



**UNIVERSIDAD TECNOLÓGICA ISRAEL**  
**ESCUELA DE POSGRADOS “ESPOG”**

**MAESTRÍA EN SEGURIDAD INFORMÁTICA**

*Resolución: RPC-SO-02-No.053-2021*

**PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER**

<b>Título del proyecto:</b>
Evaluación de la Seguridad en Aplicaciones PWAs conforme a ISO 27001:2022 y NIST SP 800-53: Un Enfoque Integral para la Identificación y Mitigación de Vulnerabilidades
<b>Línea de Investigación:</b>
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
<b>Campo amplio de conocimiento:</b>
Tecnologías de la Información y la Comunicación (TIC)
<b>Autor/a:</b>
Ing. Xavier Alejandro Diaz Paucar
<b>Tutor/a:</b>
Mg. Renato Toasa PhD. Maryory Urdaneta

**Quito – Ecuador**

**2024**

## APROBACIÓN DEL TUTOR



Yo, Mg. Renato Mauricio Toasa Guachi con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: Evaluación de la Seguridad en Aplicaciones PWAs conforme a ISO 27001:2022 y NIST SP 800-53: Un Enfoque Integral para la Identificación y Mitigación de Vulnerabilidades.

Elaborado por: Xavier Alejandro Diaz Paucar, de C.I: 1709491359, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2024



Firmado electrónicamente por:  
**RENATO MAURICIO  
TOASA GUACHI**

---

**Firma**

## APROBACIÓN DEL TUTOR



Yo, PhD. Maryory Urdaneta con C.I: 1759316126 en mi calidad de Tutor del proyecto de investigación titulado: Evaluación de la Seguridad en Aplicaciones PWAs conforme a ISO 27001:2022 y NIST SP 800-53: Un Enfoque Integral para la Identificación y Mitigación de Vulnerabilidades.

Elaborado por: Xavier Alejandro Diaz Paucar, de C.I: 1709491359, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., septiembre de 2024



Firma

## DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE



Yo, Xavier Alejandro Diaz Paucar con C.I: 170949135-9, autor/a del proyecto de titulación denominado: Evaluación de la Seguridad en Aplicaciones PWAs conforme a ISO 27001:2022 y NIST SP 800-53: Un Enfoque Integral para la Identificación y Mitigación de Vulnerabilidades. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., septiembre de 2024



Firmado electrónicamente por:  
XAVIER ALEJANDRO  
DIAZ PAUCAR

---

**Firma**

## Tabla de contenidos

APROBACIÓN DEL TUTOR .....	2
APROBACIÓN DEL TUTOR .....	3
DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE .....	4
INFORMACIÓN GENERAL .....	4
Contextualización del tema.....	4
Problema de investigación.....	6
Objetivo general.....	7
Objetivos específicos.....	7
Vinculación con la sociedad y beneficiarios directos:.....	7
CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO .....	10
1.1.    Contextualización general del estado del arte.....	10
1.2.    Proceso investigativo metodológico .....	14
1.3.    Análisis de resultados .....	15
CAPÍTULO II: PROPUESTA.....	35
2.1.    Fundamentos teóricos aplicados.....	35
2.2.    Descripción de la propuesta .....	38
2.3.    Validación de la propuesta .....	48
2.4.    Matriz de articulación de la propuesta .....	49
CONCLUSIONES.....	51
RECOMENDACIONES.....	52
BIBLIOGRAFÍA.....	53
ANEXOS .....	55

## Índice de tablas

Tabla 1. Mapeo de Controles entre ISO 27001 y NIST 800-53 .....	36
Tabla 2. Matriz de Vulnerabilidades en PWAs.....	45
Tabla 3. Matriz de Vulnerabilidades en PWAs (continuación) .....	46
Tabla 4. Matriz de articulación .....	49

## Índice de figuras

Figura 1. Estructura arquitectónica general de una Progressive Web App .....	10
Figura 2. Nueve Prácticas de seguridad en aplicaciones PWAs .....	12
Figura 3. La Triada de la Seguridad Informática .....	13
Figura 4. Pregunta No. 1 .....	16
Figura 5. Pregunta No. 2 .....	17
Figura 6. Pregunta No. 3 .....	19
Figura 7. Pregunta No. 4 .....	21
Figura 8. Pregunta No. 5 .....	23
Figura 9. Pregunta No. 6 .....	25
Figura 10. Pregunta No. 7 .....	27
Figura 11. Pregunta No. 8 .....	29
Figura 12. Pregunta No. 9 .....	31
Figura 13. Pregunta No. 10 .....	33
Figura 14. Proceso de Evaluación y Mitigación de Vulnerabilidades en Aplicaciones Web Progresivas ...	39

## INFORMACIÓN GENERAL

### Contextualización del tema

En la actualidad, las Progressive Web Applications (PWAs) han ganado una creciente popularidad como una alternativa versátil y eficaz a las aplicaciones nativas (Thakur, 2018, p. 4). Estas aplicaciones web progresivas ofrecen a los usuarios experiencias similares a las aplicaciones móviles, con ventajas notables en términos de accesibilidad, facilidad de distribución y costos de desarrollo reducidos (Bukhtinova, 2023). Sin embargo, a medida que el uso de PWAs continúa en aumento, surge una preocupación crítica: la seguridad informática.

Las PWAs, al ser aplicaciones web, están expuestas a una amplia gama de amenazas de seguridad. Estas amenazas pueden manifestarse de diversas maneras, desde vulnerabilidades comunes como “Cross-Site Scripting (XSS)” y “Cross-Site Request Forgery (CSRF)” hasta la exposición de datos sensibles y la falta de cumplimiento de regulaciones de privacidad. La seguridad de las PWAs es una preocupación clave, dado que estas aplicaciones manejan datos de usuario y a menudo se utilizan para realizar transacciones en línea (Chinprutthiwong et al., 2020, Sección 2).

La falta de un enfoque integral para abordar la seguridad en las PWAs puede tener consecuencias graves, como la exposición de datos confidenciales de usuarios, la pérdida de confianza del cliente como lo indica Radu (2023) “dado que las PWAs son esencialmente aplicaciones basadas en web, existe la preocupación de que no ofrezcan el mismo nivel de seguridad que las aplicaciones nativas. Esta falta de seguridad puede ser una barrera para los usuarios preocupados por proteger su información personal” y posibles sanciones legales por incumplimiento de regulaciones de privacidad como lo indica el Artículo 37 de la Ley Orgánica de Protección de Datos (2021) . Además, la seguridad deficiente puede socavar la experiencia del usuario y afectar la adopción general de las PWAs (Rensema, 2020, p. 9).

Para abordar este problema, es esencial llevar a cabo investigaciones en profundidad y desarrollar estrategias de seguridad efectivas específicamente adaptadas a las PWAs. En este escenario se sitúa el proyecto de titulación actual, el cual busca analizar y potenciar la seguridad de las PWAs, empleando marcos de referencia reconocidos a nivel global como ISO 27001:2022 y NIST SP 800-53. Al hacerlo, se busca no solo identificar y mitigar vulnerabilidades, sino también garantizar el cumplimiento normativo y proporcionar orientación valiosa a desarrolladores y organizaciones que buscan aprovechar al máximo estas aplicaciones web progresivas de próxima generación.



La seguridad de las PWAs ha cobrado una relevancia creciente en el contexto actual, donde la digitalización ha transformado la forma en que las organizaciones interactúan con sus clientes y empleados. La creciente adopción de las PWAs, tanto en entornos empresariales, ha puesto de manifiesto la necesidad de garantizar su seguridad para proteger la información confidencial y prevenir ataques cibernéticos. Este trabajo de investigación se centra en evaluar la seguridad de las PWAs desde una perspectiva administrativa y tecnológica, con el objetivo de identificar las vulnerabilidades más comunes y proponer medidas de mitigación basadas en estándares internacionales como ISO 27001:2022 y NIST SP 800-53. Los resultados de esta investigación contribuirán a mejorar la seguridad de las aplicaciones web progresivas y a fomentar la confianza de los usuarios en este tipo de soluciones.

El desarrollo de PWAs se sustenta en un ecosistema tecnológico en constante evolución. A continuación, se detallan los principales componentes y tecnologías involucradas en el entorno tecnológico:

#### Lenguajes de programación:

- HTML, CSS y JavaScript: La triada fundamental para la construcción de cualquier página web, incluyendo las PWAs.
- Frameworks y librerías: React, Angular, Vue.js, entre otros, simplifican el desarrollo y ofrecen funcionalidades adicionales.
- TypeScript: Un superconjunto de JavaScript que agrega tipado estático para mejorar la mantenibilidad y escalabilidad del código.

#### Herramientas de desarrollo:

- Editores de código: Visual Studio Code, Sublime Text, Atom, ofrecen funcionalidades avanzadas para la escritura y depuración de código.
- Herramientas de compilación: Webpack, Parcel, facilitan la gestión de módulos y la optimización del código.
- Emuladores y simuladores: Permiten probar las PWAs en diferentes dispositivos y sistemas operativos como por ejemplo el uso del navegador web Chrome.

#### APIs y servicios:

- Web APIs: Geolocalización, notificaciones push, almacenamiento local, entre otras, proporcionan funcionalidades nativas a las PWAs.
- Backend: Node.js, Python (Flask, Django), PHP (Laravel), Java (Spring), para la lógica del servidor y la gestión de datos.

- Bases de datos: SQL (MySQL, PostgreSQL), NoSQL (MongoDB), para almacenar y gestionar la información.

Herramientas de pruebas:

- Pruebas unitarias: Jest, Mocha, para asegurar la calidad del código a nivel de componentes.
- Pruebas de integración: Cypress, Selenium, para probar la interacción entre diferentes componentes de la aplicación.
- Pruebas de rendimiento: Lighthouse (auditoria de aplicaciones), WebPageTest, para evaluar la velocidad y el rendimiento de la PWAs.

El desarrollo de PWAs en un entorno empresarial implica considerar diversos factores como pueden ser:

- Estrategia empresarial: Las PWAs deben alinearse con los objetivos estratégicos de la empresa, mejorando la experiencia del usuario, aumentando la visibilidad y generando ingresos.
- Infraestructura tecnológica: Es necesario contar con una infraestructura tecnológica sólida y escalable para soportar el desarrollo, despliegue y mantenimiento de las PWAs.
- Seguridad: La seguridad es un aspecto crítico en el desarrollo de PWAs, especialmente cuando se manejan datos sensibles de los usuarios. Se deben implementar medidas de seguridad robustas para proteger la aplicación y los datos.

### **Problema de investigación**

El uso en constante aumento de las PWAs como una alternativa versátil a las aplicaciones nativas ha expuesto a los usuarios y desarrolladores a una serie de vulnerabilidades de seguridad potenciales. Estas vulnerabilidades pueden abarcar desde amenazas tradicionales como “Cross-Site Scripting (XSS)” y “Cross-Site Request Forgery (CSRF)” hasta desafíos de cumplimiento normativo y la exposición de datos confidenciales. La falta de un enfoque integral y normativo para abordar la seguridad en las PWAs plantea una preocupación significativa.

A medida que las PWAs se convierten en una parte esencial del ecosistema digital, es crucial garantizar la seguridad de estas aplicaciones web progresivas. Los usuarios confían en las PWAs para acceder y gestionar información sensible, realizar transacciones y mantener su privacidad en línea. La exposición a vulnerabilidades de seguridad puede resultar en consecuencias graves,

como la pérdida de confianza de los usuarios, la violación de regulaciones de privacidad y la explotación de datos personales.

El desafío principal de este estudio se centra en la importancia de detectar, analizar y reducir adecuadamente las vulnerabilidades de seguridad en las PWAs, además de garantizar el cumplimiento de normativas y estándares de seguridad pertinentes. La ausencia de un marco normativo y basado en estándares puede comprometer la integridad de los datos, la confidencialidad de la información del usuario y la seguridad de las transacciones en línea, lo que resalta la necesidad de una solución integral.

En este contexto, el proyecto de titulación se propone abordar este problema, utilizando las normas ISO 27001:2022 y NIST SP 800-53 como marcos de referencia clave. Al hacerlo, se pretende no solo mejorar la seguridad de las PWAs, sino también proporcionar directrices prácticas y recomendaciones a desarrolladores y organizaciones, con el fin de fomentar un entorno seguro y confiable en el uso de aplicaciones web progresivas.

### **Objetivo general**

Evaluar la seguridad en PWAs mediante un enfoque integral basado en las normas ISO 27001:2022 y NIST SP 800-53.

### **Objetivos específicos**

- Contextualizar los fundamentos teóricos sobre seguridad en aplicaciones PWAs, utilizando como referencia las normativas ISO 27001:2022 y NIST SP 800-53, para construir una base sólida para el análisis y evaluación de vulnerabilidades.
- Evaluar en detalle el cumplimiento de las aplicaciones PWAs con respecto a los requisitos de seguridad establecidos en las normas ISO y NIST, a través de un conjunto de pruebas diseñadas específicamente para este propósito, con el fin de identificar las áreas más vulnerables.
- Desarrollar un conjunto de estrategias de mitigación, basadas en ISO y NIST, para corregir las vulnerabilidades encontradas en las PWAs y fortalecer su seguridad.
- Validar la eficacia de las estrategias propuestas mediante la evaluación de especialistas en seguridad de la información, y garantizar que las soluciones implementadas no afecten negativamente el rendimiento y la experiencia del usuario de las PWAs.

### **Vinculación con la sociedad y beneficiarios directos:**

El presente proyecto tiene como objetivo beneficiar a la comunidad de desarrolladores y empresas que trabajan con la generación de PWAs, como referencia tenemos al siguiente Objetivo de Desarrollo Sustentable:

ODS 9.- Industria, innovación e infraestructura: Contribuyendo a la innovación tecnológica y al desarrollo de soluciones digitales.

