapa permitió definir la estructura modular de la extensión y los permisos de ejecución.

7.2.7 Desarrollo del prototipo

En sprints de dos semanas, se implementan las funcionalidades principales: detección de cambio de pestaña, bloqueo de copiado/pegado y notificaciones de alerta. Cada sprint culminó con revisiones y ajustes técnicos.

7.2.8 Pruebas piloto y validación

Se realizaron pruebas de funcionalidad y seguridad en entornos simulados, observando el comportamiento de los usuarios y la efectividad de las medidas de control.

7.2.9 Análisis de resultados y documentación

Se procesaron los datos obtenidos en las pruebas y encuestas, utilizando herramientas de análisis visual como Excel y Power BI, con el fin de evaluar la percepción de los participantes y el rendimiento del prototipo.

7.3 Población y muestra

Se tuvo en cuenta que para el estudio se buscaba que la población objetivo estuviera conformada por estudiantes de las universidades que realizan evaluaciones virtuales, esta muestra se selecciona debido a los criterios que darán usos previos de la plataforma virtuales para exámenes debido que se busca la disposición para participar en el estudio para poder tener correctamente las experiencias con herramientas de monitoreo para las evaluaciones virtuales. Esta se compuso por una muestra inicial de:

- 70 estudiantes de pregrados (sugerida por el docente de semillero)

7.4 Técnicas y muestra

- Encuestas estructuradas: Encuestas para estudiantes y docentes, para poder saber y entender los conocimientos sobre la seguridad en los exámenes virtuales, Tipos de fraudes además tener conocimiento de las experiencias sobre las herramientas tecnológicas para tener la solución propuesta.
- Observación directa: Realizada las pruebas piloto de la extensión para navegador, que proporciona una documentación de cómo funciona, el comportamiento de los estudiantes, además de tener mejoras en la extensión.

- Registros técnicos: generados automáticamente por la extensión, mostrando intentos de copiar, pegar o cambiar de pestaña durante la evaluación.

7.5 Procedimientos

1) Revisión de literatura sobre fraude académico y herramientas de monitoreo.
2) Desarrollo del prototipo de extensión.
3) Diseño y aplicación de encuestas y entrevistas.
4) Ejecución de pruebas piloto de la extensión en un entorno simulado.
5) Observación, registro y análisis de resultados.
6) Procesamiento de datos mediante herramientas estadísticas y visuales.
7) Redacción de conclusiones y recomendaciones.

7.6 Análisis de datos

Se utilizaron herramientas como Excel, Power BI para el análisis de los datos cuantitativos, lo que permite obtener estadísticas descriptivas de estos; en cuanto a los datos cualitativos, mediante entrevistas y observaciones de las pruebas de la extensión de navegador, se identificaron patrones y categorías emergentes, logrando una presentación escrita e informativa de los resultados que profundizó el análisis de los datos.

7.7 Alineación con los objetivos

Cada fase del proceso metodológico y del desarrollo del prototipo está formalmente alineada con los objetivos general y específicos del proyecto, garantizando la trazabilidad y correspondencia entre el diagnóstico inicial, la construcción de la herramienta y la evaluación de su impacto, por otro lado las historias de usuario se asegura la trazabilidad entre las necesidades de los actores del sistema y los requisitos técnicos implementados

7.8 Fases del ciclo de vida del desarrollo

El desarrollo del prototipo fue estructurado por medio de un ciclo de vida iterativo basándose en cuatro fases fundamentales de la ingeniería de software, además de la integración de la metodología Scrum:

7.8.1 Análisis

En esta fase se identificaron las necesidades del sistema, que riesgos se asocian con fraude académico digital y las limitaciones dentro de las herramientas que existen. con la revisión de las fuentes académicas, se definieron casos de uso preliminares y se establecieron los requisitos funcionales y no funcionales de la extensión.

7.8.2 Planeación

Se elaboró un prototipo del producto final, priorizando funcionalidades esenciales como detección de cambio de pestaña, bloqueo de copiar/pegar y restricción de navegación. Se definieron tres sprints de dos semanas cada uno, con reuniones de seguimiento y revisión al finalizar cada iteración.

7.8.3 Desarrollo

Se implementó las funcionalidades acordadas en cada sprint. Además de construir la arquitectura cliente-navegador bajo Manifest V3, con él desarrollaron los módulos de monitoreo y restricción, para obtener ajustes continuos con función de una retroalimentación que se obtiene en las revisiones periódicas.

7.8.4 Despliegue y validación

Se ejecutaron las pruebas piloto con estudiantes en un entorno controlado. Con registros de comportamientos sospechosos, para poder evaluar el funcionamiento del prototipo y se recopilaron opiniones de los usuarios en este caso los estudiantes. Con esto se realizó la validación de la funcionalidad y establecer mejoras para versiones futuras.

8. DESARROLLO DEL PROYECTO

El desarrollo se llevó a cabo con un enfoque mixto, combinando el enfoque cuantitativo y cualitativo, además de los principios de la ingeniería de software y la metodología ágil scrum.

El diseño cuantitativo permite recolectar datos de manera estadística sobre el uso de las tecnologías para la vigilancia durante exámenes virtuales con encuestas a estudiantes. El enfoque cualitativo da una opinión, experiencias y que se podría mejorar, con entrevistas

semiestructuradas y observación del uso de las herramientas en pruebas piloto de la extensión para navegador con esto se pudo tener una compresión al poder relacionar datos numéricos y la interpretación contextual del uso en los usuarios.

Desde la perspectiva técnica el desarrollo del prototipo se realiza aplicando los principios de la Ingeniería de Software y la metodología ágil Scrum mediante sprints iterativos que garantizan un proceso iterativo e incremental que permite la construcción de una extensión de navegador funcional, orientando a la prevención de fraude académico en evaluaciones en línea. Está estructurado en fases técnicas que aseguran la trazabilidad, mantenibilidad y validación del producto final.

8.1 Prototipo y arquitectura del sistema

8.1.2 Descripción del prototipo

La propuesta técnica se centró en el diseño y desarrollo de un prototipo de extensión de navegador orientada a prevenir el fraude académico durante los exámenes en línea. Este prototipo busca convertirse en una herramienta complementaria para docentes y estudiantes dentro de los entornos virtuales de aprendizaje, garantizando un equilibrio entre la supervisión académica y el respeto a la privacidad del usuario.

El prototipo desarrollado integró tres funciones principales:

- Monitoreo de cambios de pestaña: detecta cuando el estudiante abandona la ventana de evaluación para abrir otros sitios web.
- Detección de acciones de copiar y pegar: registra intentos de la acción de copiar y pegar mediante atajos del teclado o menús.
- Restricción de navegación durante el examen: limita el acceso a sitios externos mientras se realiza la prueba, reduciendo las posibilidades de búsqueda de respuestas en línea.

Este conjunto de funciones permite contar con una primera versión operativa del sistema, con la capacidad de supervisar comportamientos asociados con el intento de fraude académico sin convertirse en un software invasivo un ejemplo gráfico del flujo se puede observar a continuación, donde se muestra el flujo entre la extensión, el usuario y en este caso Moodle (plataformas de evaluación).

Figura 1

Flujo entre la extensión, el usuario y en este caso Moodle.

Nota. Gemini. Esquema que ilustra la interacción entre el usuario, la extensión del navegador y Moodle. 2025.

8.1.2 Arquitectura

Está se basó en un enfoque por módulos, lo que permite la escalabilidad e incorporación de nuevas funciones en versiones futuras. Los módulos principales son:

- Integración con Moodle: permite habilitar y deshabilitar la extensión en los exámenes creados por los docentes
- Supervisión local: detecta cambios de pestaña y combinación de teclas sospechosas
- Restricción de navegación: bloquea direcciones URL no autorizadas en el examen

El funcionamiento de cada módulo interactúa mediante APIs del navegador (Manifest V3), garantizando un control de permisos, eficiencia y seguridad para cuando el estudiante inicia una evaluación en Moodle, debe activar la extensión desde el cuadro de activación. Una vez habilitada, se ejecuta el monitoreo en tiempo real de la interacción del usuario con el navegador.

Figura 2

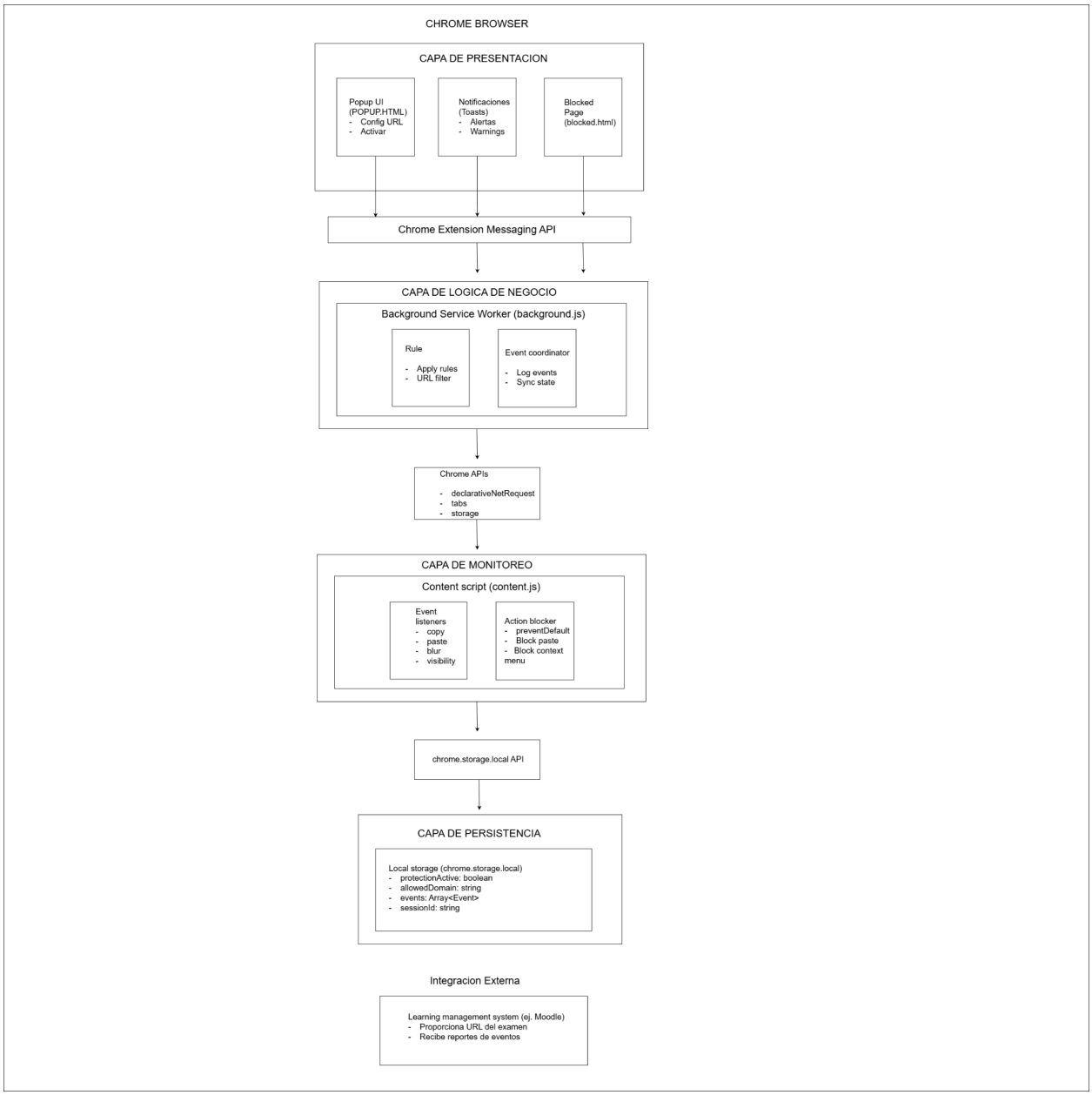
Flujo de funcionamiento de la extensión

Nota. Flujo de funcionamiento desde que entra a Moodle a la restricción de la página

8.1.2.1 Arquitectura de componentes del sistema

Figura 3

Arquitectura de componentes de ProctorGuard



Nota. Arquitectura de componentes mostrando las cuatro capas principales del sistema y sus interacciones mediante APIs de Chrome.

Capa de presentación: esta capa maneja toda la interacción visual con el usuario, está compuesta por tres elementos:

- Popup UI(popup.html/popup.js): Interfaz principal donde el estudiante configura la URL del examen y activa la protección, incluye validación de entrada y visualización del estado actual.
- Sistema de notificaciones(toasts): genera alertas visuales no intrusivas en la parte de arriba de la pantalla cuando se detecta una acción sospechosa. Utiliza CSS para animaciones y JavaScript para control de tiempo de visualización.
- Página de bloqueo(blocked.html): Página estática que se muestra cuando el estudiante intenta acceder a un dominio no autorizado durante el examen.