Para esto se realizará una guía de desarrollo con estándares ISO 27001:2022 y NIST beneficiando en este caso:

**Beneficiarios Directos:**

- Desarrolladores de software: Obtendrán conocimientos prácticos y herramientas para desarrollar PWAs más seguras, reduciendo el riesgo de ataques cibernéticos y mejorando la confianza de los usuarios en sus aplicaciones.
- Empresas: Las empresas que desarrollan o utilizan PWAs se beneficiarán al contar con aplicaciones más robustas y seguras, protegiendo sus datos y reputación.
- Usuarios finales: Los usuarios finales de las PWAs se beneficiarán de una experiencia de usuario más segura, al reducirse el riesgo de que sus datos sean comprometidos o que su dispositivo sea infectado por malware.

**Beneficiarios Indirectos:**

- La comunidad de seguridad informática: La investigación y los hallazgos de la tesis pueden contribuir al avance del conocimiento en el campo de la seguridad de las aplicaciones web y servir como base para futuras investigaciones.
- Gobiernos y reguladores: La investigación puede servir como base para la elaboración de políticas y regulaciones relacionadas con la seguridad cibernética.

**Beneficios Específicos:**

- Mejora de la seguridad en línea: La identificación y mitigación de vulnerabilidades en las PWAs contribuirá a un entorno en línea más seguro para todos.
- Fomento de la confianza en las tecnologías digitales: Al demostrar que las PWAs pueden desarrollarse de manera segura, se fomenta la confianza de los usuarios en estas tecnologías.
- Desarrollo económico: La seguridad de las aplicaciones es un factor clave para el desarrollo de la economía digital. Al fortalecer la seguridad de las PWAs, se contribuye al crecimiento de este sector.

Como se había indicado previamente, el presente trabajo generará una guía de recomendaciones para el desarrollo de seguro de aplicaciones PWAs que ayudará a los beneficiarios mencionados una base para la generación de este tipo de proyectos de desarrollo web, tanto para dispositivos móviles como para la utilización desde un navegador web.

## CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

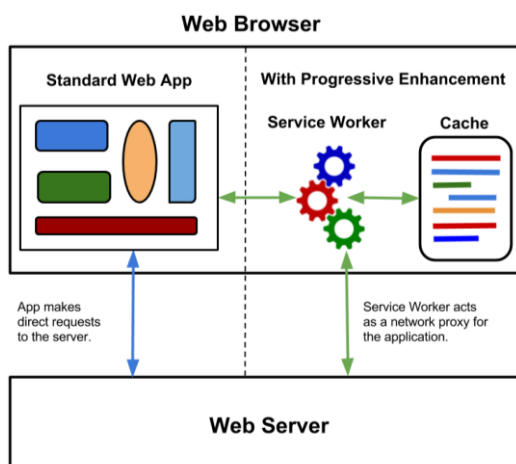
### 1.1. Contextualización general del estado del arte

La creciente popularidad de las aplicaciones web progresivas (PWAs) ha impulsado la necesidad de garantizar su seguridad. Sin embargo, a pesar de los avances en el campo de la seguridad de las aplicaciones web, las PWAs presentan desafíos únicos debido a su naturaleza híbrida entre aplicaciones web y aplicaciones móviles. Esta investigación tiene como objetivo llenar el vacío existente en el conocimiento sobre la evaluación de la seguridad de las PWAs, mediante la aplicación de los estándares ISO 27001:2022 y NIST SP 800-53.

De acuerdo con LePage y Sam (2020) “Las aplicaciones web progresivas (PWAs) son aplicaciones web creadas y mejoradas con API modernas para brindar capacidades mejoradas y al mismo tiempo llegar a cualquier usuario web en cualquier dispositivo con una única base de código. Combinan el amplio alcance de las aplicaciones web con las ricas capacidades de las aplicaciones específicas de la plataforma para mejorar la experiencia del usuario.”

**Figura 1.**

*Estructura arquitectónica general de una Progressive Web App*



*Nota.* Arquitectura tomada de la fuente Bell (2017)

Lo que implica que estas aplicaciones deben ser protegidas con estándares en forma similar a las aplicaciones web ya que su desarrollo es parecido. Las aplicaciones PWAs fundamentalmente son construidas con frameworks actuales de desarrollo de front end como Angular o React, las PWAs pueden basarse de aplicaciones normales web cumpliendo ciertas condiciones como son:

- Creación del service worker, que maneja toda la funcionalidad ya sea en línea o fuera de línea, de acuerdo con Mozilla Developer Network (2024) un Service Worker

es un script que actúa como un proxy entre una aplicación web y el navegador, permitiendo un control granular sobre la forma en que se cargan y se almacenan los recursos de la aplicación. Esta funcionalidad es especialmente útil para crear PWAs que funcionan sin conexión y ofrecen características como notificaciones push y actualizaciones en segundo plano.

- Utilización de un manifiesto para representación de aplicativo como lo indica Gómez (2021) “El manifiesto Json hace que la aplicación web le indique al navegador qué elementos mostrar para cada página web, como color, pantalla de presentación, etc. Además, todas estas tecnologías generan un icono para ser instalado en el celular sin necesidad de instalar nada adicional, ni descargar ninguna aplicación.”

#### Prácticas de seguridad en aplicaciones PWAs

Dentro de la seguridad de las PWAs hay que tener en cuenta la utilización de service workers, que de acuerdo con Mozilla Developer Network (2024), la restricción de los Service Workers a conexiones HTTPS es una medida de seguridad crucial. Las conexiones HTTP son vulnerables a ataques de "man-in-the-middle", donde un atacante puede interceptar y modificar los datos transmitidos entre el navegador y el servidor. Al requerir HTTPS, se garantiza la integridad de la comunicación y se evita que atacantes exploten las poderosas capacidades de los Service Workers para inyectar código malicioso.

Para la seguridad en aplicaciones PWAs de acuerdo con Houston (2023):

9 mejores prácticas de seguridad de PWAs, lo más importante que debe recordar sobre la seguridad de las PWAs es que siempre tienen vulnerabilidades si no implementa nuevos protocolos con regularidad, los actualiza y prueba sus capacidades para la seguridad del sistema. Y como se mencionó anteriormente, debe contratar un administrador de seguridad de aplicaciones (ASM) en su equipo de desarrollo de PWAs para incorporar los protocolos de seguridad de manera efectiva. (p. 1)

**Figura 2.**  
*Nueve Prácticas de seguridad en aplicaciones PWAs*



*Nota.* La figura es tomada de: Houston (2023)

Con respecto a la seguridad con la información en aplicaciones de acuerdo con el estándar ISO 27001 es importante tener en cuenta de acuerdo con Alomoto (2019):

Para garantizar la seguridad de la información, es crucial que la institución adopte la Norma ISO 27001. Esta norma establece directrices para gestionar la seguridad de la información, centrándose en tres aspectos clave: disponibilidad, confidencialidad e integridad de los datos, proporcionando así estabilidad y seguridad informática. La necesidad de implementar esta norma surge de la ausencia actual de procedimientos estandarizados para el manejo de la información, lo que implica una falta de bases sólidas en materia de seguridad, privacidad y control de acceso. Esta situación aumenta el riesgo de que la información quede expuesta a terceros o se pierda, ya sea por eventos catastróficos o por negligencia y malas intenciones.

(p. 4)

Indicando que para considerar la protección dentro de las aplicaciones PWAs tiene que considerar la triada de la seguridad:



**Figura 3.**  
*La Triada de la Seguridad Informática*



*Nota.* Fuente: Hacker Mentor (2024)

De acuerdo con West (2023), “La implementación de los requisitos de seguridad de aplicaciones del Anexo A 8.26 de ISO 27001 es un paso fundamental para proteger sus aplicaciones e información confidencial. Al comprender los requisitos, abordar las posibles brechas y seguir las mejores prácticas, puede establecer medidas sólidas de seguridad de las aplicaciones. Con evaluaciones y optimización continuas, puede garantizar un cumplimiento sostenido y protegerse eficazmente contra posibles riesgos de seguridad.”

Dentro de la especificación NIST 800 53, se pueden tener distintos tipos de controles dentro de aplicaciones las cuales se pueden utilizar de acuerdo con Kiuwan (2021):

RASP (Runtime Application Self-Protection) es un mecanismo de autoprotección de aplicaciones en tiempo de ejecución que detecta y bloquea la actividad maliciosa a medida que ocurre.

IAST (Interactive Application Security Testing) es una herramienta de prueba de seguridad de aplicaciones interactiva que encuentra vulnerabilidades en las aplicaciones antes de que puedan ser explotadas.

Adicional indica que RASP funciona mediante la monitorización del comportamiento de la aplicación y la identificación de actividades sospechosas. Si se detecta una actividad maliciosa, RASP puede tomar medidas para bloquearla, como detener la ejecución de la aplicación o notificar a un administrador.

IAST, por otro lado, funciona mediante el análisis del código fuente de la aplicación y la identificación de posibles vulnerabilidades. Estas vulnerabilidades pueden incluir inyección de SQL, cross-site scripting (XSS) y vulnerabilidades de inyección de comandos. Una vez identificadas las vulnerabilidades, IAST puede proporcionar información sobre cómo corregirlas.

Tanto RASP como IAST son herramientas valiosas para proteger las aplicaciones de ataques. RASP puede ayudar a prevenir ataques en tiempo real, mientras que IAST puede ayudar a identificar y corregir vulnerabilidades antes de que puedan ser explotadas.

Con respecto al uso de herramientas de análisis de vulnerabilidades en sistemas utilizando normas como la ISO 27001 de acuerdo a Cortes y Herrera (2024) "El análisis de vulnerabilidades es una parte importante en la gestión de la seguridad de los sistemas informáticos, permitiendo identificar y mitigar los riesgos de seguridad que pueden afectar a la integridad, disponibilidad y confidencialidad de los datos.", indicando la importancia del uso de herramientas como Burp Suite como complemento de verificación de vulnerabilidades.

## **1.2. Proceso investigativo metodológico**

Enfoque de la investigación: El enfoque de la investigación para este proyecto de titulación será cuantitativo. El enfoque cuantitativo donde se realizó una encuesta la misma que se encuentra en el Anexo 1, que permitirá recopilar y analizar datos numéricos para identificar, evaluar el nivel de cumplimiento de las normas ISO 27001:2022 y NIST SP 800-53 y dentro del desarrollo de las PWAs.

Tipo de investigación: El tipo de investigación será descriptivo, con elementos experimental. La investigación descriptiva permitirá caracterizar las vulnerabilidades de seguridad en las PWAs y el nivel de cumplimiento de las normas ISO 27001:2022 y NIST SP 800-53. La investigación experimental permitirá evaluar la efectividad de las estrategias de mitigación de vulnerabilidades propuestas.

- Población y muestra:
  - Población:
    - Desarrolladores de aplicaciones PWAs
    - Organizaciones que utilizan aplicaciones PWAs
    - Expertos en seguridad informática
  - Muestra:
    - Una muestra aleatoria de desarrolladores de aplicaciones PWAs.
    - Una muestra de organizaciones que utilizan aplicaciones PWAs.

- Expertos en seguridad informática con experiencia en evaluación de vulnerabilidades y pruebas de seguridad en aplicaciones web.
  - Métodos, técnicas e instrumentos:
    - Métodos:
      - Análisis de documentos: Se analizarán documentos relevantes relacionados con las normas ISO 27001:2022 y NIST SP 800-53, así como estudios de investigación sobre vulnerabilidades de seguridad en PWAs.
      - Pruebas de seguridad: Se realizarán pruebas de seguridad en aplicaciones PWAs seleccionadas para identificar vulnerabilidades y evaluar su cumplimiento con las normas ISO 27001:2022 y NIST SP 800-53.
      - Encuestas: Se diseñarán y aplicarán encuestas a desarrolladores de aplicaciones PWAs y organizaciones que utilizan PWAs para recopilar datos sobre sus prácticas de seguridad y las vulnerabilidades que han encontrado.
    - Técnicas:
      - Análisis de contenido: Se analizará el contenido de los documentos, encuestas, para identificar patrones, temas y tendencias relevantes.
      - Triangulación de métodos: Se utilizarán múltiples métodos de investigación para obtener una comprensión más completa del problema y aumentar la confiabilidad de los resultados.
    - Instrumentos:
      - Herramientas de pruebas de seguridad: Se utilizarán herramientas de pruebas de seguridad automatizadas y manuales para identificar vulnerabilidades en las aplicaciones PWAs.
      - Cuestionarios: Se diseñarán cuestionarios estructurados para las encuestas, con preguntas cerradas para recopilar datos cuantitativos.

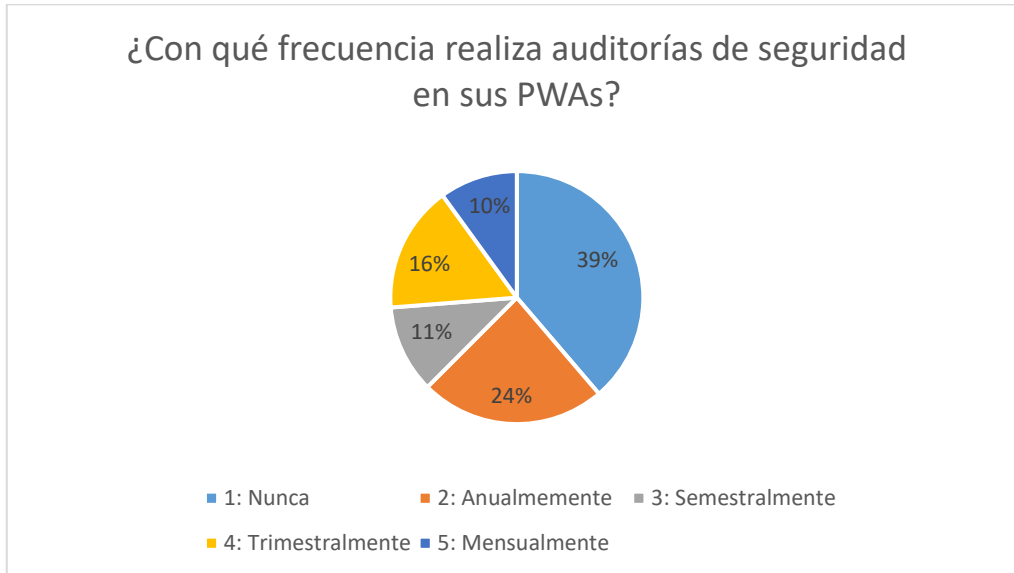
### **1.3. Análisis de resultados**

En este apartado se presentan los resultados del análisis de las encuestas realizadas a expertos en el campo de la ciberseguridad y el desarrollo de aplicaciones aleatoriamente. Las encuestas, estructuradas en torno a temas específicos relacionados con la seguridad y uso de las PWAs y alineadas a la utilización de normativas ISO 27001:2022 y NIST SP 800-53, proporcionaron una valiosa perspectiva de la necesidad, complementada con los datos cuantitativos de la investigación.

## Análisis de Tendencias Pregunta No. 1

De acuerdo con la encuesta realizada de la pregunta: ¿Con qué frecuencia realiza auditorías de seguridad en sus PWAs? se tiene los siguientes resultados en la figura:

**Figura 4.**  
*Pregunta No. 1*



La mayoría de los encuestados, el 39%, indicó que nunca realiza auditorías de seguridad en sus PWAs. Este es un hallazgo preocupante, ya que sugiere que un número considerable de aplicaciones podría estar en riesgo de exposición a vulnerabilidades durante largos períodos.

Un 24% de los encuestados realiza auditorías anualmente, lo cual, aunque es mejor que no realizarlas, podría no ser suficiente para detectar y mitigar de manera oportuna posibles amenazas en un entorno de desarrollo tan dinámico como el de las PWAs.

Por otro lado, un 16% realiza auditorías trimestralmente y un 11% semestralmente, lo que indica un enfoque más proactivo hacia la seguridad. Solo el 10% realiza auditorías mensualmente, lo cual es ideal desde el punto de vista de la seguridad, pero lamentablemente no es una práctica común entre los encuestados.

### Implicaciones para la Seguridad de las PWAs

La baja frecuencia de auditorías, especialmente el alto porcentaje de encuestados que nunca realiza auditorías es una señal de alarma. Las auditorías de seguridad son esenciales para la identificación y corrección de vulnerabilidades, y su ausencia puede dejar a las aplicaciones PWAs expuestas a ataques.

Los estándares internacionales, como ISO 27001:2022 y NIST SP 800-53, recomiendan una evaluación periódica y constante de las medidas de seguridad implementadas. La práctica ideal sería realizar auditorías trimestrales o incluso mensuales, dependiendo del nivel de riesgo asociado a la aplicación.

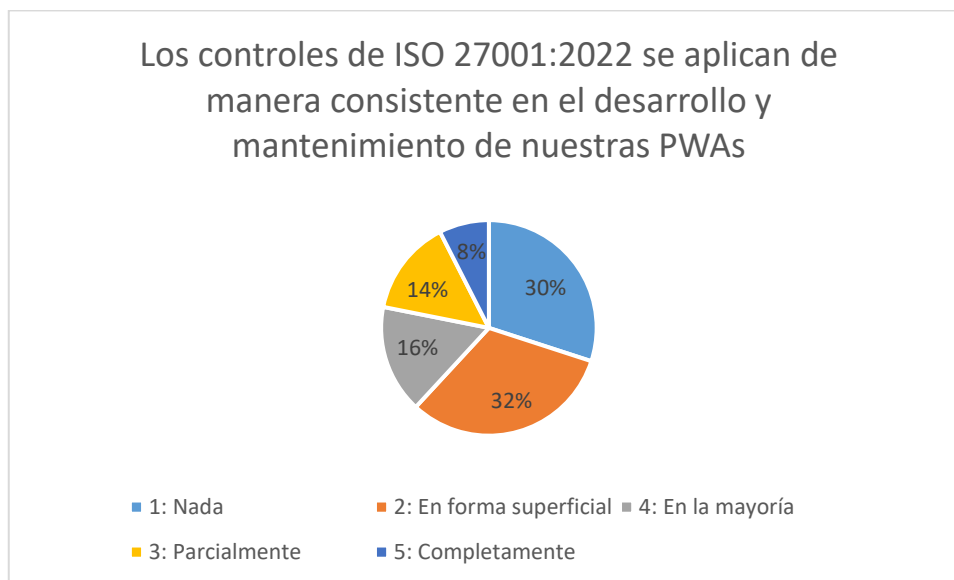
#### Recomendaciones

A la luz de estos resultados, se recomienda que las organizaciones revisen sus políticas de seguridad para garantizar que las auditorías de seguridad en PWAs se realicen con mayor frecuencia. Se sugiere adoptar un enfoque más riguroso, alineando las prácticas con las recomendaciones de las normativas ISO y NIST para minimizar el riesgo de explotación de vulnerabilidades.

#### Análisis de Tendencias Pregunta No. 2

De acuerdo con la encuesta realizada de la pregunta: - Los controles de ISO 27001:2022 se aplican de manera consistente en el desarrollo y mantenimiento de nuestras PWAs -, se tiene los siguientes resultados en la figura:

**Figura 5.**  
*Pregunta No. 2*



El análisis de los datos revela que una mayoría significativa de los encuestados, el 62% (sumando "Nada" y "En forma superficial"), considera que los controles de ISO 27001:2022 se aplican poco o nada en el desarrollo y mantenimiento de sus PWAs. Esto sugiere una implementación deficiente de las normativas de seguridad, lo cual es preocupante, dado el papel crucial que juegan estos controles en la protección de la información y la mitigación de riesgos.

Solo un 24% de los encuestados indica que los controles se aplican "En la mayoría" o "Completamente". Esto refleja que solo una minoría de organizaciones ha integrado adecuadamente las medidas de seguridad recomendadas por ISO 27001:2022 en sus procesos de desarrollo y mantenimiento de PWAs.

El 14% de los encuestados que respondió "Parcialmente" sugiere que hay un esfuerzo para aplicar estos controles, aunque no de manera completa, lo que podría indicar la existencia de procesos en marcha que aún no se han consolidado.

#### Implicaciones para la Seguridad de las PWAs

La aplicación insuficiente de los controles de ISO 27001:2022 puede tener serias implicaciones para la seguridad de las PWAs. Las respuestas que indican una implementación "Nada" o "En forma superficial" son un indicativo de que muchas aplicaciones podrían estar operando con brechas significativas en su seguridad, lo que las deja vulnerables a posibles amenazas y ataques.

El hecho de que solo un pequeño porcentaje de organizaciones aplique estos controles "Completamente" sugiere que se necesita un esfuerzo concertado para mejorar la adopción y la consistencia en la implementación de las normativas de seguridad.

#### Recomendaciones

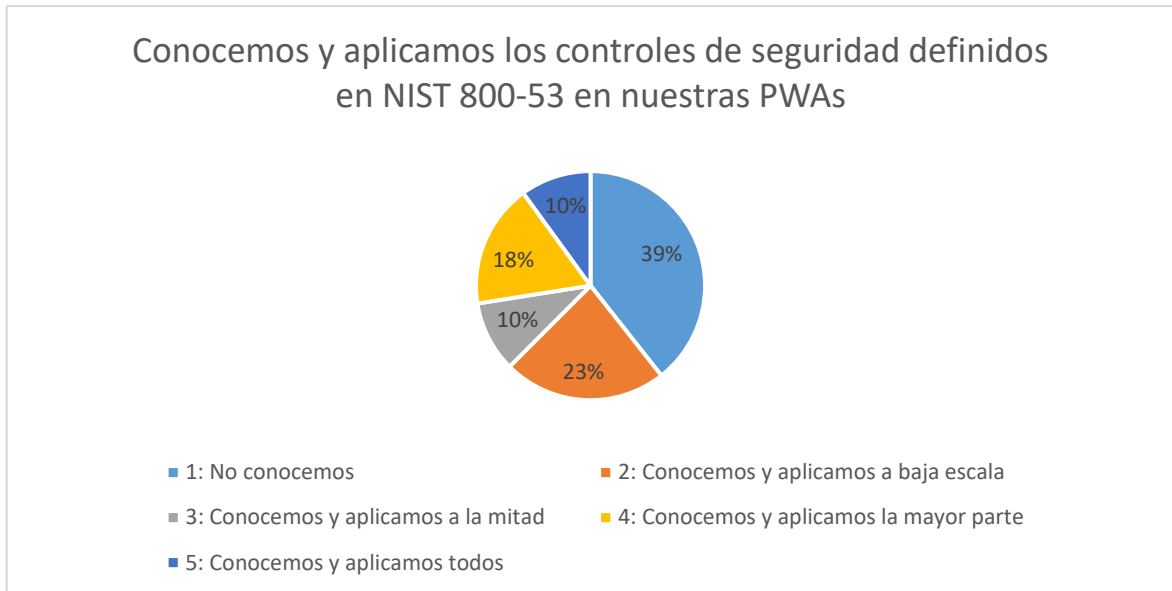
A la luz de estos resultados, es imperativo que las organizaciones revisen sus prácticas actuales de seguridad en el desarrollo de PWAs. Se recomienda:

- Evaluaciones de Seguridad: Realizar evaluaciones exhaustivas para identificar las áreas donde los controles de ISO 27001:2022 no se están aplicando correctamente.
- Capacitación y Sensibilización: Implementar programas de capacitación para asegurar que todo el equipo de desarrollo comprenda la importancia de estos controles y sepa cómo aplicarlos de manera efectiva.
- Auditorías Periódicas: Establecer auditorías regulares para monitorear y asegurar la aplicación consistente de los controles de seguridad a lo largo del ciclo de vida de las PWAs.
- Refuerzo de Políticas de Seguridad: Desarrollar y reforzar políticas internas que guíen la implementación de las normativas de ISO 27001:2022, asegurando que se adopten de manera integral y consistente.

#### Análisis de Tendencias Pregunta No. 3

De acuerdo con la encuesta realizada de la pregunta: - Conocemos y aplicamos los controles de seguridad definidos en NIST 800-53 en nuestras PWAs -, se tiene los siguientes resultados en la figura:

**Figura 6.**  
*Pregunta No. 3*



Los datos muestran que un 39% de los encuestados no está familiarizado con los controles de seguridad de NIST SP 800-53, lo que indica una significativa falta de conocimiento sobre esta normativa crucial en el ámbito de la seguridad de la información. Este resultado es alarmante, dado que NIST SP 800-53 proporciona un marco detallado para asegurar sistemas de información y servicios, incluyendo aplicaciones PWAs.

Un 23% de los encuestados afirmó que conoce y aplica los controles a baja escala, lo que sugiere que, aunque existe algún grado de conciencia sobre la normativa, su aplicación es limitada, posiblemente debido a una falta de recursos, capacitación o prioridad en la implementación.

Los encuestados que conocen y aplican los controles a la mitad o la mayor parte representan un 28% combinado. Esto indica que un segmento de las organizaciones está trabajando hacia una implementación más completa, aunque todavía queda camino por recorrer para asegurar la aplicación integral de los controles.

Finalmente, solo un 10% de los encuestados indicó que conocen y aplican todos los controles de NIST SP 800-53, lo que refleja una minoría que ha logrado implementar plenamente las recomendaciones de esta normativa.

## Implicaciones para la Seguridad de las PWAs

El hecho de que una proporción significativa de los encuestados no esté familiarizada con los controles de NIST SP 800-53 o solo los aplique en menor medida sugiere que muchas PWAs podrían estar en riesgo debido a la falta de medidas de seguridad adecuadas. La implementación parcial o inexistente de estos controles puede exponer las aplicaciones a vulnerabilidades que podrían haberse mitigado con una aplicación más rigurosa de las normativas de NIST.

Este bajo nivel de implementación también implica que las organizaciones podrían no estar cumpliendo con los estándares de seguridad esperados, lo que podría resultar en riesgos legales y reputacionales.