Capa de lógica de negocio: implementada en background service worker (background.js) es la que lleva un manejo de todas las operaciones de la extensión:

- Rule manager: es el módulo responsable de aplicar y actualizar dinámicamente las reglas de navegación usando la API declarativeNetRequest también filtra URLs y mantiene la lista de dominios permitidos.
- Event coordinator: centraliza la recepción de eventos desde el content script, los valida, los registra en el storage y coordina las respuestas.

Capa monitoreo: es ejecutada dentro del contexto de las páginas web mediante content.js:

- Event listeners: Conjunto de detectores que captan eventos del DOM como copiar, pegar, cortar, cambio de pestaña.
- Action blocker: implementa la lógica de prevención llamando a preventDefault() sobre eventos prohibidos y generando los registros.

Capa de persistencia: utiliza la API chrome.storage.local para mantener el estado de la extensión:

- protectionActive: boolean que indica si el monitoreo está activo
- allowedDomain: string con el dominio del examen

- events: array de objetos que registran cada evento detectado con timestamp y tipo
- sessionId: identificador unico de la sesión de examen

8.1.2.2 Arquitectura logica detallada

Se basa en un modelo de cuatro capas que separa las responsabilidades del sistema siguiendo principios de ingeniería de software, esta estructura facilita el mantenimiento, la escalabilidad y la comprensión del funcionamiento interno del sistema.

Tabla 4

Descripción detallada de capas de arquitectura

Capa	Responsabilidades	Componentes	Tecnologías	Interacción con otras capas
Presentación	- Capturar entrada del usuario - Mostrar estado del sistema - Renderizar notificaciones - Proporcionar feedback visual	- popup.html/popup.js - popup.css - Sistema de toasts - blocked.html	- HTML5 - CSS3 - JavaScript (ES6) - DOM API	Envía comandos a Lógica de Negocio Recibe actualizaciones de estado
Lógica de Negocio	- Orquestar operaciones - Aplicar reglas de negocio - Coordinar flujos de trabajo - Gestionar estado global	- background.js - Rule Manager - Event Coordinator - State Manager	- Service Worker API - Chrome Runtime API - Promise-based async	Solicita datos a Persistencia Recibe eventos de Monitoreo Usa Chrome APIs

Monitoreo	- Detectar eventos del DOM - Bloquear acciones prohibidas - Capturar comportamiento - Generar evidencia	- content.js - Event Listeners - Action Blocker - Toast Renderer	- Content Script API - DOM Events	Reporta a Lógica de Negocio Recibe configuración de activación
Persistencia	- Almacenar configuración - Guardar eventos - Mantener sesión - Proporcionar datos históricos	- chrome.storage.local - Event Log - Configuration Store	- Chrome Storage API - JSON serialization - Async storage	Provee datos a Lógica de Negocio Recibe datos para persistir

Nota. Cada capa tiene responsabilidades bien definidas y se comunica con las capas adyacentes mediante interfaces claras.

8.1.3 Artefactos de diseño

Como parte del diseño técnico del prototipo se elaboró un modelo de casos de uso que representan interacciones principales entre los actores y el sistema. Este artefacto permite visualizar las funcionalidades desde la perspectiva del usuario.

Actores del sistema

Estudiante: usuario que presenta la evaluación y activa la extensión

Docente: usuario encargado de recibir los reportes y supervisar el examen

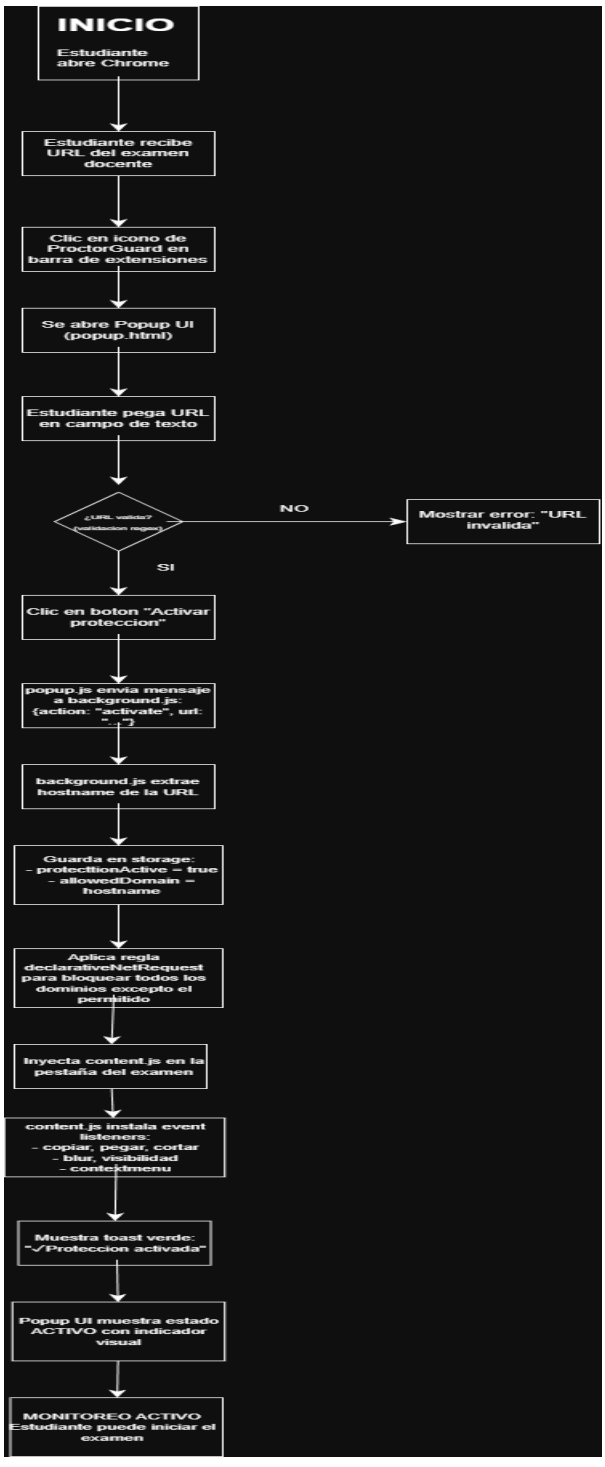
Extensión del navegador: componente responsable del monitoreo y restricciones

8.1.3.1 Diagramas de flujo de procesos

Se presentan los flujos de procesos principales que ilustran las secuencias de operaciones desde la perspectiva del usuario y del sistema.

Figura 4

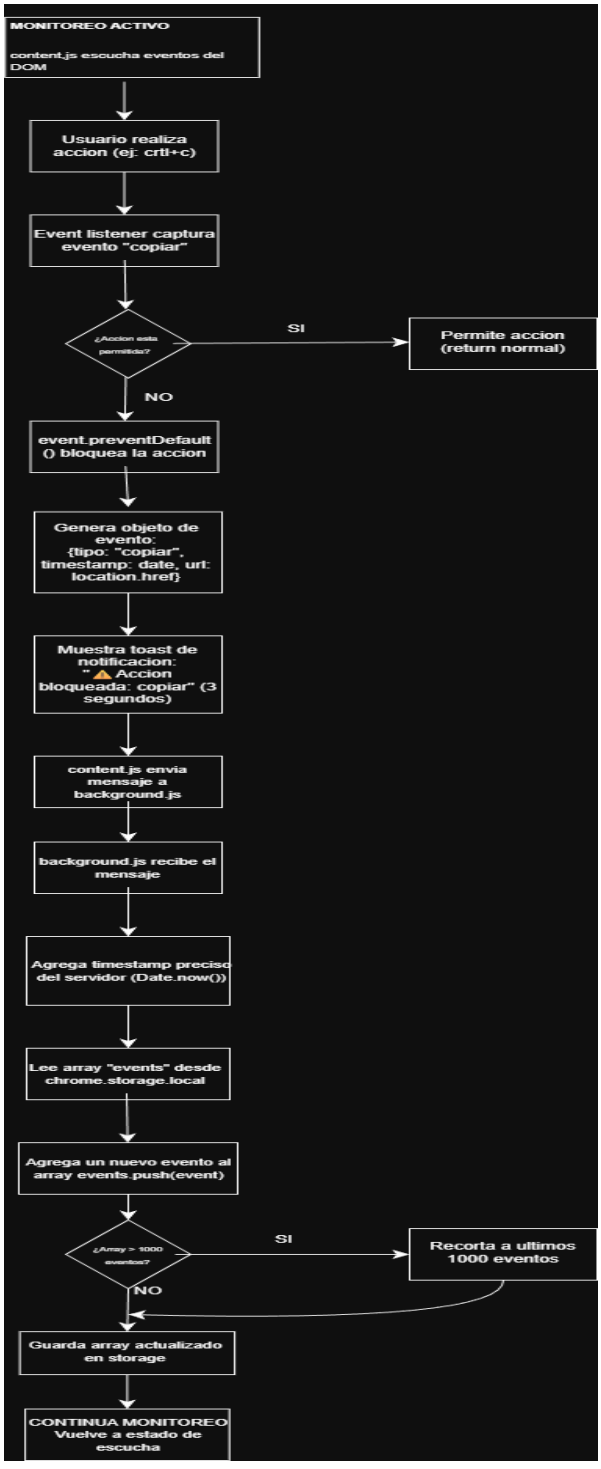
Flujo de activación de la extensión



Nota. Secuencia completa desde que el estudiante recibe la URL hasta que la protección queda activada y funcionando.

Figura 5

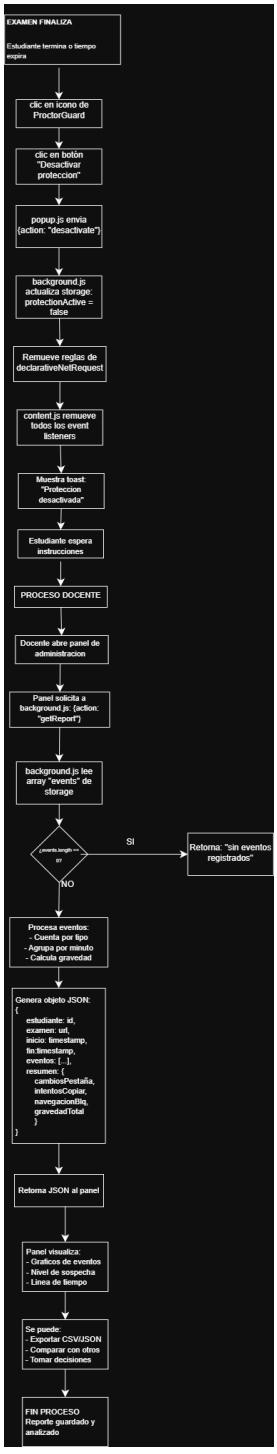
Flujo de detección de evento sospechoso



Nota. Proceso completo desde que se detecta una acción sospechosa que se registra y notifica, retornado al estado de monitoreo.

Figura 6

Flujo de generación y consulta de reportes



Nota. Secuencia desde la finalización del examen hasta la generación, consulta y análisis de reporte por parte del docente.

Flujo de Manejo de Errores y Excepciones

Adicionalmente, el sistema contempla flujos de excepción para situaciones no esperadas:

Pérdida de conexión durante el examen

- El sistema continúa monitoreando localmente
- Los eventos se almacenan en storage local
- Al recuperar conexión, se sincronizan automáticamente
- No se pierde información registrada

Estudiante cierra el navegador

- Los datos en storage.local persisten
- Al reabrir y reactivar la extensión, se crea nueva sesión
- Los eventos anteriores quedan disponibles para el reporte final

Conflicto con otra extensión

- background.js detecta interferencia (eventos no capturados)
- Genera alerta al estudiante: "Posible conflicto detectado"
- Sugiere desactivar otras extensiones
- Registra evento de "Conflicto técnico" en el reporte

Estos flujos garantizan la trazabilidad completa de las operaciones y facilitan el debugging durante el desarrollo y mantenimiento del sistema.

8.1.4 Casos de uso

Para una correcta interpretación de los requisitos del prototipo y su desarrollo iterativo bajo la metodología Scrum, se definieron los diferentes casos de uso los cuales describen de forma estructurada las acciones que pueden realizar los estudiantes , docentes y usuarios, además de las respuestas esperadas del sistema. Este conjunto de casos permite comprender el comportamiento funcional del prototipo

8.1.4.1 Activar extensión

El estudiante habilita la extensión al iniciar el examen pegando el link para poder permitir la ejecución de los controles definidos.

8.1.4.2 Monitorear cambio de pestaña

Se realiza la detección en los que los estudiantes abandonan la ventana del examen.

8.1.4.2 Bloquear copiar/pegar

Se capturan los intentos de copiar y pegar usando las teclas o menú contextual.

8.1.4.3 Restringir navegación externa

Se bloquea el acceso a direcciones no permitidas durante el examen.

8.1.4.5 Generar reportes de eventos

El sistema registra intentos sospechosos y genera un informe con todos las acciones intentadas por los estudiantes siendo un apoyo de información para el docente.