## Recomendaciones

Basado en estos resultados, se recomienda lo siguiente:

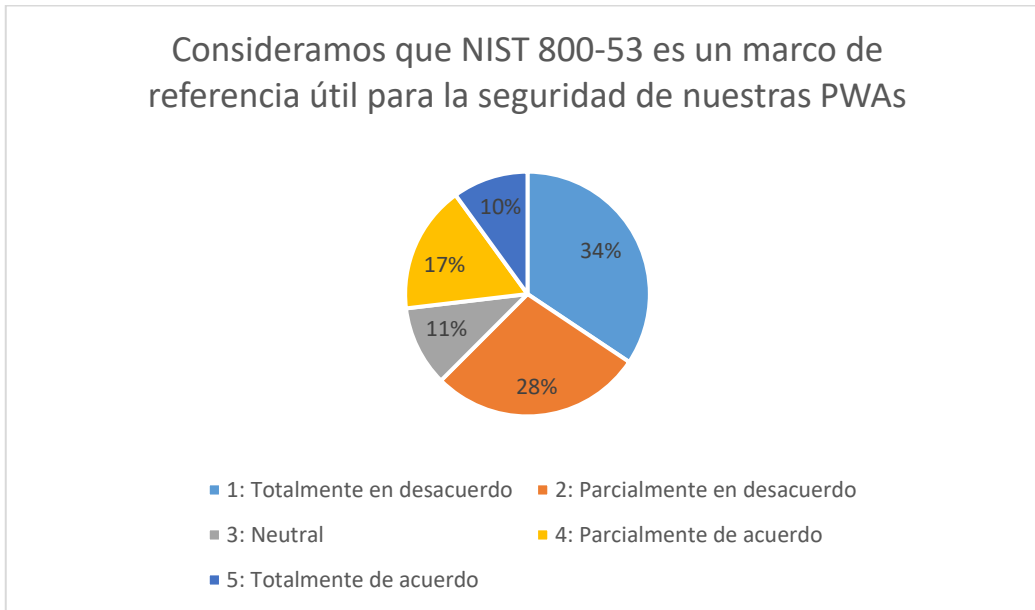
- Capacitación y Concienciación: Implementar programas de capacitación para familiarizar a los equipos de desarrollo y seguridad con los controles de NIST SP 800-53, enfatizando la importancia de su aplicación para la seguridad integral de las PWAs.
- Evaluación de Cumplimiento: Realizar una auditoría para evaluar el nivel actual de cumplimiento con los controles de NIST SP 800-53 y desarrollar un plan de acción para cerrar las brechas identificadas.
- Implementación Gradual: Para las organizaciones que conocen, pero no aplican completamente los controles, se sugiere una estrategia de implementación gradual que priorice los controles más críticos y expanda su aplicación a lo largo del tiempo.
- Revisión de Políticas de Seguridad: Reforzar las políticas de seguridad internas para alinearlas con los controles de NIST SP 800-53, asegurando que se conviertan en una parte integral del ciclo de desarrollo de las PWAs.

## Análisis de Tendencias Pregunta No. 4

De acuerdo con la encuesta realizada de la pregunta: - Consideramos que NIST 800-53 es un marco de referencia útil para la seguridad de nuestras PWAs -, se tiene los siguientes resultados en la figura:



**Figura 7.**  
*Pregunta No. 4*



Los resultados revelan una división notable en la percepción de NIST SP 800-53 como un marco de referencia útil para la seguridad de las PWAs:

Un 62% de los encuestados (sumando "Totalmente en desacuerdo" y "Parcialmente en desacuerdo") no considera que NIST SP 800-53 sea un marco de referencia útil para la seguridad de sus PWAs. Esto podría estar relacionado con una falta de conocimiento profundo sobre el marco, o con la percepción de que sus controles no se adaptan bien a las necesidades específicas de las PWAs en ciertos contextos.

Un 11% de los encuestados adoptó una postura neutral, lo que sugiere que este grupo no tiene una opinión fuerte ni a favor ni en contra de la utilidad del marco, posiblemente debido a una falta de experiencia o familiaridad con los detalles de NIST SP 800-53.

Por otro lado, un 27% de los encuestados (sumando "Parcialmente de acuerdo" y "Totalmente de acuerdo") considera que NIST SP 800-53 es un marco útil para la seguridad de sus PWAs. Este grupo ve valor en los controles y prácticas recomendadas por NIST, reconociendo su aplicabilidad para mitigar riesgos y fortalecer la seguridad.

#### Implicaciones para la Seguridad de las PWAs

El alto porcentaje de desacuerdo con la utilidad de NIST SP 800-53 sugiere que muchas organizaciones pueden estar pasando por alto un marco de seguridad reconocido que podría proporcionarles un enfoque estructurado y robusto para proteger sus aplicaciones. Esta

percepción negativa podría estar limitando la adopción de buenas prácticas de seguridad que son ampliamente aceptadas en la industria.

Además, la falta de confianza en este marco podría indicar una necesidad de personalización o adaptación de las guías de NIST SP 800-53 para que sean más accesibles y relevantes para el contexto específico de las PWAs.

#### Recomendaciones

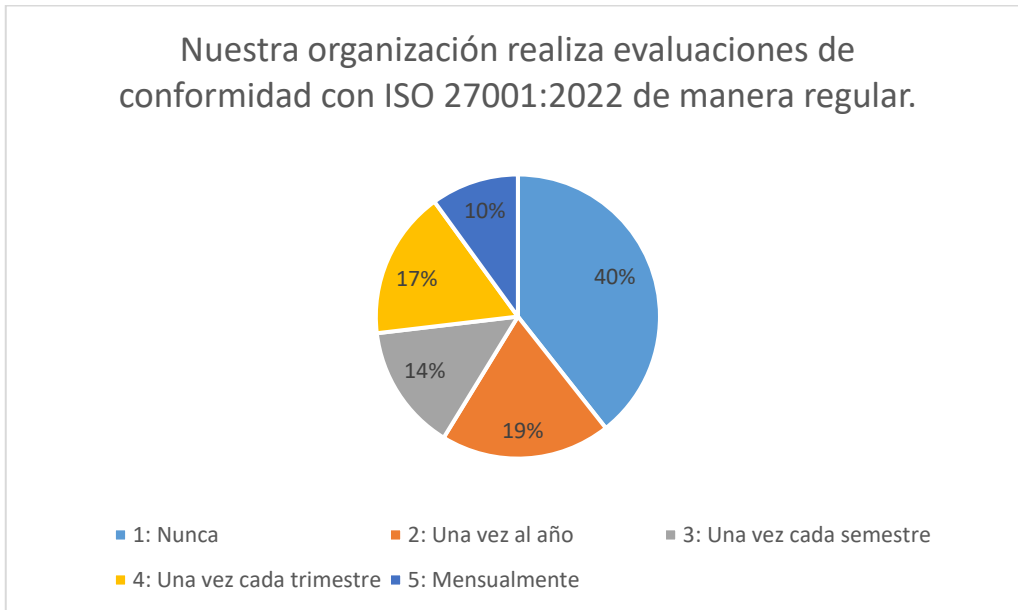
A la luz de estos resultados, se recomienda lo siguiente:

- Capacitación y Difusión: Implementar programas de capacitación que destaquen los beneficios y la aplicabilidad de NIST SP 800-53 específicamente para las PWAs. Es crucial que las organizaciones comprendan cómo los controles del marco pueden adaptarse para mejorar la seguridad de sus aplicaciones.
- Evaluación de Adaptabilidad: Considerar la posibilidad de adaptar los controles de NIST SP 800-53 para que se ajusten mejor al entorno de desarrollo de las PWAs, posiblemente combinándolos con otros marcos o guías específicos para este tipo de aplicaciones.
- Promoción de Casos de Éxito: Compartir ejemplos y casos de éxito donde la aplicación de NIST SP 800-53 ha mejorado significativamente la seguridad de las PWAs, para demostrar su valor práctico y fomentar una percepción más positiva del marco.
- Revisión Interna: Las organizaciones deberían realizar una revisión interna de sus políticas de seguridad y evaluar cómo los controles de NIST SP 800-53 podrían ser integrados o mejorados para brindar una mayor protección a sus aplicaciones PWAs.

#### Análisis de Tendencias Pregunta No. 5

De acuerdo con la encuesta realizada de la pregunta: - Nuestra organización realiza evaluaciones de conformidad con ISO 27001:2022 de manera regular -, se tiene los siguientes resultados en la figura:

**Figura 8.**  
*Pregunta No. 5*



40% de los encuestados indicó que nunca se realizan evaluaciones de conformidad con ISO 27001:2022 en su organización. Este es un resultado preocupante, ya que sugiere que una gran proporción de organizaciones no está realizando las revisiones necesarias para asegurar que sus sistemas y procesos cumplan con las normativas de seguridad establecidas por ISO 27001:2022. La falta de evaluaciones regulares puede exponer a la organización a riesgos significativos y a una mayor probabilidad de sufrir incidentes de seguridad.

Un 19% de los encuestados indicó que su organización realiza evaluaciones una vez al año. Aunque esta frecuencia es aceptable para muchas organizaciones, puede no ser suficiente en entornos dinámicos donde las amenazas y los riesgos cambian rápidamente. Las evaluaciones anuales pueden dejar periodos prolongados en los que las vulnerabilidades no se identifican ni se mitigan a tiempo.

Un 14% de los encuestados reportó que las evaluaciones se realizan una vez cada semestre, lo cual es un mejor enfoque, ya que permite a la organización revisar y ajustar sus prácticas de seguridad cada seis meses.

Un 17% de los encuestados mencionó que las evaluaciones se realizan una vez cada trimestre. Esta frecuencia es ideal para mantener un control más estricto sobre la conformidad con ISO 27001:2022, ya que permite a la organización adaptarse más rápidamente a cualquier cambio en el entorno de seguridad o a nuevas amenazas emergentes.

Finalmente, solo un 10% de los encuestados indicó que las evaluaciones se realizan mensualmente. Este enfoque es el más riguroso y asegura que la organización esté constantemente monitoreando y ajustando su conformidad con la norma, lo cual es esencial en entornos altamente sensibles o con requisitos de seguridad críticos.

#### Implicaciones para la Seguridad de las PWAs

La falta de evaluaciones regulares de conformidad con ISO 27001:2022 podría resultar en una implementación deficiente de las medidas de seguridad necesarias para proteger las PWAs. Aquellas organizaciones que no realizan estas evaluaciones o que las hacen con poca frecuencia están en mayor riesgo de no detectar fallos de seguridad, lo cual podría derivar en brechas importantes y posibles incidentes de seguridad.

Por otro lado, las organizaciones que realizan evaluaciones más frecuentes, especialmente de manera trimestral o mensual, tienen una mayor capacidad de responder de manera proactiva a los riesgos de seguridad y de asegurar que sus PWAs cumplen con las normativas de seguridad internacionalmente reconocidas.

#### Recomendaciones

Con base en estos resultados, se sugiere:

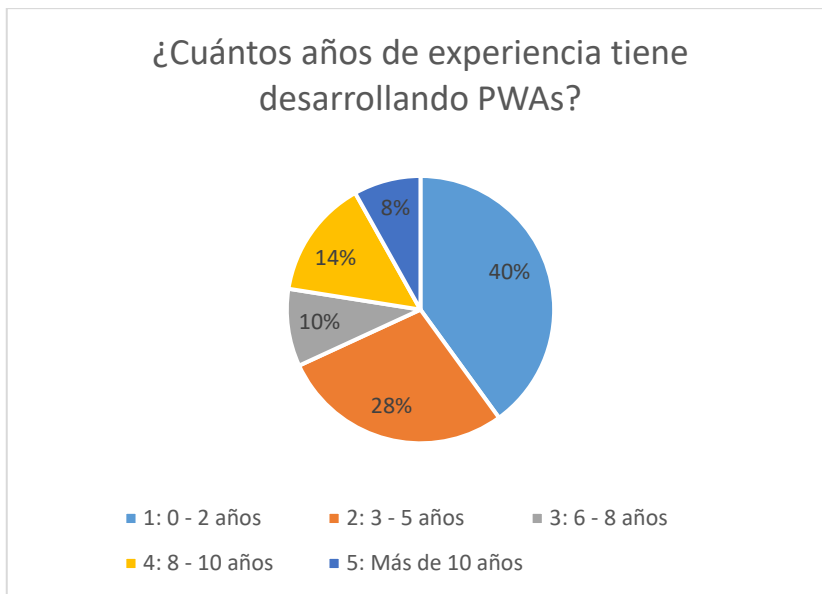
- Aumentar la Frecuencia de Evaluaciones: Para aquellas organizaciones que nunca realizan evaluaciones o lo hacen solo una vez al año, es recomendable aumentar la frecuencia de las evaluaciones. Una revisión semestral o trimestral puede ayudar a mantener un nivel de seguridad más adecuado y acorde con las mejores prácticas internacionales.
- Implementar Monitoreo Continuo: Para las organizaciones que ya realizan evaluaciones frecuentes, se podría considerar la implementación de un sistema de monitoreo continuo que complemente estas evaluaciones y proporcione una visión en tiempo real de la conformidad con ISO 27001:2022.
- Capacitación en Conformidad: Ofrecer programas de capacitación específicos para el personal encargado de la seguridad y el cumplimiento de ISO 27001:2022, asegurando que comprendan la importancia de las evaluaciones regulares y cómo llevarlas a cabo de manera efectiva.
- Revisión de Procesos: Revisar los procesos actuales de evaluación para identificar áreas de mejora, asegurando que las evaluaciones no solo se realicen con la frecuencia adecuada, sino que también sean efectivas en identificar y mitigar riesgos.

En la perspectiva del Desarrollador se tienen el siguiente análisis de las preguntas en la encuesta:

#### Análisis de Tendencias Pregunta No. 6

De acuerdo con la encuesta realizada de la pregunta: ¿Cuántos años de experiencia tiene desarrollando PWAs?, se tiene los siguientes resultados en la figura:

**Figura 9.**  
*Pregunta No. 6*



El análisis de estos resultados muestra que la mayoría de los encuestados tiene poca experiencia en el desarrollo de PWAs:

40% de los encuestados tienen entre 0 y 2 años de experiencia desarrollando Paz. Este grupo probablemente incluye a desarrolladores relativamente nuevos en esta tecnología, lo que podría implicar una curva de aprendizaje en cuanto a las mejores prácticas, incluidas las relativas a la seguridad.

28% de los encuestados reportaron tener 3 a 5 años de experiencia en el desarrollo de PWAs. Este grupo ha tenido más tiempo para familiarizarse con las tecnologías y prácticas necesarias, aunque aún puede estar en proceso de consolidar su conocimiento en áreas críticas como la seguridad.