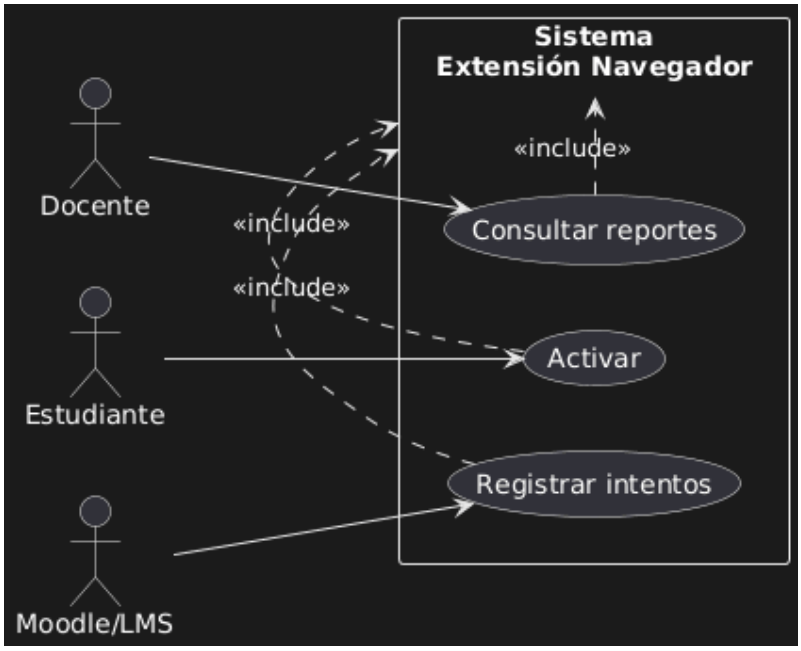
8.1.4.6 Consultar reportes

El docente revisa los registros obtenidos durante la prueba.

Diagrama UML

Figura 7

Modelo casos de uso



Nota. Representa las interacciones principales entre los actores y el sistema

8.2 Implementación del sistema

Las historias de usuario fueron priorizadas y distribuidas en los sprints de desarrollo para la implementación adecuada de la siguiente manera:

Sprint 1 (Semanas 1-2): Infraestructura base

- HU-01: Configuración del dominio permitido (3 puntos)

- Tareas técnicas: Manifest V3, estructura de archivos, chrome.storage

Sprint 2 (Semanas 3-4): Detección y notificaciones

- HU-03: Detección de cambio de pestaña (3 puntos)

- HU-03: Notificación de acciones sospechosas (5 puntos) - Total: 8 puntos

Sprint 3 (Semanas 5-6): Bloqueo de acciones

- HU-04: Bloqueo de navegación externa (8 puntos)

Sprint 4 (Semanas 7-8): Activación y reportes

- HU-04: Activación de la extensión (3 puntos)

-HU-04: Generación de reportes (5 puntos) - Total: 8 puntos

Sprint 5 (Semanas 9-10): Refinamiento y desactivación

-HU-01: Desactivación post-examen (2 puntos)

-HU-01: Compatibilidad con recursos (5 puntos)

Pruebas piloto y corrección de bugs - Total: 7 puntos

Backlog futuro (Post-MVP):

-HU-04: Prevención de capturas de pantalla

Esta priorización permitió entregar un Producto Mínimo Viable (MVP) funcional al finalizar el Sprint 4, dedicando el Sprint 5 a la validación con usuarios reales.

La codificación del desarrollo con JavaScript (ES6), HTML5 y CSS3, utilizando Visual Studio Code y control de versiones en GitHub, se realizó siguiendo las historias de usuario definidas en la sección 7.2.1.1. Cada iteración del desarrollo (sprint) tuvo una duración de dos semanas, implementando las funcionalidades planificadas según la priorización MoSCoW, seguido de pruebas internas y ajustes.

8.3 Pruebas pilotos y validación

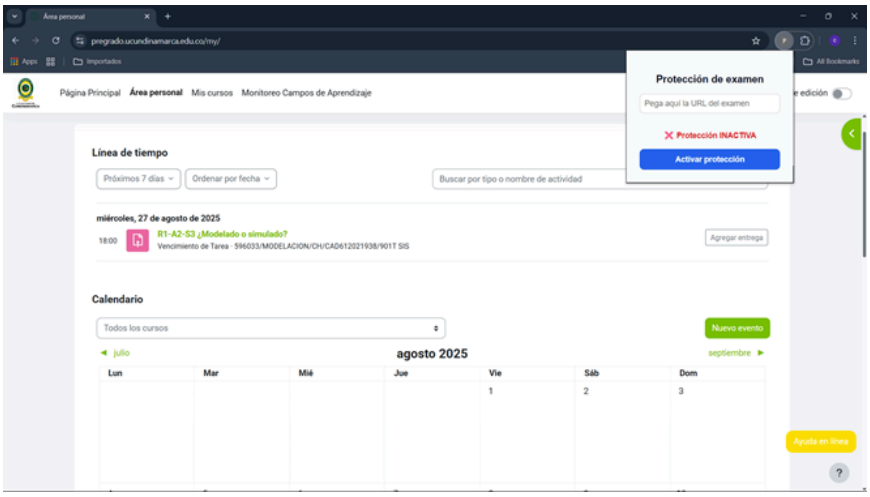
Estas pruebas se realizaron en un entorno simulado de evaluación virtual con 10 estudiantes , El objetivo principal fue validar la funcionalidad del prototipo de extensión de navegador y evidenciar, mediante capturas de pantalla, el funcionamiento de cada una de las características.

8.3.1 Evidencia de funcionalidad mediante capturas

A continuación se describen las funciones principales del prototipo y se acompaña cada explicación con la respectiva captura

Figura 8

Pantallazo en Moodle de la extensión

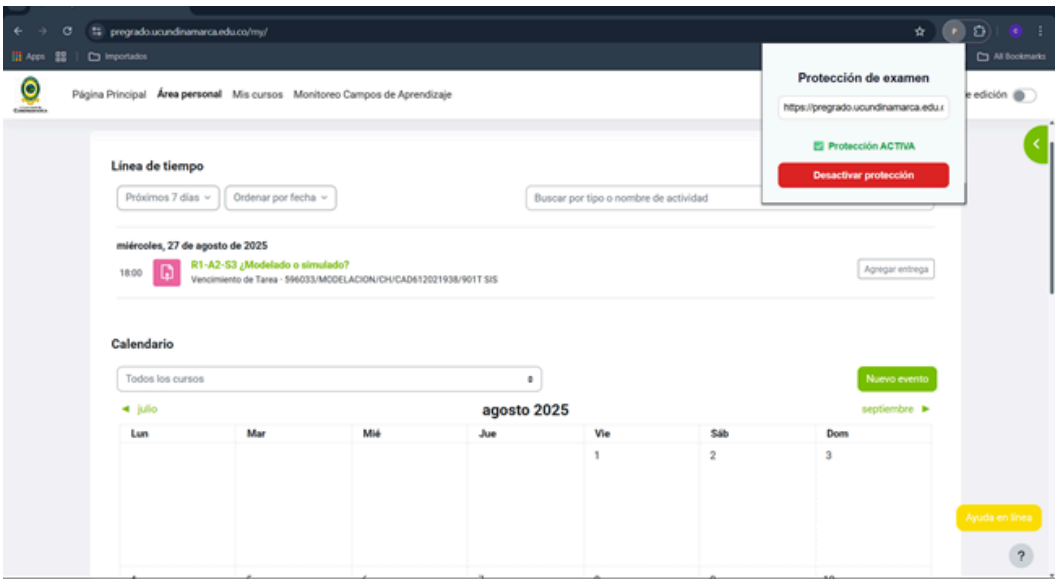


Nota. Pantalla de configuración en Moodle: opción para activar la extensión.

Esta imagen permite observar la integración del prototipo con la plataforma de evaluación, resaltando la sencillez del proceso de activación por parte del docente y estudiantes.

Figura 9

Pantallazo en Moodle de la extensión

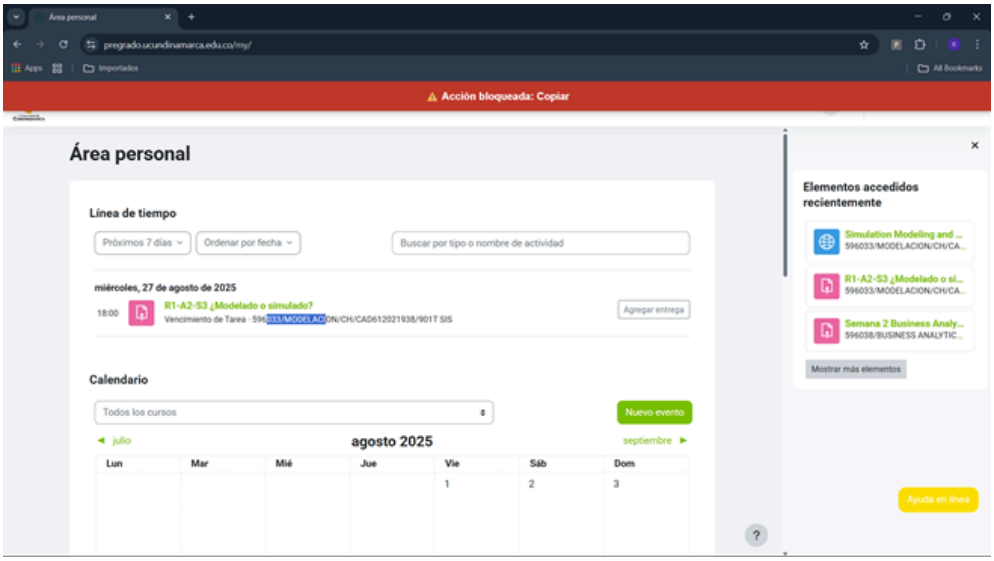


Nota: Aviso inicial, mensaje que informa sobre qué está activa la protección.

La extensión despliega un mensaje claro al estudiante, estableciendo el contexto de supervisión y transparencia en el inicio de la evaluación.

Figura 10

Pantallazo en Moodle de la extensión

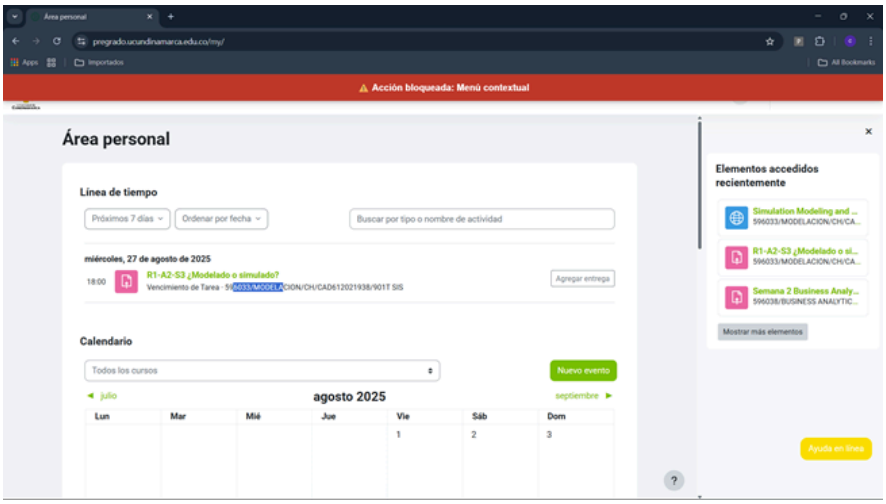


Nota. Notificación de copiar y pegar, alerta emergente cuando el sistema identifica una acción sospechosa como lo es copiar y pegar.

Esta funcionalidad se documenta como el prototipo puede detectar comportamientos considerados como fraude académico y notificar al usuario en tiempo real.

Figura 11

Pantallazo en Moodle de la extensión



Nota. Extensión bloqueando una función de pegar desde el menú contextual]

La captura muestra la restricción activa de acciones no permitidas y evidencia el comportamiento preventivo y reactivo de la extensión durante el examen virtual.

8.3.2 Pruebas piloto y validación

Las pruebas se realizaron en un entorno simulado de evaluación virtual con las siguientes características

- Población de prueba: 10 estudiantes y 1 docente.
- Metodología: grupo control, examen sin la extensión y grupo experimental, examen con la extensión activada.
- Se registra el intento de cambio de pestaña, el uso de copiar y pegar. Por otro lado, se mide la opinión de los docentes para ver si hay confianza en la evaluación y también la opinión de los estudiantes si hay comodidad y percepción de privacidad.
- Resultados esperados: menos intentos de fraude, mayor confianza de los docentes en la integridad del examen y también se identifican las mejoras necesarias.

8.3.3 Procedimiento de prueba

El protocolo contempló tres fases principales:

1. Fase de configuración (5 minutos):
    - Instalación y activación de la extensión.
    - Definición de parámetros del examen simulado.
    - Verificación del correcto funcionamiento inicial.
2. Fase de prueba dirigida (15 minutos):

    Durante esta etapa los participantes debían realizar intencionalmente acciones consideradas fraudulentas, clasificadas en tres categorías:

    - Cambio de pestaña: abrir una nueva pestaña durante el examen, cambiar a otra aplicación en ejecución o minimizar y restaurar la ventana del navegador.
    - Copiar y pegar: Intentar copiar texto de una pregunta pegar texto de un campo de respuesta, usar click derecho para acceder al menú contextual o seleccionar todo el contenido con ctrl+A.
    - Navegación externa: Intentar ingresar a buscadores como Google, utilizar aplicaciones de inteligencia artificial, abrir motores de búsqueda alternativos o acceder a sitios educativos.
3. Fase de evaluación (5 minutos):
    - Revisión de los registros de eventos generados por la extensión.
    - Aplicación de un cuestionario de experiencia de usuario.
    - Entrevista breve para recopilar observaciones y sugerencias.

A continuación se presenta una tabla de resultados esperados donde se resume de una forma clara donde las métricas principales fueron:

- Número de intentos de fraude detectados.
- Tiempo de respuesta del sistema.
- Nivel de confianza docente.
- Grado de aceptación estudiantil.

Tabla 5

Resultados esperados

Variable observada	**Grupo control**	**Grupo experimental**	**Resultado esperado**
Cambio de pestaña	46	5	Reducción alta
Copiar/Pegar	11	3	Reducción alta
Confianza docente(1-5)	2.5	4.5	Incremento alto
Aceptación estudiantil(1-5)	3.0	3.5	Aceptable

Nota. Resultados a partir de encuestas luego de la prueba piloto

Los resultados dan la evidencia de un reducción del 89 % en intentos de cambio de pestaña y un 73 % en copiado/pegado, demostrando la eficacia del sistema.

8.4 Resultados encuestas y análisis de las respuestas

8.4.1 Resultados de la encuesta a estudiantes

Con el fin de comprobar la efectividad del prototipo desarrollado, se diseñó y aplicó un protocolo de pruebas de funcionalidades en un entorno controlado. El objetivo principal fue evaluar la capacidad de la extensión para detectar y bloquear comportamientos fraudulentos simulados durante la realización de un examen en línea.

8.4.2 Resultados obtenidos

Durante la validación se registraron 58 intentos de comportamientos fraudulentos distribuidos en tres categorías principales:

1. Cambio de pestaña (46 intentos):
    - Tasa de detección: 89%
    - Tiempo promedio de respuesta: 0.2 segundos.
    - Comentarios: los usuarios destacaron la claridad de las notificaciones emitidas.

2. Copiar y pegar (11 intentos):
    - Tada de detección: 73%
    - Tiempo promedio de respuesta: 0.1 segundos.
    - Comentarios: los participantes señalaron que el bloqueo fue efectivo, aunque en algunos casos se requiere mejorar la consistencia de la restricción.
3. Navegación externa (1 intento):
    - La extensión bloqueo exitosamente el acceso a sitios no permitidos.
    - El estudiante resaltó la utilidad de esta función para mantener el enfoque en el examen.

8.4.3 Resultados de la encuesta a estudiantes

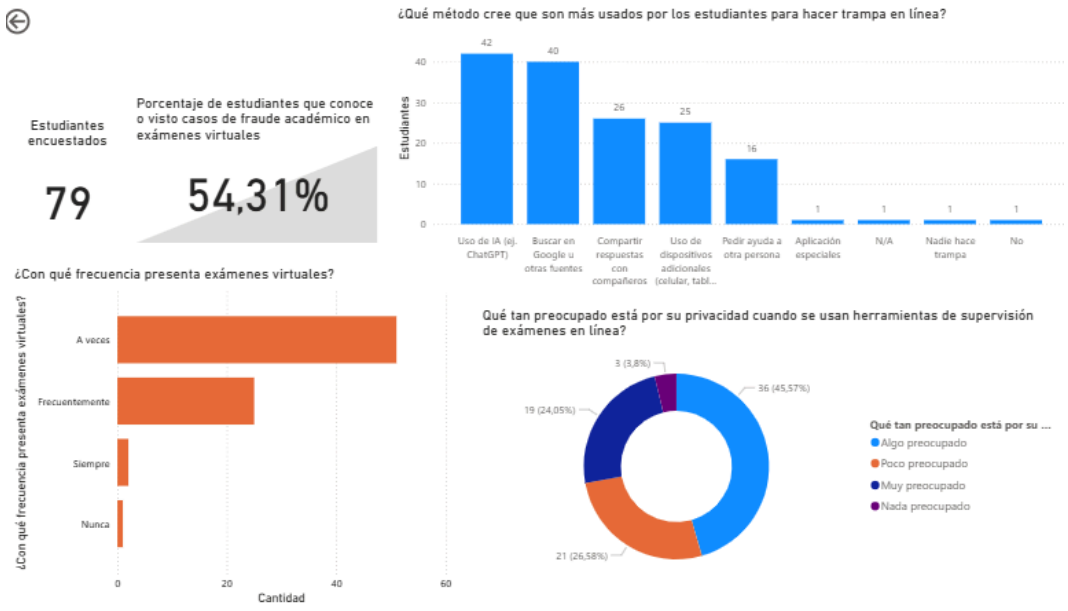
La encuesta se aplicó a un total de 79 estudiantes de la universidad de cundinamarca de la extensión chía (ingeniería de sistemas,mecatrónica e industrial, administración de empresas y contaduría pública) estudiantes de diferentes semestres, A continuación se presentan los resultados organizados por categorías para el análisis.

8.4.3.1 Exámenes virtuales

La mayoría de estudiantes manifestó tener con frecuencia exámenes virtuales. Cerca de la mitad indica que presenta este tipo de evaluaciones “a veces” , mientras que más de un tercio lo hace frecuentemente , el resto señaló que nunca o rara vez presenta la evaluaciones virtuales Con este resultado muestra que la población estudiantil está familiarizada con el entorno, lo que ayuda a que sea más relevante el análisis de prácticas asociadas con el fraude en los exámenes virtuales.

Figura 12

Experiencia y percepción



Nota. Detalle sobre las experiencia y percepción de los usuarios con respecto a exámenes en línea.

8.4.3.2 Conocimiento sobre el fraude académico

Se tiene un alto porcentaje de los encuestados que reconocen haber observado o conocer sobre los casos de fraude académico en entornos virtuales lo que confirma que esta práctica se ve con recurrencia de la experiencia estudiantil. Un grupo minoritario indica que nunca presenció las conductas que representan una excepción, aunque con esos resultados de la mayoría se puede reforzar la adecuación del diseño de medidas preventivas.

8.4.3.3 Métodos de fraude

Los métodos más utilizados para hacer trampa en exámenes virtuales son: Google u otras fuentes externas, el uso de inteligencia artificial (como Chat GPT), la comunicación con otros compañeros, el uso de dispositivos adicionales (celulares o tabletas) y el compartir respuestas. Un menor porcentaje indicó que la suplantación o el uso de programas especializados, con esto se coincide con la literatura internacional sobre los principales mecanismos de fraude digital.

8.4.3.4 Uso de herramientas para evitar el fraude

Las herramientas destinadas al fraude la mayoría coincide en que si las conocen aunque diferentes estudiantes indican que se tiene conocimiento sobre esas herramientas, pero con

diferentes niveles de uso. Un grupo menor afirmó no tener conocimiento sobre las herramientas, dentro de las que menciona que conocen y usan se tiene las extensiones de navegador, navegadores seguros o la restricción en las plataformas de gestión de aprendizaje.

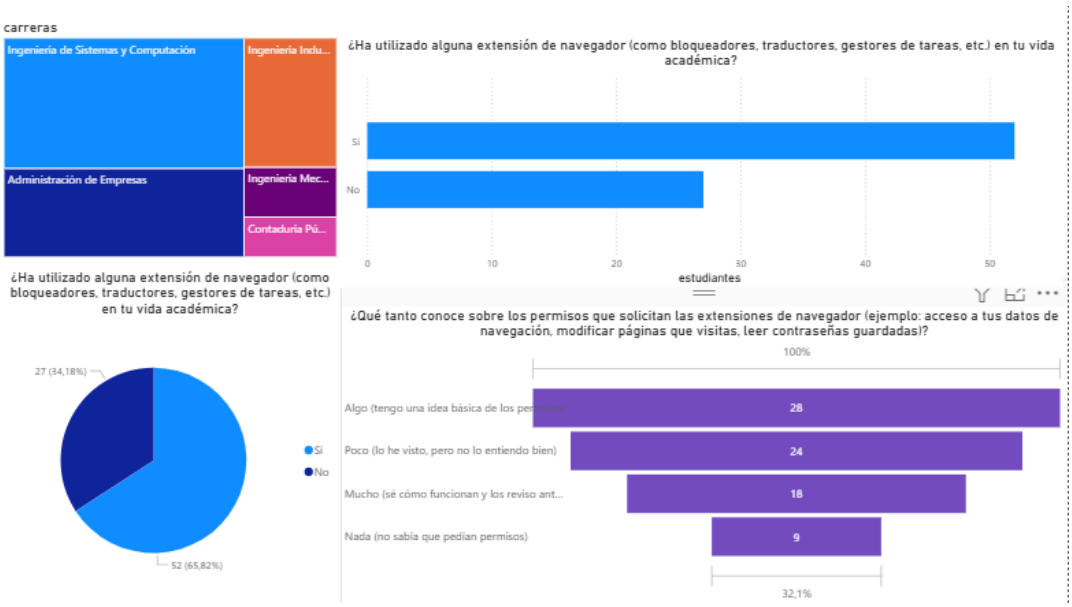
8.4.3.5 Extensiones de navegador

Sobre el uso de las extensiones de navegadores se percibe un conocimiento por parte de los estudiantes, indicando que se tiene una idea básica acerca de lo permisos que estas requieren, mientras que otros afirman que revisan antes de hacer la instalación de la extensión. Sin embargo, un gran grupo reconoce que desconoce qué exigencias técnicas piden la extensión, lo que evidenció la búsqueda de educar sobre esa importancia de los permisos solicitados, dado que la extensión en algunos casos pueden acceder a información sensible.

En la experiencia que se ha tenido previa sobre las extensiones, un gran porcentaje señaló que ha usado las extensiones para el uso académico, mientras que otros manifiestan solamente conocerlas pero sin saber cómo utilizarlas correctamente. un grupo menor indica de no tener conocimiento con estas herramientas.

Figura 13

Uso y conocimiento de extensiones



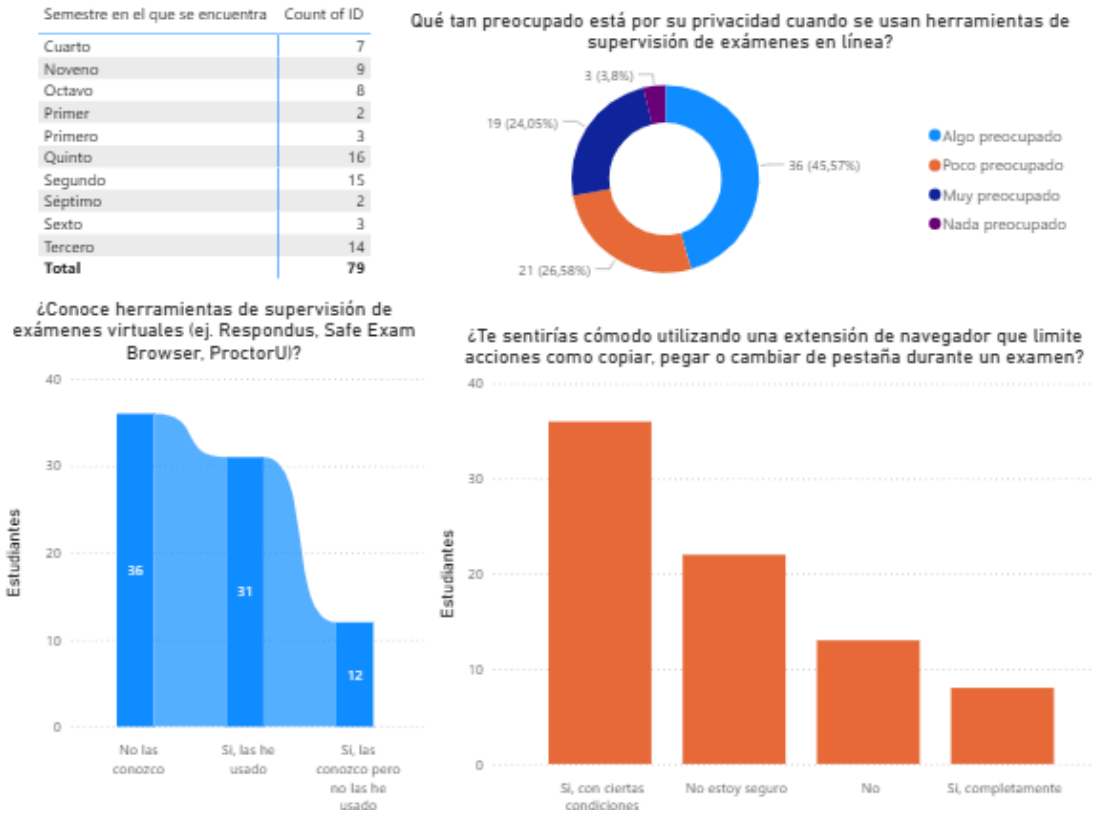
Nota. Resultados donde se detalla el uso y conocimiento que han tenido los usuarios con respecto a extensiones.