10% de los encuestados tienen 6 a 8 años de experiencia, y 14% reportan tener 8 a 10 años de experiencia. Estos grupos suman un 24% de la muestra total, representando a desarrolladores con una base sólida en la creación de PWAs, lo que sugiere un nivel de

experiencia avanzado, especialmente en la implementación de características complejas y posiblemente en la adopción de normas de seguridad como ISO 27001 y NIST SP 800-53.

Finalmente, solo 8% de los encuestados tienen más de 10 años de experiencia en el desarrollo de PWAs. Este grupo representa a expertos en el campo, con un profundo conocimiento de las tecnologías, prácticas de desarrollo y, posiblemente, una fuerte comprensión de las consideraciones de seguridad.

#### Implicaciones para la Seguridad de las PWAs

La alta concentración de desarrolladores con poca experiencia (0 - 5 años) en el desarrollo de PWAs podría tener implicaciones significativas para la seguridad de estas aplicaciones. Los desarrolladores con menos experiencia podrían no estar completamente familiarizados con las mejores prácticas de seguridad y podrían ser más propensos a cometer errores que dejen vulnerabilidades en las aplicaciones.

Por otro lado, la menor proporción de desarrolladores con más de 6 años de experiencia sugiere que, aunque existen individuos con un conocimiento profundo, su número es relativamente bajo. Este desequilibrio podría afectar la capacidad de las organizaciones para mantener estándares de seguridad elevados en sus PWAs.

#### Recomendaciones

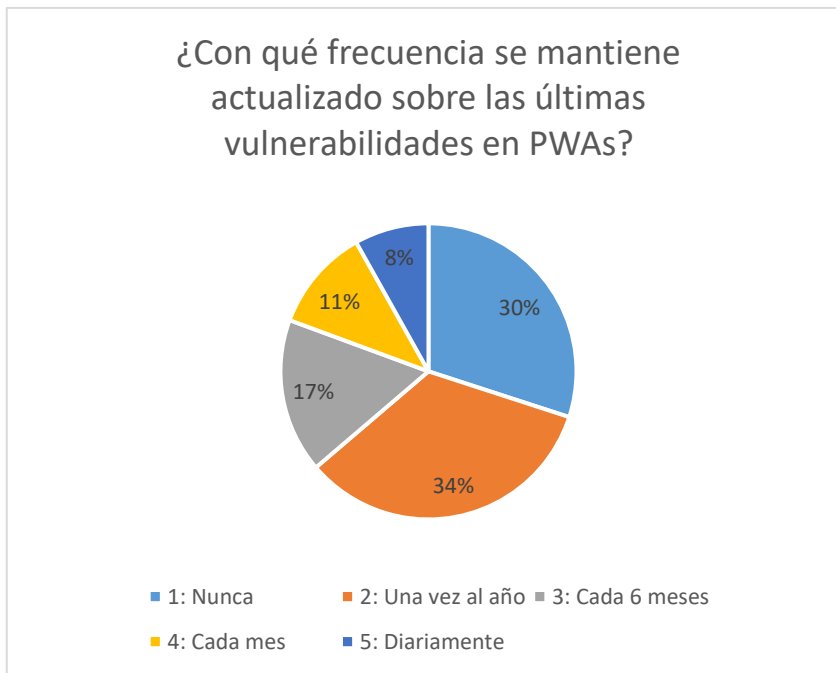
- Capacitación Continua: Dado el alto porcentaje de desarrolladores con 0 - 5 años de experiencia, es fundamental implementar programas de capacitación continua que aborden no solo las tecnologías básicas de las PWAs, sino también las mejores prácticas de seguridad específicas para estas aplicaciones.
- Mentoría y Apoyo: Las organizaciones deben fomentar la mentoría, donde desarrolladores más experimentados puedan guiar a los menos experimentados, ayudando a cerrar las brechas de conocimiento y asegurando que las prácticas de seguridad sean comprendidas y aplicadas correctamente.
- Evaluaciones de Código: Se sugiere la implementación de evaluaciones de código regulares, con un enfoque particular en la seguridad, para asegurar que las PWAs desarrolladas por personal con menos experiencia cumplan con los estándares de calidad y seguridad.
- Promoción de Buenas Prácticas: Crear y difundir guías internas de buenas prácticas para el desarrollo de PWAs, adaptadas a diferentes niveles de experiencia,

asegurando que todos los desarrolladores tengan acceso a la información necesaria para crear aplicaciones seguras.

#### Análisis de Tendencias Pregunta No. 7

De acuerdo con la encuesta realizada de la pregunta: ¿Con qué frecuencia se mantiene actualizado sobre las últimas vulnerabilidades en PWAs?, se tiene los siguientes resultados en la figura:

**Figura 10.**  
*Pregunta No. 7*



Los resultados revelan que la mayoría de los encuestados no se mantienen actualizados con regularidad sobre las vulnerabilidades en PWAs, lo cual podría tener serias implicaciones para la seguridad de las aplicaciones:

30% de los encuestados indicaron que nunca se actualizan sobre las últimas vulnerabilidades en PWAs. Este es un resultado preocupante, ya que sugiere una falta de compromiso con la seguridad continua. La ausencia de actualización sobre nuevas vulnerabilidades expone a las organizaciones a riesgos elevados, ya que pueden estar utilizando tecnologías o prácticas obsoletas que no protegen contra amenazas actuales.

34% de los encuestados mencionaron que se actualizan una vez al año. Aunque esto es un poco mejor que "nunca", sigue siendo insuficiente dado el ritmo al que evolucionan las amenazas de seguridad. Una actualización anual puede dejar a las aplicaciones vulnerables durante largos periodos de tiempo.

17% de los encuestados informaron que se actualizan cada 6 meses, lo cual es un enfoque más proactivo. Sin embargo, en un entorno de seguridad que cambia rápidamente, incluso seis meses pueden ser demasiado tiempo para no estar al tanto de nuevas vulnerabilidades.

11% de los encuestados se actualizan cada mes, lo que demuestra un compromiso más sólido con la seguridad continua. Mantenerse informado mensualmente permite a los desarrolladores y a las organizaciones reaccionar de manera más oportuna ante las nuevas amenazas y aplicar medidas correctivas antes de que las vulnerabilidades sean explotadas.

Solo 8% de los encuestados se actualizan diariamente sobre las vulnerabilidades en PWAs. Este grupo está altamente comprometido con la seguridad y probablemente sigue de cerca las fuentes de información relevantes, lo cual es crucial para mantener una postura de seguridad robusta.

#### Implicaciones para la Seguridad de las PWAs

La baja frecuencia de actualización sobre vulnerabilidades por parte de la mayoría de los encuestados es una señal de que las PWAs desarrolladas o mantenidas por estas organizaciones pueden estar en riesgo. Sin una vigilancia continua y actualizada, las aplicaciones pueden quedar expuestas a amenazas conocidas que ya tienen mitigaciones disponibles, pero que no han sido implementadas por falta de conocimiento.

Además, la seguridad en las PWAs es un área que requiere atención constante debido a la naturaleza cambiante de las amenazas y las nuevas técnicas que los atacantes desarrollan para explotar vulnerabilidades.

#### Recomendaciones

- Fomentar la Cultura de Seguridad: Es esencial crear una cultura de seguridad en la organización donde mantenerse actualizado sobre las vulnerabilidades sea una prioridad para todos los miembros del equipo. Esto puede incluir capacitaciones regulares y recordatorios sobre la importancia de seguir las últimas tendencias en seguridad.
- Establecer Protocolos de Actualización: Implementar protocolos internos que requieran que los desarrolladores y equipos de seguridad revisen y se actualicen sobre las nuevas vulnerabilidades al menos trimestralmente, si no mensualmente.
- Utilización de Recursos Automatizados: Aprovechar herramientas automatizadas y suscripciones a boletines de seguridad que informen a los equipos sobre nuevas



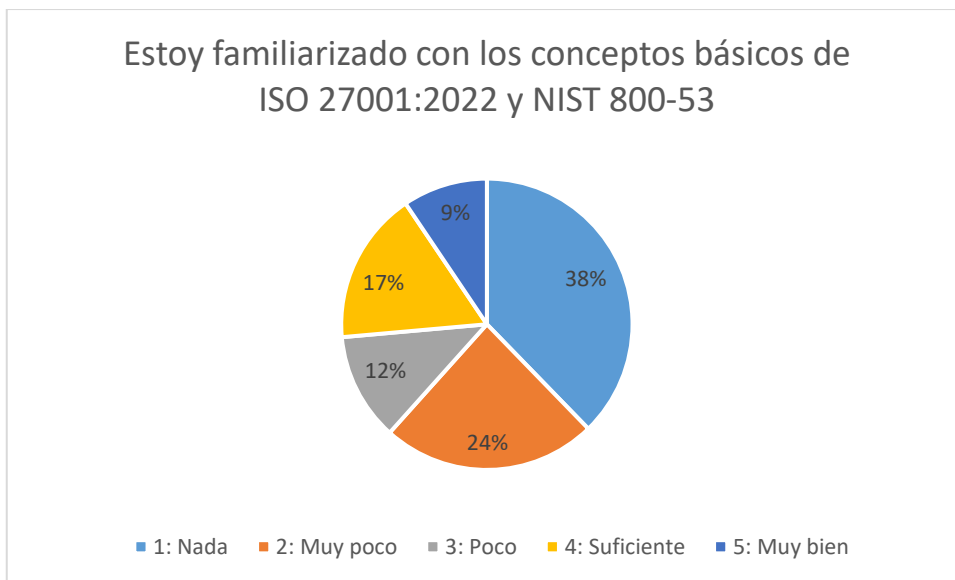
vulnerabilidades en tiempo real. Esto puede incluir alertas diarias o semanales sobre vulnerabilidades y parches disponibles.

- Asignación de Responsabilidades: Designar responsables dentro de los equipos que se encarguen específicamente de monitorear las nuevas vulnerabilidades y de informar a los demás miembros sobre las acciones que deben tomarse para mitigar los riesgos.

#### Análisis de Tendencias Pregunta No. 8

De acuerdo con la encuesta realizada de la pregunta: - Estoy familiarizado con los conceptos básicos de ISO 27001:2022 y NIST 800-53 -, se tiene los siguientes resultados en la figura:

**Figura 11.**  
*Pregunta No. 8*



Los resultados muestran que una parte significativa de los encuestados tiene un bajo nivel de familiaridad con los conceptos básicos de ISO 27001:2022 y NIST 800-53:

38% de los encuestados indicaron que no tienen ninguna familiaridad con los conceptos básicos de ISO 27001:2022 y NIST 800-53. Este es un resultado preocupante, ya que estos estándares son fundamentales para la seguridad de las PWAs, y la falta de conocimiento puede llevar a un incumplimiento significativo en las mejores prácticas de seguridad.

24% de los encuestados afirmaron que tienen muy poca familiaridad con estos estándares. Aunque algo mejor que "nada", este grupo aún necesita una considerable formación y apoyo para comprender y aplicar efectivamente los principios de ISO 27001:2022 y NIST 800-53.

12% de los encuestados se consideran poco familiarizados con estos conceptos. Este grupo puede tener un conocimiento básico pero insuficiente para asegurar que las prácticas de seguridad se implementen de manera efectiva en el desarrollo y mantenimiento de las PWAs.

17% de los encuestados tienen un nivel de familiaridad suficiente con los conceptos básicos, lo que indica que están en una posición relativamente buena para aplicar estos estándares en su trabajo diario. Sin embargo, este grupo representa menos de una quinta parte de los encuestados, lo que sugiere una necesidad generalizada de mejora.

9% de los encuestados se consideran muy bien familiarizados con ISO 27001:2022 y NIST 800-53. Este pequeño grupo es probablemente la fuente principal de conocimiento dentro de sus organizaciones y podría desempeñar un papel clave en la capacitación y apoyo a otros miembros del equipo.

#### Implicaciones para la Seguridad de las PWAs

La baja familiaridad general con los conceptos básicos de ISO 27001:2022 y NIST 800-53 podría tener implicaciones serias para la seguridad de las PWAs. La falta de comprensión de estos estándares puede conducir a la implementación inadecuada o superficial de controles de seguridad, lo que aumenta el riesgo de vulnerabilidades en las aplicaciones.

#### Recomendaciones

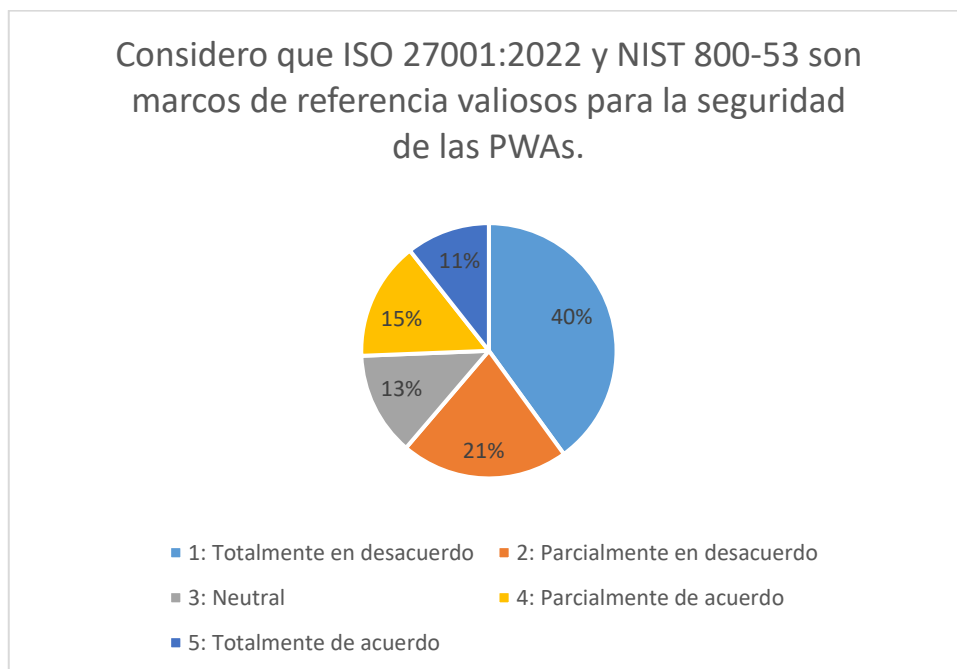
- Capacitación Intensiva: Implementar un programa de capacitación intensiva que cubra los conceptos básicos de ISO 27001:2022 y NIST 800-53. Esta formación debe ser obligatoria para todos los desarrolladores y personal de seguridad involucrados en el desarrollo de PWAs.
- Recursos de Aprendizaje: Proporcionar recursos de aprendizaje accesibles, como guías, manuales y cursos en línea, que los empleados puedan utilizar para mejorar su comprensión de estos estándares de manera continua.
- Evaluaciones Regulares: Realizar evaluaciones regulares para medir el nivel de familiaridad de los empleados con estos estándares, y ajustar las capacitaciones según sea necesario para cerrar cualquier brecha de conocimiento.
- Mentoría: Fomentar un sistema de mentoría donde aquellos que tienen un buen dominio de ISO 27001:2022 y NIST 800-53 puedan guiar y apoyar a sus colegas menos familiarizados con estos estándares.

- Integración en Procesos: Asegurarse de que los principios de ISO 27001:2022 y NIST 800-53 estén integrados en todos los procesos de desarrollo de PWAs, de manera que el personal pueda aprender a aplicarlos en un entorno práctico.

#### Análisis de Tendencias Pregunta No. 9

De acuerdo con la encuesta realizada de la pregunta: - Considero que ISO 27001:2022 y NIST 800-53 son marcos de referencia valiosos para la seguridad de las PWAs -, se tiene los siguientes resultados en la figura:

**Figura 12.**  
*Pregunta No. 9*



Los resultados muestran que una parte considerable de los encuestados no ve el valor de ISO 27001:2022 y NIST 800-53 como marcos de referencia para la seguridad de las PWAs:

40% de los encuestados están totalmente en desacuerdo con la afirmación de que estos marcos son valiosos. Este alto porcentaje indica que una gran parte de los encuestados no percibe la importancia o la aplicabilidad de estos estándares en el contexto de las PWAs, lo que podría reflejar una falta de conocimiento o comprensión de cómo estos marcos pueden contribuir a mejorar la seguridad.

21% de los encuestados están parcialmente en desacuerdo. Aunque este grupo no rechaza completamente el valor de estos marcos, sigue siendo escéptico acerca de su utilidad, lo que sugiere que podría haber percepciones erróneas o una falta de evidencia práctica que demuestre la efectividad de estos estándares en el desarrollo de PWAs.

13% de los encuestados se muestran neutrales, lo que podría indicar una falta de conocimiento suficiente para formar una opinión sólida o una percepción de que estos marcos tienen un impacto limitado en su contexto específico.

15% de los encuestados están parcialmente de acuerdo con la afirmación, lo que sugiere que reconocen algún valor en estos marcos, aunque tal vez no lo consideren completamente relevante o adecuado para sus necesidades específicas.

11% de los encuestados están totalmente de acuerdo en que ISO 27001:2022 y NIST 800-53 son valiosos para la seguridad de las PWAs. Este grupo reconoce plenamente la importancia de estos marcos y probablemente los integra en sus prácticas de desarrollo y mantenimiento de aplicaciones.

#### Implicaciones para la Seguridad de las PWAs

El escepticismo o la falta de reconocimiento del valor de ISO 27001:2022 y NIST 800-53 como marcos de referencia para la seguridad de las PWAs puede llevar a una implementación insuficiente de los controles de seguridad recomendados. Esto, a su vez, podría aumentar el riesgo de vulnerabilidades en las aplicaciones, ya que no se están aplicando las mejores prácticas basadas en estos estándares.

#### Recomendaciones

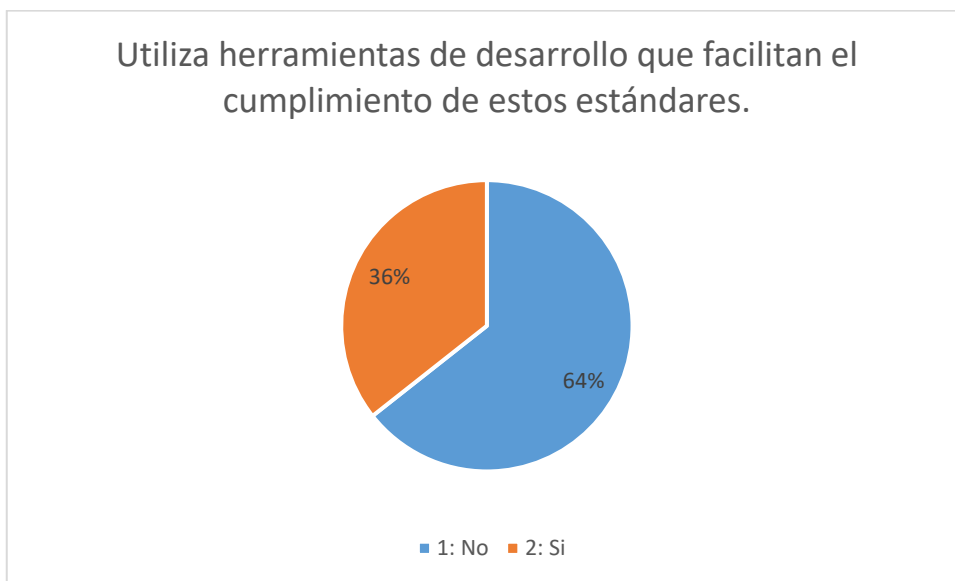
- **Concientización y Capacitación:** Es crucial aumentar la concientización sobre la relevancia y los beneficios de ISO 27001:2022 y NIST 800-53 para la seguridad de las PWAs. Esto puede lograrse a través de talleres, seminarios y materiales educativos que demuestren casos prácticos de éxito y las ventajas de adoptar estos marcos.
- **Demostración de Impacto:** Proporcionar ejemplos concretos y estudios de caso que muestren cómo la implementación de estos marcos ha mejorado la seguridad en PWAs puede ayudar a cambiar la percepción de su valor.
- **Integración en Procesos:** Asegurar que los principios de ISO 27001:2022 y NIST 800-53 se integren en los procesos de desarrollo y mantenimiento de PWAs, para que los equipos puedan ver cómo estos marcos contribuyen directamente a la seguridad de sus aplicaciones.
- **Evaluación de Percepciones:** Realizar evaluaciones periódicas de las percepciones del personal sobre estos marcos para identificar áreas donde se necesiten más recursos o apoyo para mejorar la adopción y aplicación de estos estándares.

- Soporte de Expertos: Involucrar a expertos en ISO 27001:2022 y NIST 800-53 para que ofrezcan orientación directa y personalizada a los equipos de desarrollo, ayudándoles a entender cómo estos marcos pueden ser aplicados eficazmente en sus proyectos específicos.

#### Análisis de Tendencias Pregunta No. 10

De acuerdo con la encuesta realizada de la pregunta: - Utiliza herramientas de desarrollo que facilitan el cumplimiento de estos estándares -, se tiene los siguientes resultados en la figura:

**Figura 13.**  
*Pregunta No. 10*



Los resultados muestran una tendencia clara en cuanto al uso de herramientas de desarrollo para facilitar el cumplimiento de los estándares ISO 27001:2022 y NIST 800-53:

64% de los encuestados no utilizan herramientas de desarrollo que faciliten el cumplimiento de estos estándares. Este es un hallazgo preocupante, ya que las herramientas especializadas pueden ayudar significativamente a asegurar que las aplicaciones PWAs cumplan con los requisitos de seguridad establecidos por estas normas. La falta de uso de dichas herramientas sugiere que muchas organizaciones podrían estar implementando controles de seguridad de manera manual, lo que aumenta el riesgo de errores y omisiones.

36% de los encuestados sí utilizan herramientas de desarrollo que facilitan el cumplimiento de estos estándares. Este grupo está aprovechando la tecnología para automatizar y simplificar la implementación de los controles de seguridad, lo que probablemente contribuye a una mayor consistencia y eficacia en la protección de sus aplicaciones.

## Implicaciones para la Seguridad de las PWAs

El bajo porcentaje de encuestados que utilizan herramientas de desarrollo adecuadas sugiere que muchas organizaciones pueden estar subestimando el valor de la automatización en la implementación de normas de seguridad. Sin estas herramientas, es más probable que se pasen por alto aspectos clave de los estándares, lo que puede llevar a vulnerabilidades en las aplicaciones.

### Recomendaciones

- **Promoción de Herramientas Especializadas:** Es crucial promover el uso de herramientas de desarrollo diseñadas específicamente para ayudar a cumplir con ISO 27001:2022 y NIST 800-53. Estas herramientas pueden automatizar la aplicación de controles de seguridad, facilitar auditorías internas y garantizar que los desarrolladores sigan las mejores prácticas.
- **Capacitación en el Uso de Herramientas:** Proporcionar capacitación para el personal sobre cómo utilizar efectivamente estas herramientas. A menudo, la resistencia al cambio se debe a la falta de familiaridad con nuevas tecnologías, por lo que ofrecer una formación adecuada puede aumentar la adopción.
- **Evaluación y Selección de Herramientas:** Realizar una evaluación interna para identificar las herramientas más adecuadas para el contexto específico de la organización. Esta evaluación debe considerar factores como la integración con el flujo de trabajo existente, la facilidad de uso y la compatibilidad con otros sistemas.
- **Inversión en Tecnología:** Invertir en la adquisición y mantenimiento de herramientas que faciliten el cumplimiento de los estándares de seguridad. Esta inversión es crítica para reducir el riesgo de seguridad y asegurar que las aplicaciones PWAs estén protegidas contra amenazas.
- **Monitoreo del Cumplimiento:** Implementar un sistema de monitoreo continuo para evaluar el nivel de cumplimiento con los estándares mediante el uso de estas herramientas. Esto puede incluir la generación de informes regulares que destaquen áreas de mejora y éxitos en la implementación.

## CAPÍTULO II: PROPUESTA

### 2.1. Fundamentos teóricos aplicados

#### **Normativas de Seguridad:**

##### **ISO 27001:2022: Gestión de la Seguridad de la Información**

La norma ISO 27001:2022 es un estándar internacional para la gestión de la seguridad de la información, diseñado para ayudar a las organizaciones a proteger sus activos de información a través de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) como lo indican Nizo y Molina (2023) “En la actualidad, se encuentran diversas metodologías y normas con las cuales se pueda implementar un SGSI, tales como la norma técnica ISO 27001, 27002”. La norma establece requisitos específicos para la evaluación y el tratamiento de riesgos, que son fundamentales para asegurar la confidencialidad, integridad y disponibilidad de la información (Melo y León 2024, p. 20).

En el contexto de las PWAs, ISO 27001:2022 se convierte en un marco esencial para abordar las complejidades de seguridad que estas aplicaciones introducen. Las PWAs, al operar tanto en línea como fuera de línea y al integrar tecnologías web avanzadas como Service Workers, exponen nuevos vectores de ataque que requieren controles de seguridad robustos.

##### **NIST SP 800-53: Controles de Seguridad y Privacidad para Sistemas de Información**

El NIST SP 800-53 es un estándar desarrollado por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos, que proporciona un marco exhaustivo de controles de seguridad y privacidad para sistemas de información de igual manera lo menciona Gavilanes (2023) “los controles de seguridad y privacidad descritos en esta publicación tienen una organización bien definida y estructurada para facilitar su uso en el proceso de especificación y selección de controles de seguridad y privacidad” . Esta guía es ampliamente utilizada, especialmente en el ámbito gubernamental y en industrias que manejan información sensible, para garantizar la protección adecuada contra amenazas cibernéticas NIST (2022).

En el contexto de las PWAs, que combinan las capacidades de las aplicaciones web y nativas, el NIST SP 800-53 ofrece una serie de controles que pueden ser aplicados para mitigar las vulnerabilidades inherentes a estas aplicaciones. Dado que las PWAs tienen acceso a características del dispositivo como la cámara, la ubicación, y el almacenamiento, es crucial implementar controles robustos para proteger tanto la información del usuario como la integridad del sistema.