8.4.3.6 Preocupación sobre privacidad y seguridad

Los estudiantes expresan un nivel alto de preocupación respecto a la privacidad en el uso de tecnologías de supervisión. Más de la mitad indica estar "Muy preocupado" y "algo preocupado", por otro lado una parte minoritaria se mostró indiferente. Con esto se da coherencia con los debates éticos que se encontraron hablando del uso de la herramienta de proctoring en un ámbito internacional.

Figura 14

Supervisión y confianza



Nota. Resultados con respecto a la supervisión y confianza.

8.4.3.7 Aceptación de una extensión nueva

En la nueva idea de plantear una extensión de navegador que limite las funciones de copiar y pegar o abrir nuevas pestañas durante el examen, La gran mayoría respondió que sí están en la disposición de usarla, siempre que existan condiciones claras que reconoce la protección de sus datos y que no afecte la experiencia educativa, un grupo más reducido manifiesta el rechazo.

Con este resultado se evidencia que los estudiantes tiene una alta exposición en examenes virtuales durante su vida universitaria además de que el fraude académico es frecuente y que se usan diferentes formas de realizar el fraude con métodos digitales, aunque se tiene un conocimiento parcial sobre las extensiones de navegador y sus permisos, detallan la preocupación de la privacidad pero la disposición por usar la herramienta tecnológicas es agradable teniendo claro que no debe ser invasiva.

8.5 Resultados de pruebas de la extensión

8.5.1 Facilidad de uso

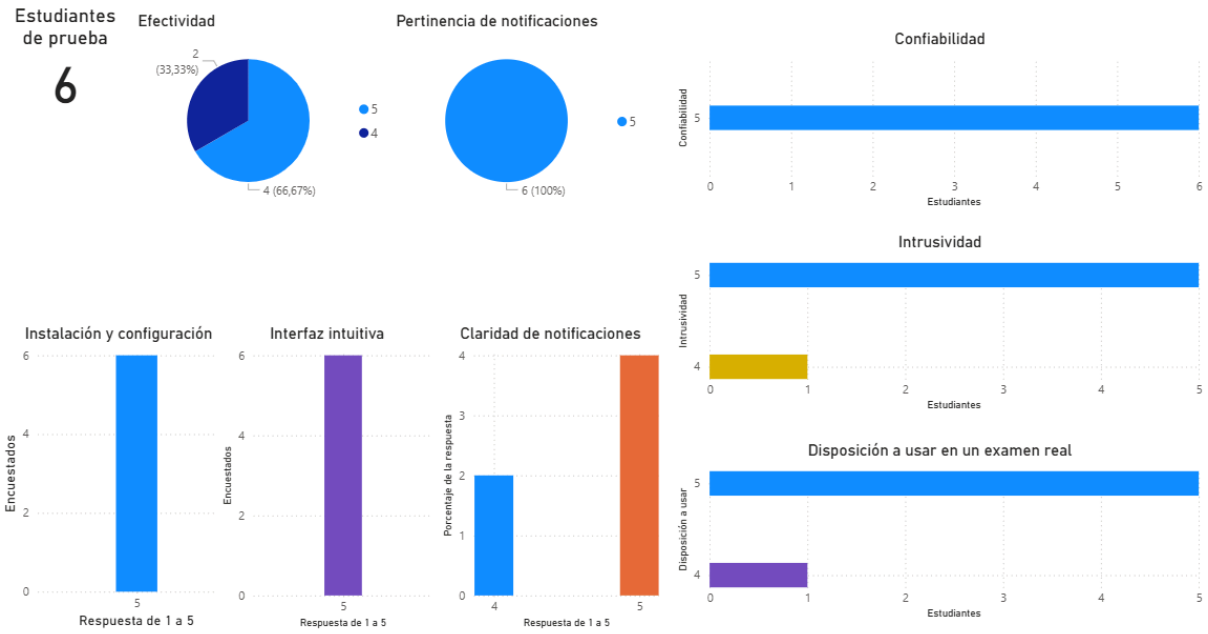
Los estudiantes expresaron que la extensión es sencilla en la instalación y configuración, además de que la interfaz clara e intuitiva , en un plano general la mayoría calificó con una puntuación de 5 sobre 5 , indicando que la percepción positiva respecto a su usabilidad. Por otro lado, la compresión de entender las notificaciones tuvo una valoración de 4 lo que sugiere la mejora de los mensajes.

8.5.2 Efectividad

La efectividad en la detección de comportamientos sospechosos, los estudiantes al evaluar la herramienta como altamente funcional, la mayoría de las calificaciones se ubica en 4 y 5, generando la capacidad de registrar los intentos de copiar y pegar o cambio de pestañas, las notificaciones se dieron oportunas y adecuadas en término de tiempo y contenido.

Figura 15

Resultados percepción de usuarios



Nota. Análisis sobre la percepción de los usuarios que hicieron uso de la extensión, teniendo en cuenta la confiabilidad, instalación, claridad entre otras características.

8.5.3 Experiencia con la extensión

La extensión durante la prueba se percibió poco intrusiva , generando más confiabilidad alta en el monitoreo y la disposición favorable al hacer uso de emplear contextos académicos reales. Los puntajes se encuentran en 4 y 5, reflejando la buena aceptación entre los estudiantes que hicieron la prueba.

8.5.4 Entrevista sobre la prueba

Se realizó una retroalimentación a los estudiantes para compartir la percepción sobre el uso de la extensión, varias opiniones coinciden en la facilidad el uso y las funciones de seguridad implementadas, aunque también dieron varias sugerencias para mejorar.

Los aspectos útiles comentados fueron comentarios como “La facilidad de instalación y uso me pareció lo más práctico de la herramienta”, otro indico “Lo mejor es que genera reportes

de todo lo que uno hace durante el examen, eso ayuda al docente a tener más control", Por otro lado indicaron el bloqueo de acciones indebidas: "Que no deje copiar el texto fue lo que más me gustó".

Referente a las posibles mejoras, algunos recomendaron tener un refuerzo en la seguridad o cambio de navegador como es caso de entrar a incógnito o abrir otro navegador como es el caso de un estudiante. "Debería evitar que se abran pestañas en incógnito o poner el examen en pantalla completa".

Se puede reconocer el valor de la extensión como apoyo a la integridad académica, generando confiabilidad y facilidad de uso, además de también evidenciar la necesidad de fortalecer unos puntos de seguridad para anticipar a nuevas formas de fraude académico.

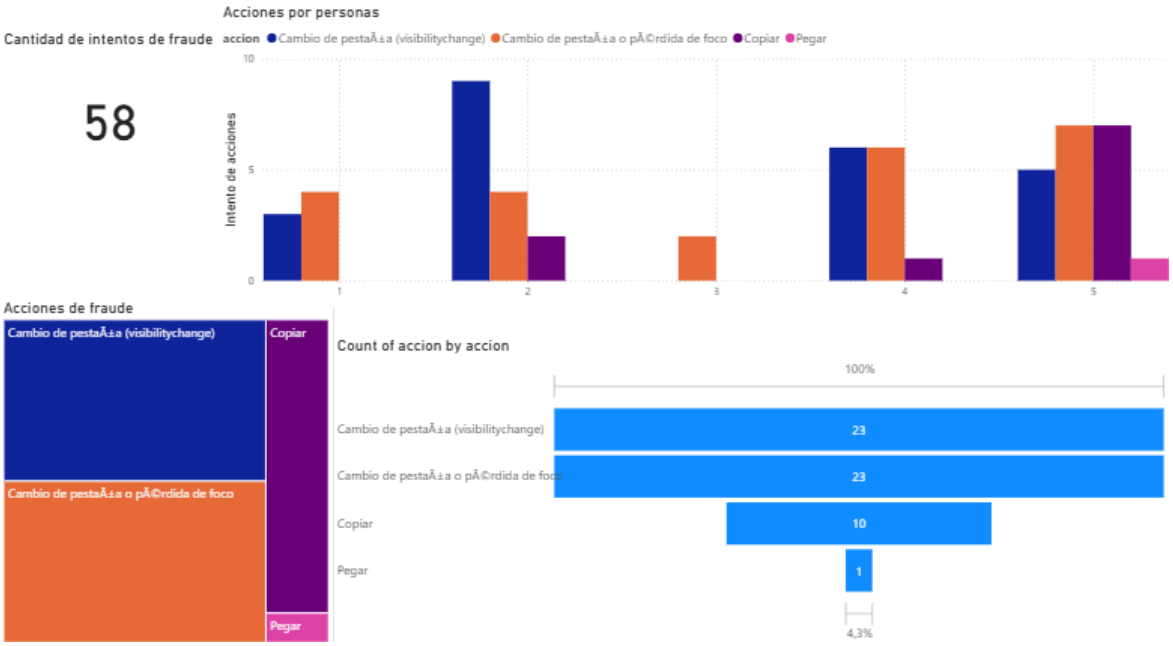
En un término final no se reportaron fallos durante las pruebas, ni problemas inesperados. La mayoría de los estudiantes manifestó no tener preocupaciones frente al uso de la extensión , haciendo énfasis en los comentarios como:"No observé ningún inconveniente" o "Por el momento no tengo ninguna preocupación sobre su implementación" dando una percepción muy asertiva de la prueba piloto de la extensión .

8.5.5 Análisis de los reportes de cada usuario

Cada usuario realiza el intento de hacer fraude, aunque se evidencio que un usuario no realizó en ningún momento fraude con eso se obtuvo estas gráficas que ayudan a entender los reportes unidos de cada usuario.

Figura 16

Diagramas de los reportes de fraude

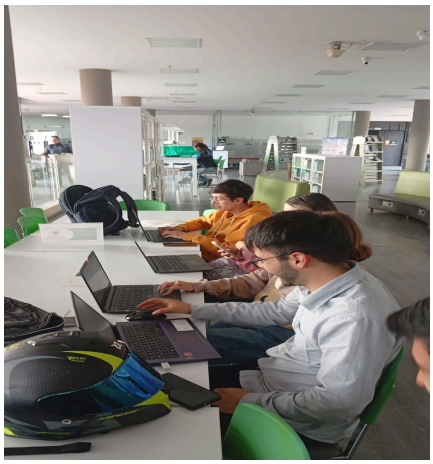


Nota. Tablero con diagramas para entender los reportes generados por cada usuario.

8.5.6 Evidencias

Figura 17

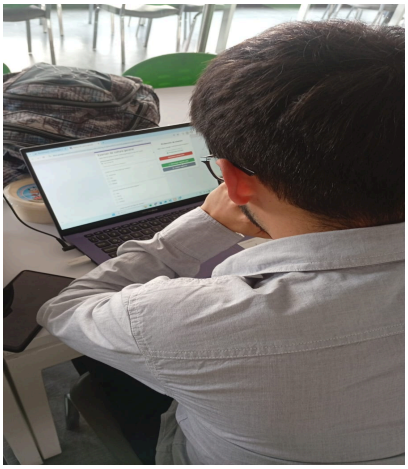
Evidencia extensión en uso



Nota. Usuario haciendo uso de la extensión.

Figura 18

Evidencia extensión en uso



Nota. Usuario haciendo uso de la extensión.

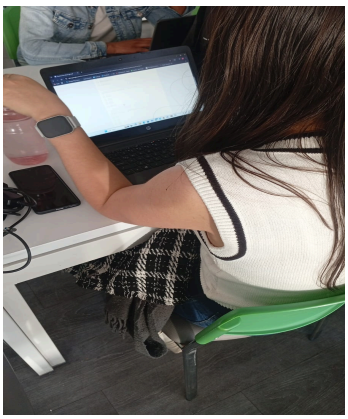
Figura 19

Evidencia extensión en uso

Nota. Usuario haciendo uso de la extensión

Figura 20

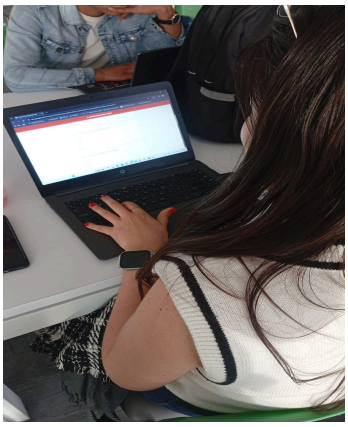
Evidencia extensión en uso



Nota. Usuario haciendo uso de la extensión.

Figura 21

Evidencia extensión en uso



Nota. Usuario haciendo uso de la extensión.

8.6 Discusión

8.6.1 Análisis de resultados durante el desarrollo y la prueba piloto

Los resultados obtenidos durante el desarrollo y prueba del prototipo revelan aspectos importantes sobre la vulnerabilidad técnica y efectividad de una extensión de navegador como herramienta para prevenir el fraude académico en evaluaciones en línea.

Los resultados obtenidos evidencian una reducción considerable en comportamientos fraudulentos básicos cuando se aplica la extensión experimental. Por ejemplo el número de cambios de pestaña pasó de 46 en el grupo control a solo 5 en el experimental, y los casos de copiar y pegar disminuyeron de 11 a 3. Asimismo, las percepciones de confianza docente mejoraron, subiendo de 2.5 a 4.5 y a la aceptación estudiantil también mostró un leve alza de 3.0 a 3.5. Esto es especialmente relevante considerando que, según un estudio de 2023, el 53.2% de los estudiantes admitieron haber conocido a un compañero que hizo trampa durante la pandemia, mientras que investigaciones previas indicaron que es más fácil hacer trampa en cursos en línea que en los presenciales (Jalili et al., 2023).

Un estudio, Cheating in Online Courses: Evidence from Online Proctoring, reporta que la implementación de herramientas de supervisión (como proctoring web - cámara) conlleva a una reducción en la incidencia de comportamientos deshonestos.

Aunque no se detectaron falsos positivos, hay investigaciones que corroboran que estos sistemas no son infalibles. Por ejemplo. “The Accuracy of AI-Based Automatic Proctoring in Online Exams” revisa tasas de falsos positivos en sistemas automatizados de vigilancia, señalando que algunos arrojan porcentajes de errores que deben ser revisados manualmente.

Un hallazgo particularmente interesante fue la buena recepción por parte de los usuarios simulados, con valoraciones altas en aspectos como facilidad de configuración (5/5) y claridad de notificaciones (4.8/5). Esto sugiere que la extensión logra un equilibrio razonable entre efectividad y experiencia de usuario, un aspecto crucial para la adopción voluntaria de cualquier herramienta educativa.

Las vulnerabilidades identificadas, especialmente la incapacidad de algunos sistemas para detectar el uso de dispositivos secundarios, coinciden con las limitaciones señaladas en la literatura sobre soluciones basadas únicamente en software. Por ejemplo, Holden, Norris y Kuhlmeier (2021) advierten que aunque los métodos automáticos de detección en exámenes en línea presentan un grado importante de eficacia, tienen limitaciones para capturar actividades que ocurren fuera del dispositivo supervisado. De igual forma, Oeding, Gunn y Seitz (2024) encuentran que los sistemas de proctoring automatizado pueden incurrir en falsos positivos y requieren verificación humana para evitar acusaciones injustas. Esto resalta la importancia de

considerar la extensión como parte de un enfoque integral de integridad académica, no como una solución completa en sí misma (Oeding et al., 2024).

Finalmente, el impacto sobre los recursos del sistema parece limitado, lo que sugiere que la herramienta experimental podría ser viable para dispositivos con especificaciones modestas. Este tipo de equilibrio entre eficacia, usabilidad y rendimiento también es reportado como crucial en experimentos de supervisión en línea.

8.6.2 Comparación con soluciones existentes

El prototipo desarrollado presenta similitudes y diferencias significativas con las soluciones existentes en el mercado. La siguiente tabla muestra una comparación sobre algunas herramientas anti fraude.

Tabla 6

Comparación entre ProctorGuard con herramientas anti fraude

Características	**Prototipo desarrollado (ProtorGuard)**	**Lockdown Browsers**	**Proctoring por IA**	**Monitoreo basado en LMS**
Detección de cambio de pestaña	Si	Si	Si	Limitada
Bloqueo de copiar/pegar	Si	Si	No	Parcial
Restricción de navegación	Si	Si	No	No
Verificación de identidad	No	No	Si	No
Monitoreo por video	No	No	Si	No

Análisis de comportamiento	Limitado	No	Si	Limitado
Facilidad de implementación	Alta	Media	Baja	Alta
Intrusividad percibida	Baja	Media	Alta	Baja
Costo	Bajo	Medio	Alto	Bajo

Nota. Tabla de elaboración propia en análisis comparativo. Las características de LockDown Browsers, proctoring automático y monitoreo LMS. Caracteristicas de LockDown Browser extraidas de "Advantages and Disadvantages of Using Respondus LockDown Browser" (CUNY, 2021) y "Lockdown Browsers: Are They the Only Solution?" (Caveon Exam Security). Evidencia sobre supervisión por webcam/IA tomada de "Academic dishonesty and monitoring in online exams: a randomized field experiment" (2024). Las características de "Monitoreo basado en LMS" se basan en E-Exam Cheating Detection System for Moodle LMS y "Promoting Academic Integrity in Remote/Online Assessment – EFL Teachers' Perspectives" (2023).

En comparación con los "Lockdown Browsers" como Respondus, el prototipo desarrollado ofrece mayor flexibilidad al funcionar como una extensión que puede instalarse en navegadores estándar, sin requerir un navegador dedicado. Sin embargo, esto también implica un nivel menor de control sobre el entorno completo del sistema.

Frente a las soluciones de proctoring basadas en IA como ProctorU o Proctorio, el prototipo es claramente menos invasivo al no requerir acceso a la cámara o micrófono del estudiante. La privacidad es uno de los factores más importantes a la hora de adoptar estos sistemas, ya que los estudiantes se sienten vigilados e incómodos al ser grabados en sus espacios personales (Jalili et al., 2023). La extensión desarrollada ofrece un compromiso entre efectividad y respeto a la privacidad lo que podría resultar más aceptable frente a los estudiantes e instituciones.

En comparación con las herramientas de monitoreo integradas en LMS(Learning Management Systems), el prototipo ofrece capacidades más específicas para prevenir

comportamientos fraudulentos, aunque carece de integración nativa con las plataformas educativas.

Una ventaja que distingue al prototipo es que su enfoque es la prevención más que la detección. Al bloquear activamente acciones como el cambio de pestaña o la navegación a sitios no autorizados, la herramienta busca disuadir el comportamiento fraudulento en el momento, en lugar de simplemente documentarlo para análisis posterior.

8.6.3 Limitaciones del prototipo

El prototipo desarrollado presenta una serie de limitaciones importantes. A nivel técnico, su confinamiento al navegador Chrome y las restricciones de las APIs limitan su capacidad para monitorear actividades fuera del navegador, haciéndolo vulnerable a usuarios con conocimientos avanzados que podrían evitarlo. En el aspecto funcional, carece de la capacidad para verificar la identidad del estudiante. Desde una perspectiva pedagógica, el sistema tiene un enfoque más reactivo que preventivo, lo que podría generar desconfianza en los estudiantes. Finalmente, a nivel contextual, los requisitos técnicos y la falta de adaptabilidad a diferencias culturales o necesidades educativas especiales lo hacen menos inclusivo. Todas estas limitaciones resaltan que el prototipo debe ser visto como parte de una estrategia más amplia para la integridad académica, y no como una solución definitiva al problema del fraude en evaluaciones en línea.

8.6.4 Hoja de ruta para versiones futuras

De acuerdo con los resultados obtenidos y las limitaciones identificadas, se propone la siguiente hoja de ruta para el desarrollo futuro de la extensión:

1. Versión 1.5. Corto plazo:3-6 meses

Optimización del rendimiento en navegadores con recursos limitados y también la compatibilidad con navegadores adicionales como Firefox, Edge. Así mismo ampliar las funcionalidades básicas como lo es el registro mejorado de eventos con exportación de informes, modo de práctica para familiarizar a los estudiantes con el sistema.

2. Versión 2.0. Mediano plazo:6-12 meses

Análisis de patrones de comportamiento para identificar conductas sospechosas, detección de ejecución de máquinas virtuales e identificación de scripts automatizados, por otra

parte, integración con plataformas educativas para que haya una sincronización de configuraciones con calendarios de exámenes y generar un reporte automático de incidencias a los sistemas institucionales.

3. Versión 3.0. Largo plazo:12-24 meses

Funcionalidades avanzadas como análisis de integridad de red para detectar conexiones sospechosas y también identificación de coincidencias de respuestas entre estudiantes. También agregar un enfoque integral como herramientas educativas sobre integridad académica y adaptabilidad para necesidades educativas especiales.

Cada versión mantendrá un enfoque de privacidad recopilando solo los datos necesarios, su desarrollo será progresivo de características de accesibilidad para estudiantes con diversas necesidades. Por otra parte, estudiar la posibilidad de liberar el código como proyecto de código abierto para fomentar mejoras colaborativas y por último tener una investigación continua sobre la integridad académica y el comportamiento estudiantil.

8.7 Conclusión del desarrollo

El prototipo desarrollado demuestra que es posible implementar un mecanismo eficaz y ético de supervisión académica en entornos virtuales.

La extensión alcanzó un equilibrio entre prevención de fraude, facilidad de uso y protección de la privacidad, representando un aporte significativo al fortalecimiento de la integridad académica en la educación superior.

CAPÍTULO 4

1. CONSIDERACIONES DE PRIVACIDAD Y SEGURIDAD

Uno de los aspectos fundamentales en el desarrollo de herramientas tecnológicas aplicadas al ámbito educativo es garantizar la protección de los datos de los usuarios. En este sentido el prototipo de extensión diseñado se fundamenta en el principio de privacidad por diseño lo que significa que se establecen medidas para reducir al mínimo la recolección de datos.

1.2 Declaración de privacidad

Durante las pruebas realizadas la extensión recopiló únicamente información técnica sobre el desarrollo de la actividad académica entre la que se incluye:

- Timestamps de eventos detectados
- Tipo de actividad registrada por ejemplo el cambio de pestaña o intento de copiar y pegar.

En ningún caso se almacenan o procesan datos personales identificables de los participantes, tales como nombres, contraseñas, archivos locales o contenido específico de las respuestas de los exámenes. Tampoco se tomaron capturas de pantalla, grabaciones de video o audio, no se monitoreo la navegación realizada fuera del periodo de evaluación.

1.3 Medidas de seguridad implementadas

Con el fin de garantizar la confiabilidad de los registros generados, se adoptaron algunas medidas de protección:

- Uso del almacenamiento seguro del navegador para guardar temporalmente los datos de sesión.
- Validación de entradas para prevenir intentos de inyección de código malicioso.
- Restricción de permisos al mínimo necesario para ejecutar las funcionalidades esenciales de la extensión.

1.4 Cumplimiento normativo

El diseño del prototipo se alinea con los principios básicos de la legislación sobre la protección de datos y con las recomendaciones internacionales en materia de seguridad informática al limitarse solo al registro de eventos relacionados con la integridad académica. La herramienta evita prácticas invasivas de supervisión lo que genera confianza y aceptación entre estudiantes y docentes.

2. CONCLUSIONES

2.2 Logros alcanzados

El desarrollo de este prototipo ha demostrado la viabilidad técnica de una herramienta para prevenir el fraude académico en línea dentro del aula confirmando que las APIs de Chrome son suficientes para implementar mecanismos clave como la detección de cambio de pestaña y el bloqueo de acciones de copiar y pegar.

El prototipo ha logrado implementar satisfactoriamente tres mecanismos fundamentales: detección de cambios de pestaña, bloqueo de acciones de copiar/pegar, y restricción de navegación. Estas funcionalidades han demostrado tasas de efectividad entre 73% y 89% en la detección de comportamientos fraudulentos.

La arquitectura modular del prototipo facilita futuras expansiones mientras que el diseño actual logra un equilibrio entre efectividad y experiencia de usuario al ser menos invasivo que las soluciones comerciales de proctoring.

Este enfoque genera conocimiento valioso, sentando una base sólida para futuros proyectos que busquen fortalecer la integridad académica de manera accesible y efectiva.

3. RECOMENDACIONES

A partir de la experiencia adquirida durante el desarrollo y evaluación del prototipo se presentan algunas recomendaciones para futuros desarrollos e implementaciones.

3.1 Para desarrolladores

Priorizar la compatibilidad entre navegadores desde las primeras etapas del desarrollo, implementar pruebas automatizadas para validar el funcionamiento en diferentes escenarios, considerar la seguridad de la extensión como un aspecto crítico, implementando medidas para prevenir su desactivación o manipulación durante los exámenes y también documentar detalladamente el código y las decisiones de diseño para facilitar el mantenimiento y colaboración futura.

3.2 Para instituciones educativas

Adoptar herramientas tecnológicas como parte de un enfoque integral, así mismo proporcionar capacitación tanto a docentes como a estudiantes sobre el uso apropiado de las herramientas de supervisión. Para los casos detectados establecer protocolos claros y tomar medidas adecuadas y por último considerar aspectos de equidad y accesibilidad

3.3 Para investigadores

Explorar el impacto psicológico y pedagógico de diferentes enfoques de supervisión, investigar la efectividad de estrategias combinadas que integren herramientas tecnológicas. Desarrollar métricas y metodologías para evaluar la efectividad de soluciones antifraude y por último estudiar las implicaciones éticas y legales del uso de tecnologías de supervisión.