##### **Mapeo de controles relaciones entre ISO y NIST**

A continuación, se presenta una tabla con un mapeo de los distintos controles entre ISO 27001 y NIST:

**Tabla 1.**  
*Mapeo de Controles entre ISO 27001 y NIST 800-53*

NIST SP 800-53 CONTROLS		ISO/EC 27001 CONTROLS
		Nota: Un asterisco (*) indica que el control ISO/IEC no satisface completamente la intención del control NIST.
AC-1	Access Control Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.9.1.1, A. 12.1.1, A. 18.1.1, A. 18.2.2, <b>A.5.15 (2022)</b>
AC-2	Account Management	A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.5, A.9.2.6
AC-3	Access Enforcement	A. 6.2.2, A.9.1.2, A.9.4.1, A.9.4.4, A.9.4.5, A. 13.1.1, A. 14.1.2, A.14.1.3, A. 18.1.3
AC-4	Information Flow Enforcement	A. 13.1.3, A. 13.2.1, A. 14.1.2, A. 14.1.3
AC-5	Separation of Duties	A.6.1.2
AC-6	Least Privilege	A.9.1.2, A.9.2.3, A.9.4.4, A.9.4.5
AC-7	Unsuccessful Logon Attempts	A.9.4.2
AC-8	System Use Notification	A.9.4.2
AC-9	Previous Logon (Access) Notification	A.9.4.2
AC-10	Concurrent Session Control	None
AC-11	Session Lock	A. 11.2.8, A. 11.2.9
AC-12	Session Termination	None
AC-14	Permitted Actions without Identification or Authentication	None
AC-16	Security Attributes	None
AC-17	Remote Access	A.6.2.1, A.6.2.2, A.13.1.1, A. 13.2.1, A. 14.1.2
AC-18	Wireless Access	A.6.2.1, A. 13.1.1, A. 13.2.1
AC-19	Access Control for Mobile Devices	A. 6.2.1, A. 11.2.6, A. 13.2.1
AC-20	Use of External Information Systems	A. 11.2.6, A. 13.1.1, A. 13.2.1
AC-21	Information Sharing	None
AC-22	Publicly Accessible Content	None
AC-23	Data Mining Protection	None
AC-24	Access Control Decisions	A.9.4.1*
SI-7	Software, Firmware, And Information Integrity	A.12.1, A.12.2, A.13.1, A.13.2, A.14.1, A.14.2, A.15.1, A.16.1, A.17.1, A.18.1, <b>A.8.25 (2022)</b>
SC-8	Transmission Confidentiality And Integrity	A.7.1, A.7.2, A.8.1, A.8.2, A.13.5, A.15.1, A.15.2, A.16.1, A.17.4

Nota. La tabla es tomada de: Databrakets (2021)

Aplicabilidad de ISO 27001:2022 a las PWAs: Los controles establecidos en ISO 27001:2022 (se puede revisar en el Anexo 3) pueden aplicarse a las PWAs en varios niveles:

- Control de Acceso (A 5.15): Dado que las PWAs permiten el acceso sin conexión, es crucial implementar controles de acceso estrictos para evitar accesos no autorizados a los datos almacenados en caché. La autenticación robusta y el cifrado de datos son medidas recomendadas por la norma para mitigar estos riesgos.
- Seguridad en el Desarrollo (A 8.25): La sección A 8.25 de ISO 27001:2022 enfatiza la seguridad durante el desarrollo y la implementación de software. En el caso de las PWAs, esto implica garantizar que los Service Workers, que gestionan la funcionalidad offline y el almacenamiento en caché, sean diseñados y desarrollados con principios de seguridad desde el principio, evitando vulnerabilidades como ataques de man-in-the-middle o la exposición de datos sensibles.



- Gestión de Incidentes de Seguridad (A 5.24): Las PWAs deben tener planes de respuesta a incidentes que incluyan la detección, análisis y recuperación de incidentes relacionados con la seguridad. ISO 27001:2022 proporciona directrices para establecer un proceso formal de gestión de incidentes, lo cual es crucial dado el potencial de las PWAs para funcionar en entornos de red vulnerables.

Aplicabilidad de NIST SP 800-53 a las PWAs: Los controles que se pueden utilizar de NIST 800-53 que pueden aplicarse a las PWAs:

- AC-3 Control de Acceso Basado en Roles (RBAC): NIST SP 800-53 sugiere la implementación de controles de acceso basados en roles para minimizar el riesgo de acceso no autorizado a recursos críticos. En las PWAs, esto es particularmente relevante debido a su capacidad para operar offline, donde los datos sensibles pueden quedar expuestos si no se establecen controles de acceso adecuados. Implementar RBAC en las PWAs garantiza que solo los usuarios con los permisos necesarios puedan acceder a funciones o datos específicos.
- SI-7 Seguridad del Software y Protección contra Vulnerabilidades: Este control se enfoca en la protección contra vulnerabilidades en el software, lo cual es vital en el desarrollo de PWAs. Las PWAs dependen en gran medida de tecnologías como JavaScript y Service Workers, que pueden ser objetivos de ataques como Cross-Site Scripting (XSS) o ataques de inyección de código. La norma NIST SP 800-53 recomienda la implementación de prácticas de codificación seguras, así como el uso de herramientas automatizadas de análisis de código para identificar y corregir vulnerabilidades en etapas tempranas del desarrollo.
- SC-8 Transmisión Segura de Información: La transmisión de datos entre la PWAs y el servidor debe estar protegida para evitar interceptaciones y manipulación por parte de atacantes. El control SC-8 de NIST SP 800-53 aboga por el uso de protocolos de comunicación seguros, como HTTPS y TLS, para garantizar la confidencialidad e integridad de los datos durante su transmisión. Esto es esencial en PWAs, que pueden transmitir datos sensibles, como información de autenticación, mientras están conectadas a redes potencialmente inseguras.

Los criterios de evaluación para el presente trabajo constan de:

Cumplimiento de Controles de Seguridad:

- Evaluar si las PWAs cumplen con los controles específicos de ISO 27001:2022, como la gestión de acceso y seguridad en el desarrollo.
- Verificar la aplicación de controles de NIST SP 800-53, como RBAC y transmisión segura de información.

#### Evaluación de Riesgos:

- Análisis de la efectividad en la identificación y mitigación de riesgos según las normativas.
- Revisión de los procedimientos implementados para la gestión de incidentes de seguridad.

#### Impacto en la Seguridad y Usabilidad:

- Medir cómo las estrategias de mitigación mejoran la seguridad sin afectar negativamente la usabilidad de las PWAs.

#### Conformidad con Estándares Internacionales:

- Validar la conformidad general del sistema de gestión de seguridad de la información de las PWAs con ISO 27001:2022 y NIST SP 800-53.

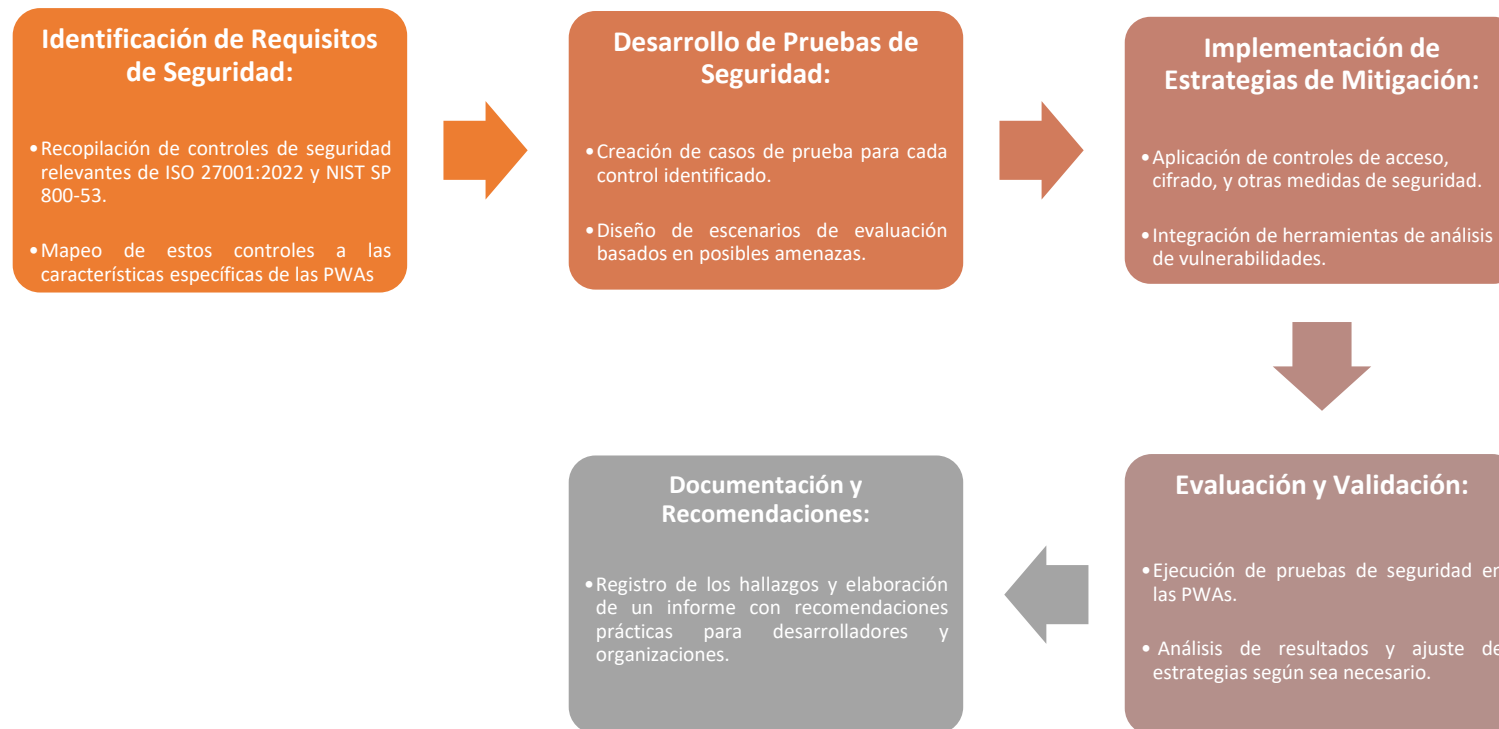
## **2.2. Descripción de la propuesta**

La propuesta tiene como objetivo desarrollar y evaluar un conjunto de pruebas de seguridad para PWAs utilizando los estándares ISO 27001:2022 y NIST SP 800-53. Se busca identificar vulnerabilidades, implementar controles y validar su eficacia.

### a. Estructura general

El diagrama de proceso descrito en la Figura 14 que se presenta a continuación visualiza la estructura general de la propuesta, destacando los componentes principales desde la identificación de vulnerabilidades hasta la validación y mejora continua. Cada etapa está diseñada para proporcionar un enfoque integral y metodológico, asegurando que las prácticas de seguridad implementadas sean coherentes y eficaces.

**Figura 14.**  
*Proceso de Evaluación y Mitigación de Vulnerabilidades en Aplicaciones Web Progresivas*



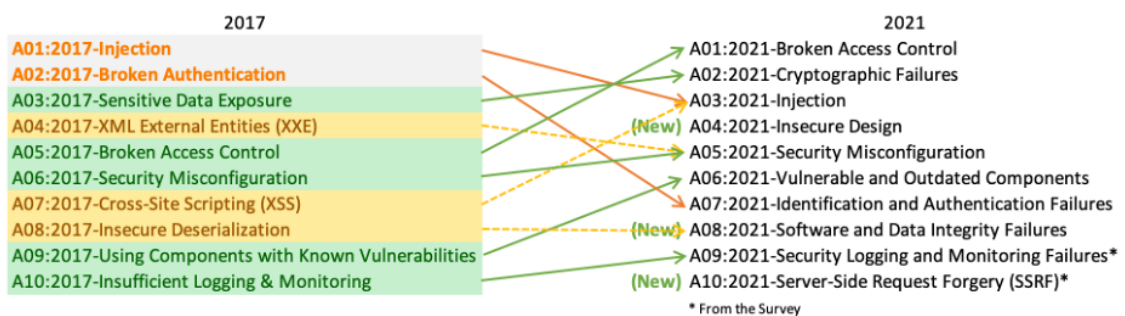
## b. Explicación del aporte

Dentro del ciclo de desarrollo de software, que es una parte crucial del proceso metodológico para la creación de aplicaciones, se realizará una evaluación exhaustiva de la seguridad en las PWAs. Este análisis se enfocará en los siguientes puntos clave para garantizar un enfoque integral y efectivo hacia la protección de la información:

### Fase de Requisitos y Diseño:

- Identificación de requisitos de seguridad: Definir los requisitos de seguridad específicos basados en ISO 27001:2022 y NIST SP 800-53, como el control de acceso (A 5.15 de ISO 27001 y AC-3 de NIST) y la protección de datos sensibles durante la transmisión (SC-8 de NIST).
- Análisis de riesgos de seguridad: Realizar un análisis de riesgos para identificar posibles amenazas y vulnerabilidades en la aplicación y determinar las medidas de mitigación necesarias.
- Diseño seguro de la aplicación: Incorporar principios de diseño seguro, como la segregación de funciones y el principio de privilegio mínimo, asegurando que las funcionalidades críticas estén protegidas desde el diseño como también es importante la utilización del OWASP que describe los 10 riesgos en aplicaciones web.

**Figura 15.**  
*Top 10 Web Application Security Risks*



*Nota.* Imagen tomada de OWASP (2021)

### Fase de Desarrollo:

- Codificación segura: Aplicar prácticas de codificación segura según las recomendaciones de NIST (SI-7) y los controles de desarrollo seguro (A 8.25 de ISO 27001). Esto incluye la validación y sanitización de entradas, la implementación de controles de autenticación robustos y el uso de herramientas para detectar vulnerabilidades durante el desarrollo.

- Gestión de dependencias y librerías: Evaluar y mantener actualizadas las dependencias y librerías utilizadas para desarrollar la PWAs, asegurando que no contengan vulnerabilidades conocidas.

#### Fase de Pruebas:

- Pruebas de seguridad específicas: Realizar pruebas de penetración y análisis estático y dinámico del código para identificar vulnerabilidades de seguridad, como inyecciones SQL, Cross-Site Scripting (XSS), y errores de configuración.
- Revisión de código: Llevar a cabo revisiones de código enfocadas en la seguridad, utilizando listas de verificación y herramientas de análisis automatizado para encontrar posibles fallos de seguridad.