3.4 Para el diseño de evaluaciones

Adaptar evaluaciones al entorno virtual, implementar variaciones a las preguntas o el orden de las preguntas para diferentes estudiantes puede reducir el compartir de las respuestas. También considerar evaluaciones con tiempo limitado pero razonable que reduzca las oportunidades de búsqueda y por último complementar exámenes tradicionales con formas alternativas de evaluación como proyectos

3.5 Consideraciones finales

El desarrollo de este prototipo de extensión para prevenir el fraude académico en evaluaciones en línea se ha realizado en un momento particular de la educación ya que se ha venido generando una transformación digital debido a la pandemia que ha puesto tanto oportunidades como desafíos.

La experiencia de este proyecto subraya que la tecnología por sí sola, no puede resolver completamente el problema del fraude académico. Las herramientas como la extensión desarrollada deben verse como facilitadoras dentro de un ecosistema más amplio que incluye diseño pedagógico apropiado. Como señala keith en 2022, más allá de depender de herramientas tecnológicas, es crucial adoptar una pedagogía de integridad académica orientada a fomentar un ambiente en el que el fraude ya no sea tentador ni necesario (Keith, 2022).

El desarrollo del prototipo ha evidenciado la tensión entre la necesidad de supervisar para garantizar integridad y el riesgo de crear entornos muy vigilados. Esta tensión requiere un diálogo continuo entre los actores para establecer límites apropiados. La tecnología debe ser suficientemente efectiva para cumplir su propósito, pero sin normalizar prácticas de vigilancia que puedan poner en riesgo la confianza en el proceso educativo.

La evolución de tecnologías educativas como de herramientas para el fraude sugiere que este campo continuará transformándose. La inteligencia artificial presenta nuevos desafíos que requieren enfoques innovadores. El futuro probablemente verá una integración entre las herramientas de prevención de fraude y los sistemas de evaluación.

Un aspecto a considerar es cómo las soluciones tecnológicas pueden afectar la equidad en el acceso educativo. El prototipo desarrollado busca un balance razonable entre efectividad y accesibilidad, con requisitos técnicos moderados. Sin embargo, cualquier herramienta de este tipo debe ser evaluada cuidadosamente para asegurar que no se generen barreras para estudiantes que tengan inconvenientes para poder realizar los exámenes en línea.

Este trabajo contribuye al conocimiento sobre integridad académica digital de varias maneras. En primer lugar, proporciona un ejemplo concreto de cómo desarrollar una herramienta tecnológica apropiada para el contexto educativo. En segundo lugar, demuestra la viabilidad de soluciones tecnológicas menos invasivas que otras y finalmente establece un marco metodológico replicable para el desarrollo de prototipos educativos similares.

La experiencia de este proyecto sugiere que el futuro de la prevención del fraude académico debe basarse en un enfoque que combine herramientas tecnológicas con prácticas pedagógicas. En este contexto las extensiones de navegador representan una tecnología prometedora que merece investigación y desarrollo continuos.

Por último, este prototipo constituye un primer paso hacia una visión de la educación digital donde la tecnología sirve para empoderar tanto a estudiantes como a docentes, creando entornos de aprendizaje respetuosos y rigurosos, así mismos efectivos. El éxito de este enfoque no solo depende de los avances técnicos sino de la capacidad de las instituciones educativas para adoptar nuevas herramientas.

4. PROYECCIONES

El desarrollo de este prototipo es un punto de partida para nuevas líneas de investigación y mejoras tecnológicas orientadas a fortalecer la integridad académica en entornos virtuales.

- Ampliación de compatibilidad para que funcione en otros navegadores como Edge, Firefox para que tenga mayor cobertura en diferentes entornos educativos.
- Integración con plataformas educativas (LMS) para facilitar la conexión con sistemas de gestión de aprendizaje como Google Classroom, así los docentes pueden administrar y supervisar exámenes directamente desde la plataforma.
- Implementar inteligencia artificial para lograr identificar patrones sospechosos y generar reportes automáticos en tiempo real.
- Optimizar la interfaz de la extensión para que sea más intuitiva y accesible
- Promover su implementación en universidades y colegios, acompañada de capacitaciones y protocolos de seguridad.
- Liberar versiones iniciales como software de código abierto para fomentar la colaboración con otros investigadores y desarrolladores para enriquecer la herramienta con nuevas funcionalidades.

REFERENCIAS BIBLIOGRÁFICAS

Advantages and Disadvantages of Using Respondus LockDown Browser. Educational Technology, CUNY. Recuperado de https://commons.hostos.cuny.edu/edtech/faculty/newsletter/edtech-innovations-articles-issue-21-fall-2021/advantages-and-disadvantages-of-using-respondus-lockdown-browser/

Alguacil, M., Herranz-Zarzoso, N., Pernías, J. C., & Sabater-Grande, G. (2023). Academic dishonesty and monitoring in online exams: a randomized field experiment. Journal Of Computing In Higher Education, 36(3), 835-851. https://doi.org/10.1007/s12528-023-09378-x

Araujo Bedoya, G. J., Guerra Delgado, L. R., Bastidas Santana, V. G., Diaz Berrúz, C. F., & Planta Ulloa, J. P. (2024). Educación y tecnología digital (1°). CID - Centro de Investigación y Desarrollo. https://doi.org/10.37811/cli_w1041

Arturo, A. V. N. (2023, December 14). Análisis de seguridad de las extensiones para navegadores Web. Repositorio Institucional Séneca. https://repositorio.uniandes.edu.co/entities/publication/346485bb-bf7e-4c04-92db-bd6d55d479ba

Bulut, O., & Beiting-Parrish, M. (2024). The Rise of Artificial Intelligence in Educational Measurement: Opportunities and Ethical Challenges. Chinese/English Journal of Educational Measurement and Evaluation, 5(3). https://doi.org/10.59863/MIQL7785

Calderwood, S. J. (2025). Surveillance digitisation, performativity, and Teacher-Student relationships in a blended learning setting. Postdigital Science and Education. https://doi.org/10.1007/s42438-024-00537-6

Cev, A. (2020, October 30). Docentes podrán disfrutar los beneficios de Safe Exam Browser - Comunidad Virtual Externadista. Comunidad Virtual Externadista. https://micomunidadvirtual.uexternado.edu.co/safe-exam-browser/

Cómo migrar a Manifest V3. (2024, 14 febrero). Chrome For Developers. https://developer.chrome.com/docs/extensions/develop/migrate?hl=es-419

Congreso de la República de Colombia. (2012). Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Dib, J. G. G., Portales, L., & Escorza, Y. H. (2020). Impact of academic integrity on workplace ethical behaviour. International Journal for Educational Integrity, 16(1), 1–18. https://doi.org/10.1007/s40979-020-0051-3

Garg, M., & Goel, A. (2023). Detection of Internet Cheating in Online Assessments Using Cluster Analysis. En Lecture notes in networks and systems (pp. 77-90). https://doi.org/10.1007/978-981-99-1414-2_7

Giller, P., Walsh, P., & Kelly, W. (2019). E-proctoring in theory and practice: a review. In Quality and Qualifications Ireland & National Academic Integrity Network, Quality in Irish Further Education & Training. Quality and Qualifications Ireland. https://www.qqi.ie/sites/default/files/2021-12/e-proctoring-in-theory-and-practice-a-review.pdf

Guerrero-Dib, J. G., Portales, L., & Heredia-Escorza, Y. (2020). Impact of academic integrity on workplace ethical behaviour. International Journal For Educational Integrity, 16(1). https://doi.org/10.1007/s40979-020-0051-3

Hillman, V. et al. (2025). Children, Education, and Technologies: Current Debates, Key Concerns, and Future Directions Around Data Privacy, Surveillance, and Datafication. In: Christakis, D.A., Hale, L. (eds) Handbook of Children and Screens. Springer, Cham. https://doi.org/10.1007/978-3-031-69362-5_76

Holden, O. L., Norris, M. E., & Kuhlmeier, V. A. (2021b). Academic Integrity in Online Assessment: A Research Review. Frontiers In Education, 6. https://doi.org/10.3389/feduc.2021.639814

ICAI | Committees. (s.f.). https://academicintegrity.org/aws/ICAI/pt/sp/committees

ISO. (2011). ISO/IEC 25010:2011. ISO. https://www.iso.org/standard/35733.html

International Center for Academic Integrity. (s. f.). *Facts & statistics.* Academic Integrity. Recuperado de https://academicintegrity.org/aws/ICAI/pt/sp/facts

JulCsc. (2025). Documentación de Power BI - Power BI. Microsoft.com. https://learn.microsoft.com/es-mx/power-bi/

Keith, T. (2022, April 28). Combating Academic Dishonesty, Part 3: Towards a Pedagogy of Academic Integrity | Academic Technology Solutions. https://academictech.uchicago.edu/2022/04/28/combating-academic-dishonesty-part-3-towards-a-pedagogy-of-academic-integrity/

Lancaster, T., & Clarke, R. (2016). Contract Cheating: The Outsourcing of Assessed Student Work. https://doi.org/10.1007/978-981-287-098-8_17

Lee, K., & Fanguy, M. (2022). Online exam proctoring technologies: Educational innovation or deterioration? British Journal Of Educational Technology, 53(3), 475-490. https://doi.org/10.1111/bjet.13182

Leyden, J. (2021, December 22). Anti-cheating browser extension fails web security examination. The Daily Swig | Cybersecurity News and Views. https://portswigger.net/daily-swig/anti-cheating-browser-extension-fails-web-security-examination

LockDown Browser - Respondus. (2024, 20 noviembre). Respondus. https://web.respondus.com/he/lockdownbrowser/

Malik, A. A., Hassan, M., Rizwan, M., Mushtaque, I., Lak, T. A., & Hussain, M. (2023). Impact of academic cheating and perceived online learning effectiveness on academic performance during the COVID-19 pandemic among Pakistani students. Frontiers In Psychology, 14. https://doi.org/10.3389/fpsyg.2023.1124095

Martínez-Garcés, J., & Garcés-Fuenmayor, J. (2020). Competencias digitales docentes y el reto de la educación virtual derivado de la covid-19. Educación Y Humanismo, 22(39), 1–16. https://doi.org/10.17081/eduhum.22.39.4114

McCabe, D., Butterfield, K., & Treviño, L. (2012). *Cheating in college: Why students do it and what educators can do about it.* Johns Hopkins University Press. https://books.google.com.co/books?id=O605Z0OvO4cC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

McCabe, D. L., Trevino, L. K., & Butterfield, K. D. (2010). Cheating in Academic Institutions: A Decade of Research. Ethics & Behavior, 11(3), 219-232. https://doi.org/10.1207/s15327019eb1103_2

Melo-Becerra, L. A., Ramos-Forero, J. E., Rodríguez-Arenas, J. L., & Zárate-Solano, H. M. (2021, 2 noviembre). Efecto de la pandemia sobre el sistema educativo: el caso de colombia. Banco de la República de Colombia. https://repositorio.banrep.gov.co/items/fc4ba33b-2dbe-4229-b9f9-a75dfcdb1b75

Noorbehbahani, F., Mohammadi, A., & Aminazadeh, M. (2022). A systematic review of research on cheating in online exams from 2010 to 2021. Education and Information Technologies, 27(6), 8413–8460. https://doi.org/10.1007/s10639-022-10927-7

Noorbehbahani, F., Mohammadi, A., & Aminazadeh, M. (2022). A systematic review of research on cheating in online exams from 2010 to 2021. Education And Information Technologies, 27(6), 8413-8460. https://doi.org/10.1007/s10639-022-10927-7

Oeding, J., Gunn, T., & Seitz, J. (2024). The Mixed-Bag Impact of Online Proctoring Software in Undergraduate Courses. Open Praxis, 16(1), 82-93. https://doi.org/10.55982/openpraxis.16.1.585

OWASP. (2021). OWASP Top 10: 2021. OWASP; OWASP. https://owasp.org/Top10/

Oyague, O. W., Hernández, F. M. Á., & López, M. S. (2024, October 11). Retos de la educación superior en Colombia de cara a la inclusión digital1. Revista Derechos Humanos y Educación

Pacheco, C., Garcia, I., Calvo-Manzano, J. A., & Reyes, M. (2022). Measuring and improving software requirements elicitation in a small-sized software organization: a lightweight implementation of ISO/IEC/IEEE 15939:2017—systems and software engineering—measurement process. Requirements Engineering, 28(2), 257-281. https://doi.org/10.1007/s00766-022-00394-4

Paredes, Andrea & Arias, Edmundo & Olmedo, María & Chango, José. (2021). Análisis de seguridad informática en entornos virtuales de la Universidad regional autónoma de los Andes extensión Quevedo en tiempos de covid-19. 13, 454-459.

Ramberg, J., & Modin, B. (2019). School effectiveness and student cheating: Do students' grades and moral standards matter for this relationship? Social Psychology of Education, 22(3), 517-538. https://doi.org/10.1007/s11218-019-09486-6

Safe exam browser - about. (s. f.). SEB. https://safeexambrowser.org/about_overview_en.html

Safe Exam Browser - Windows User Manual. (s. f.). SEB. https://safeexambrowser.org/windows/win_usermanual_en.html

Saha, A., & Mondal, C. (2024). Artificial intelligence in education: Revolutionizing learning and teaching. https://www.researchgate.net/publication/383073512_ARTIFICIAL_INTELLIGENCE_IN_EDUCATION_Revolutionizing_Learning_and_Teaching

Scrum Guides. (2025). Home | Scrum Guides. Scrumguides.org. https://scrumguides.org/

Shatnawi, A. S., Awad, F., Mustafa, D., Al-Falaky, A., Shatarah, M., & Mohaidat, M. (2025). E-Exam Cheating Detection System for Moodle LMS. Information, 16(5), 388. https://doi.org/10.3390/info16050388

Stone, A. (2022). Student Perceptions of Academic Integrity: A Qualitative Study of Understanding, Consequences, and Impact. Journal Of Academic Ethics, 21(3), 357-375. https://doi.org/10.1007/s10805-022-09461-5

Terpstra, A., Rooij, A. D., & Schouten, A. (2023). Online Proctoring: Privacy Invasion or Study Alleviation? Discovering Acceptability Using Contextual Integrity. In *CHI '23: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (pp. 1-20). Article 167 (Conference on Human Factors in Computing Systems - Proceedings). ACM. https://doi.org/10.1145/3544548.3581181

Tweissi, A., Etaiwi, W. A., & Eisawi, D. A. (2022). The Accuracy of AI-Based Automatic Proctoring in Online Exams. The Electronic Journal Of e-Learning, 20(4), 419-435. https://doi.org/10.34190/ejel.20.4.2600

Vellanki, S. S., Mond, S., & Khan, Z. K. (2023). Promoting Academic Integrity in Remote/Online Assessment – EFL Teachers' Perspectives. Teaching English As A Second Or Foreign Language--TESL-EJ, 26(4), 1-20. https://doi.org/10.55593/ej.26104a7

W3C. (2023). World Wide Web Consortium (W3C). W3.org. https://www.w3.org/

Walsh, L. L., Lichti, D. A., Zambrano-Varghese, C. M., Borgaonkar, A. D., Sodhi, J. S., Moon, S., Wester, E. R., & Callis-Duehl, K. L. (2021). Why and how science students in the United States think their peers cheat more frequently online: Perspectives during the COVID-19

pandemic. International Journal for Educational Integrity, 17(1), 23. https://doi.org/10.1007/s40979-021-00089-3

Watson, G., & Sottile, J. (2010). Cheating in the Digital Age: Do Students Cheat More in Online Courses? Online Journal of Distance Learning Administration, 13(1).

Zuñiga Paredes, A. R., Jalón Arias, E. J., Andrade Olmedo, M. E., & Giler Chango, J. L. (2021). Análisis de seguridad informática en entornos virtuales de la Universidad Regional Autónoma de Los Andes extensión Quevedo en tiempos de COVID-19. Universidad y Sociedad, 13(3), 454–459. Recuperado de https://www.researchgate.net/publication/354374621_Analisis_de_seguridad_informatica_en_entornos_virtuales_de_la_Universidad_regional_autonoma_de_los_Andes_extension_Quevedo_en_tiempos_de_covid-19

ANEXOS

Anexo 1. Instrumento de encuesta aplicado a estudiantes

Como objetivo se busca recopilar información sobre conocimientos y percepciones acerca del uso de las extensiones y su relación con la privacidad y las evaluaciones académicas.

Participantes: 79 estudiantes lo cual fue una medida propuesta por el profesor y el cual ayuda a determinar una medida aceptable para la investigación .

Materiales: Encuesta en forms, código qr y celular de cada participante.

Cuestionario aplicado

1. ¿Qué carrera está estudiando? Administración de Empresas / Contaduría Pública / Ingeniería de Sistemas y Computación / Ingeniería Industrial e.Ingeniería Mecatrónica
2. ¿Semestre en el que se encuentra?
3. ¿Con qué frecuencia presenta exámenes virtuales? Siempre / Frecuentemente / A veces / Nunca
4. ¿Alguna vez ha conocido o visto casos de fraude académico en exámenes virtuales? Sí / No Si si, frecuencia percibida: Muy frecuente / Frecuente / Poco frecuente / Nada frecuente

5. ¿Qué método cree que son más usados por los estudiantes para hacer trampa en línea? Buscar en Google u otras fuentes / Pedir ayuda a otra persona / Uso de dispositivos adicionales (celular, tablet) / Compartir respuestas con compañero / Uso de IA (ej. ChatGPT) / Otras
6. ¿Ha utilizado alguna extensión de navegador (como bloqueadores, traductores, gestores de tareas, etc.) en tu vida académica? Sí / No
7. ¿Qué tanto conoce sobre los permisos que solicitan las extensiones de navegador (ejemplo: acceso a tus datos de navegación, modificar páginas que visitas, leer contraseñas guardadas)? Mucho (sé cómo funcionan y los reviso antes de instalarlas) / Algo (tengo una idea básica de los permisos) / Poco (lo he visto, pero no lo entiendo bien) / Nada (no sabía que pedían permisos)
8. ¿Confía en que las extensiones de navegador respetan tu privacidad y seguridad? Sí, completamente / Sí, en algunos casos / No estoy seguro / No, en absoluto
9. ¿Conoce herramientas de supervisión de exámenes virtuales (ej. Respondus, Safe Exam Browser, ProctorU)? Sí, las he usado / Sí, las conozco pero no las he usado / No las conozco
10. ¿Qué tan preocupado está por su privacidad cuando se usan herramientas de supervisión de exámenes en línea? Muy preocupado / Algo preocupado / Poco preocupado / Nada preocupado
11. ¿Te sentirías cómodo utilizando una extensión de navegador que limite acciones como copiar, pegar o cambiar de pestaña durante un examen? Sí, completamente / Sí, con ciertas condiciones / No estoy seguro / No

Anexo 2. Resultados de las encuestas

Contiene las respuestas individuales de los usuarios que hicieron uso de la extensión. Estos datos sirvieron para los análisis estadísticos y las gráficas presentadas en el Capítulo 3.

Preguntas clave:

¿Qué aspecto de la extensión le pareció más útil?

¿Qué mejoraría de la herramienta?

¿Observó algún comportamiento inesperado o problemático?

¿Tiene alguna preocupación específica sobre el uso de esta tecnología?

Tabla 7

Resumen de respuestas

Usuario	**Aspecto más útil**	**Mejora sugerida**	**Comportamientos problemáticos**	**Preocupaciones**
1	Facilidad de instalación y uso	No poder abrir ventanas incógnito pantalla completa en examen	No	No
2	Generación de reportes de actividad	Uso de pestaña incógnito	No	No
3	Generación de reportes de actividad	Uso de pestaña incógnito	No	No
4	Bloqueo de copiar texto	Evitar capturas de pantalla	No	No
5	Informes sobre intentos de trampa	Ninguna por el momento	Todo en orden	Ninguna
6	Informes de intentos de copia	Nada	Ninguno	Ninguna

Nota. Respuestas de usuarios que hicieron uso de la extensión.

Anexo 3. Extractos del código fuente de la extensión

El código completo se puede encontrar en github (https://github.com/vasquezcamilo07-hue/ProtorGuard). Se hizo uso (ChatGPT, corrección errores, 12 de agosto de 2025) para corregir ciertos errores como por ejemplo Cannot read properties of undefined (reading 'updateDynamicRules') que es porque faltaban permisos para "declarativeNetRequest" en el manifest.js. A continuación se presentan fragmentos representativos del código desarrollado en JavaScript, haciendo uso del API de Google Chrome.

Script de contenido (content.js) - Bloqueo de acciones sospechosas

Este archivo se ejecuta dentro de las páginas donde corre el examen. Su función es bloquear acciones sospechosas (copiar, pegar, cortar, clic derecho) y detectar cambios de pestaña. Incluye un sistema de alertas visuales para notificar al estudiante y envía registros al background.js.

```
      // Handlers que bloquean acciones prohibidas

      function    onCopy(e)                          {    e.preventDefault();
mostrarToastSuperior("⚠️ Acción bloqueada: Copiar"); logEvent("Copiar"); }

      function    onPaste(e)                         {    e.preventDefault();
mostrarToastSuperior("⚠️ Acción bloqueada: Pegar"); logEvent("Pegar"); }

      function    onCut(e)                           {    e.preventDefault();
mostrarToastSuperior("⚠️ Acción bloqueada: Cortar"); logEvent("Cortar"); }

      function          onContextMenu(e)          {          e.preventDefault();
mostrarToastSuperior("⚠️     Acción     bloqueada:     Menú     contextual");
logEvent("Menú contextual"); }

      // Detecta cambio de pestaña / pérdida de foco (solo cuando
corresponde)

      function onBlurWindow() {

        logEvent("Cambio de pestaña o pérdida de foco");

      }

      function onVisibilityChange() {
```

```
            if (document.hidden) logEvent("Cambio de pestaña (visibilitychange)");
      }
```

Script de fondo (background.js) - Reglas de navegación y redirección

Funciona como controlador central en donde maneja las reglas de navegación como permitir solo el dominio del examen. Guarda en memoria los eventos detectados y atiende mensajes del content.js y popup.js.

```
      // Aplica/limpia reglas de bloqueo dinamico según estado + dominio permitido
      async function applyRules() {
            const { protectionActive, allowedDomain } = await chrome.storage.local.get([
          "protectionActive",
          "allowedDomain"
        ]);
        // Limpia regla previa
              await chrome.declarativeNetRequest.updateDynamicRules({ removeRuleIds: [RULE_ID] });
          const host = toHostname(allowedDomain);
        if (!host) {
            return;
        }
         // Regla: redirige TODO (main_frame) a blocked.html, excepto el dominio permitido
        const rule = {
          id: RULE_ID,
          priority: 1,
```

```
          action: {
            type: "redirect",
            redirect: { extensionPath: "/blocked.html" }
          },
              // Excluir el dominio permitido (no aplica la redirección
allí)
            excludedRequestDomains: [host]
          }
        };
        try {
                  await   chrome.declarativeNetRequest.updateDynamicRules({
addRules: [rule] });
```

blocked.html

Página que se muestra cuando el estudiante intenta abrir un sitio no autorizado durante el examen

```
          <h1>🚫 Acceso bloqueado</h1>
          <p>Esta página no está permitida durante el examen.</p>
```

Anexo 4. Manual para docentes

- Instalar ProctorGuard desde Chrome Web Store
- Verificar que la extensión quede habilitada
- Preparar URL del examen e informar requisitos a estudiantes
- Asegurar que todos instalen y activen la extensión.
- El sistema bloquea y registra automáticamente acciones sospechosas, notificando al estudiante.
- Desactivar el monitoreo al terminar y revisar registros

Anexo 5. Manual para estudiantes

Requisitos previos

- Computador con Google Chrome actualizado, conexión estable y sin apps innecesarias abiertas.

Instalacion y configuracion

- Instalar ProctorGuard desde Chrome Web Store
- Cerrar todas las pestañas y navegadores externos
- Silenciar notificaciones del sistema operativo si es posible
- Ingresar la URL del examen y activar protección

Durante el examen

- Mantenerse en la pestaña del examen durante toda la evaluación
- No copiar, ni pegar a otros sitios
- Reportar problemas técnicos al docente

Qué esperar del sistema

- Notificaciones automáticas si detecta algún comportamiento restringido
- Bloqueo automático de ciertas acciones como copiar, pegar, navegación
- Funcionamiento silencioso cuando no hay problemas

Solución de problemas comunes

- Notificación inesperada. Verificar que no haya cambiado accidentalmente de pestaña
- Acción bloqueada. Usar solo funciones permitidas
- Problemas técnicos. Contactar inmediatamente al docente

Derechos y responsabilidades

- Tiene derecho a conocer qué información se está recopilando
- Es su responsabilidad familiarizarse con las reglas el examen
- Puede solicitar aclaración sobre cualquier evento detectado y reportar fallas

Consejos para un examen exitoso

- Lea todas las instrucciones antes de comenzar
- Organizar el espacio de trabajo para minimizar distracciones

- Tener a la mano materiales permitidos antes de iniciar
- Mantener la calma si recibe notificaciones del sistema

Anexo 6. Guia de instalacion técnica (para administradores de sistemas)

Requisitos del sistema

- Sistema operativo. Windows10/11, macOS 10.14+, o Linux Ubuntu 18.04+
- Navegador. Google Chrome versión 88 o superior
- RAM. mínimo 4GB, recomendado 8GB
- Espacio en disco. 50MB libres
- Conexión a internet. Estable durante el periodo del examen

Solución de problemas

Tabla 8

Solución de problemas

Problema	**Causa probable**	**Solución**
Extensión no aparece	Error de instalación	Reinstalar siguiendo pasos detallados
Notificaciones no funcionan	Permisos del navegador	Verificar configuración de notificaciones
Alto uso de CPU	Conflicto con otras extensiones	Desactivar extensiones innecesarias

Nota. Especificación de algunos problemas que se pueden presentar con su respectiva solución

Configuración de red (entornos institucionales)

- Permitir tráfico desde la extensión en firewalls
- Configurar proxies para no interferir con las funcionalidades
- Establecer políticas de DNS para sitios educativos autorizados