#### Fase de Implementación:

- Configuración segura del entorno: Asegurar que el entorno de producción esté configurado según las mejores prácticas de seguridad, incluyendo la configuración de HTTPS para la transmisión segura de información (SC-8 de NIST).
- Gestión de credenciales y secretos: Implementar políticas adecuadas para la gestión de credenciales y secretos, evitando su almacenamiento en código fuente o configuraciones sin protección.

#### Fase de Mantenimiento:

- Monitoreo y gestión de incidentes: Establecer un proceso de monitoreo continuo para detectar y responder a incidentes de seguridad (A 5.24 de ISO 27001). Esto puede incluir el uso de sistemas de detección de intrusos (IDS) y el monitoreo de logs.
- Actualización y parcheo continuo: Mantener la aplicación actualizada con parches de seguridad y actualizaciones de software, así como realizar revisiones periódicas de la seguridad para identificar y mitigar nuevas amenazas.

Al tener definida la fase se procederá con el flujo de proceso de evaluación y mitigación de acuerdo con la Figura 14 se detalla cada uno de sus pasos:

#### Identificación de Requisitos de Seguridad:

Descripción: Este paso consiste en la identificación de los controles de seguridad específicos que son relevantes para las PWAs, de acuerdo con las normativas ISO 27001:2022 y NIST SP 800-53. Aquí se evalúan los requisitos de confidencialidad, integridad y

disponibilidad de la información, y se mapean estos requisitos a las características técnicas y operativas de las PWAs.

Actividades Involucradas:

- Análisis de los estándares ISO y NIST.
- Revisión de las funcionalidades de las PWAs que requieren protección como almacenamiento en caché y acceso offline.
- Selección de controles específicos como control de acceso y la gestión de incidentes.

Desarrollo de Pruebas de Seguridad:

Descripción: En esta fase, se desarrollan casos de prueba específicos que permitirán evaluar la seguridad de las PWAs frente a los controles identificados. Esto incluye la simulación de amenazas y vulnerabilidades que podrían explotar las debilidades en las PWAs.

Actividades Involucradas:

- Creación de escenarios de prueba basados en vulnerabilidades comunes como Cross-Site Scripting y ataques de inyección de código.
- Implementación de pruebas de penetración para verificar la efectividad de los controles de seguridad.
- Uso de herramientas automatizadas para la evaluación continua de vulnerabilidades con Burp Suite.

Implementación de Estrategias de Mitigación:

Descripción: Aquí se llevan a cabo las acciones necesarias para mitigar las vulnerabilidades identificadas durante la fase de prueba. Esto puede incluir la aplicación de controles de acceso, cifrado de datos, y otras medidas de seguridad recomendadas por ISO y NIST.

Actividades Involucradas:

- Configuración de controles de acceso basados en roles para restringir el acceso a datos sensibles.
- Implementación de cifrado de datos en tránsito y en reposo.
- Integración de Service Workers con principios de seguridad para proteger la funcionalidad offline.

Evaluación y Validación:

Descripción: Esta fase se enfoca en evaluar la efectividad de las estrategias de mitigación implementadas. Se vuelven a ejecutar las pruebas de seguridad para verificar si las vulnerabilidades han sido corregidas y si los controles son efectivos.

**Actividades Involucradas:**

- Revisión de los resultados de las pruebas de penetración post-implementación.
- Validación de los controles de seguridad por expertos en seguridad de la información.
- Ajuste de las estrategias de mitigación según sea necesario.

**Documentación y Recomendaciones:**

Descripción: Finalmente, se documentan todos los hallazgos, las pruebas realizadas, y las medidas de mitigación adoptadas. Se elabora un informe detallado que incluye recomendaciones prácticas basadas en los resultados obtenidos, orientadas a desarrolladores y organizaciones que trabajan con PWAs.

**Actividades Involucradas:**

- Elaboración de un informe técnico con los resultados de las pruebas.
- Formulación de recomendaciones para mejorar la seguridad de las PWAs.
- Creación de un manual de buenas prácticas de seguridad específico para PWAs, basado en ISO 27001:2022 y NIST SP 800-53 se puede revisar el Anexo 2.

**c. Estrategias y/o técnicas**

**Identificación de Requisitos de Seguridad**

**Estrategias:**

- Análisis de brechas: Comparar las características actuales de las PWAs con los controles de seguridad exigidos por ISO 27001:2022 y NIST SP 800-53 para identificar brechas (Gaps).
- Entrevistas con Expertos: Consultar con expertos en seguridad para validar la aplicabilidad de ciertos controles específicos en el contexto de las PWAs.

**Técnicas:**

- Mapeo de Controles: Crear un mapeo detallado de los controles de seguridad específicos a las características de las PWAs.

- Evaluación de Riesgos: Utilizar métodos de evaluación de riesgos para priorizar los controles a implementar.

#### Desarrollo de Pruebas de Seguridad

##### Estrategias:

- Desarrollo Ágil de Pruebas: Implementar un enfoque ágil para crear pruebas de seguridad que se adapten a las actualizaciones continuas de la PWAs.
- Incorporación de Modelos de Amenazas: Utilizar el modelado de amenazas para identificar posibles vectores de ataque específicos para las PWAs.

##### Técnicas:

- Test de Penetración Automatizado: Emplear herramientas automatizadas para realizar pruebas de penetración y detectar vulnerabilidades.
- Análisis de Código Estático: Revisar el código fuente de la PWAs en busca de vulnerabilidades mediante herramientas de análisis estático.

#### Implementación de Estrategias de Mitigación:

##### Estrategias:

- Aplicación de DevSecOps: Integrar la seguridad en el ciclo de vida del desarrollo de software (SDLC) mediante prácticas DevSecOps.
- Seguridad por Diseño: Adoptar principios de diseño seguro para garantizar que la seguridad sea considerada desde el inicio del desarrollo de la PWAs.
- Generación de una matriz de vulnerabilidades en la que se puede apreciar cuales son las amenazas y controles utilizar con su respectiva medida correctiva con lo podemos apreciar en las tablas 2 y 3:



**Tabla 2.**  
*Matriz de Vulnerabilidades en PWAs*

Vulnerabilidad	Descripción	Amenazas Potenciales	Controles de Seguridad (ISO 27001 / NIST 800-53)	Impacto	Probabilidad	Medida Correctiva
Inyección de Código (SQL, XSS)	Inserción de código malicioso en la aplicación a través de entradas no validadas.	Robo de datos, ejecución no autorizada de comandos.	ISO 27001: A.8.25 NIST: SI-7	Alto	Media	Validación y filtrado de entradas, uso de ORM, sanitización.
Autenticación Débil	Contraseñas débiles o falta de mecanismos de autenticación robustos.	Acceso no autorizado, suplantación de identidad.	ISO 27001: A.5.15 NIST: AC-3	Alto	Alta	Implementar autenticación de múltiples factores, controles RBAC.
Fallos en la Configuración de Seguridad	Configuraciones predeterminadas o mal configuradas que exponen la aplicación.	Acceso a configuraciones sensibles, ataques de explotación.	ISO 27001: A.5.24 NIST: SC-8	Medio	Media	Revisiones periódicas de configuración, implementación de herramientas de seguridad automatizadas.
Almacenamiento Inseguro de Datos	Datos sensibles almacenados sin cifrado o con algoritmos débiles.	Robo de datos, exposición de información confidencial.	ISO 27001: A.8.25 NIST: SC-8	Alto	Media	Cifrado de datos en reposo y en tránsito, uso de protocolos seguros.
Control de Acceso Roto	Falta de controles adecuados para restringir el acceso a recursos específicos.	Modificación no autorizada, acceso a datos sensibles.	ISO 27001: A.5.15 NIST: AC-3	Alto	Alta	Implementar controles de acceso basados en roles (RBAC), validación de permisos.

*Nota.* Por el autor, basado en varias referencias

**Tabla 3.**  
*Matriz de Vulnerabilidades en PWAs (continuación)*

Vulnerabilidad	Descripción	Amenazas Potenciales	Controles de Seguridad (ISO 27001 / NIST 800-53)	Impacto	Probabilidad	Medida Correctiva
Insuficiente Validación de Entradas	Entradas no validadas permiten ejecutar acciones inesperadas en el servidor.	Ejecución de código no autorizado, explotación de errores lógicos.	ISO 27001: A.8.25 NIST: SI-7	Alto	Media	Validación estricta de entradas, uso de frameworks seguros.
Exposición de APIs Sensibles	APIs expuestas sin autenticación o con controles de acceso deficientes.	Robo de datos, ataques de denegación de servicio.	ISO 27001: A.5.24 NIST: AC-3	Alto	Alta	Autenticación de APIs, monitoreo de tráfico y control de acceso estricto.
Gestión Inadecuada de Sesiones	Sesiones no protegidas, tokens expuestos o no expirados adecuadamente.	Suplantación de sesión, acceso no autorizado.	ISO 27001: A.5.15 NIST: AC-3	Alto	Media	Uso de tokens de sesión seguros, expiración automática y controles de renovación.
Transmisión Insegura de Información	Datos transmitidos sin cifrado o usando protocolos inseguros.	Interceptación de datos, ataques Man-in-the-Middle.	ISO 27001: A.8.25 NIST: SC-8	Alto	Media	Uso de HTTPS, TLS para la transmisión segura de información.
Falta de Monitoreo y Registro	Ausencia de registros de actividad y monitoreo continuo de la seguridad.	Dificultad para detectar y responder a incidentes.	ISO 27001: A.5.24 NIST: SI-7	Alto	Media	Implementar sistemas de monitoreo y registro de eventos de seguridad.

*Nota.* Por el autor, basado en varias referencias

#### Técnicas:

- Implementación de Controles RBAC: Configurar controles de acceso basados en roles para restringir el acceso a funciones y datos sensibles.
- Cifrado de Datos: Aplicar cifrado avanzado, tanto en tránsito como en reposo, utilizando protocolos seguros como TLS/HTTPS.

#### Evaluación y Validación:

##### Estrategias:

- Auditorías de Seguridad Regulares: Realizar auditorías de seguridad periódicas para validar la efectividad de las medidas de mitigación.
- Revisión por Pares: Involucrar a expertos en seguridad para revisar los resultados de las pruebas y validar las estrategias implementadas.

##### Técnicas:

- Pruebas de Regresión de Seguridad: Ejecutar pruebas de regresión para asegurar que las nuevas medidas de seguridad no introduzcan nuevas vulnerabilidades.
- Validación con Herramientas de Conformidad: Utilizar herramientas que verifican la conformidad con las normas ISO y NIST para validar los controles implementados.

#### Documentación y Recomendaciones:

##### Estrategias:

- Elaboración de Manuales de Buenas Prácticas: Desarrollar documentación con buenas prácticas de seguridad específicas para PWAs.
- Divulgación de Resultados: Compartir los hallazgos con las partes interesadas y proponer mejoras continuas.

##### Técnicas:

- Documentación Detallada de Procesos: Redactar informes técnicos detallados que describan cada paso del proceso y sus resultados.
- Creación de Recomendaciones Prácticas: Formular recomendaciones prácticas basadas en los resultados obtenidos para fortalecer la seguridad de las PWAs en futuras implementaciones.

### **2.3. Validación de la propuesta**

La propuesta de evaluación de seguridad en aplicaciones PWA conforme a las normas ISO 27001:2022 y NIST SP 800-53 ha sido revisada por tres expertos en seguridad informática y desarrollo de software, obteniendo como resultado que ofrece una guía sólida y coherente para abordar los desafíos de seguridad específicos de las PWAs. Su enfoque integral en la identificación, evaluación y mitigación de vulnerabilidades, alineado con estándares reconocidos internacionalmente, la convierte en una herramienta válida para cualquier organización que busque proteger la información y asegurar la robustez de sus aplicaciones web progresivas.

El respaldo de estos expertos subraya la pertinencia y el valor de la propuesta, destacando su capacidad para establecer una estrategia de seguridad eficaz en el contexto de las PWAs. La alineación con normas como ISO y NIST, su enfoque proactivo en la gestión de riesgos, y su flexibilidad para adaptarse a los cambios tecnológicos, la consolidan como una guía esencial en la búsqueda de la protección de la información y la seguridad en entornos dinámicos.

## 2.4. Matriz de articulación de la propuesta

En la Tabla 4 se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

**Tabla 4.**  
*Matriz de articulación*

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Identificación de Requisitos	Basado en los principios de ISO 27001:2022 y NIST SP 800-53 para garantizar la seguridad de la información en PWAs.	Análisis documental y diagnóstico inicial de las prácticas actuales de seguridad en PWAs.	Revisión de documentación, entrevistas con expertos, y análisis de brechas.	Identificación de áreas vulnerables y requisitos de seguridad específicos para las PWAs.	Cuestionarios, entrevistas, y análisis de documentos.
Desarrollo de Pruebas	Diseño de pruebas basadas en las normativas de seguridad establecidas en ISO 27001:2022 y NIST SP 800-53.	Método experimental para evaluar la efectividad de las pruebas de seguridad en escenarios simulados.	Implementación de pruebas automatizadas y manuales para evaluar la seguridad de las PWAs.	Resultados detallados sobre las vulnerabilidades detectadas y su severidad.	Herramientas de pruebas automatizadas, checklist de evaluación.
Estrategias de Mitigación	Aplicación de controles de seguridad recomendados por ISO 27001:2022 y NIST SP 800-53.	Desarrollo y aplicación de estrategias de mitigación basadas en la evaluación de riesgos.	Desarrollo de políticas de seguridad, implementación de cifrado, autenticación robusta, y RBAC.	Reducción significativa en el número de vulnerabilidades y mejoras en la seguridad general de las PWAs.	Herramientas de seguridad y control de acceso, análisis comparativo.
Evaluación y Validación	Validación de la efectividad de las medidas de seguridad implementadas conforme a las normativas ISO y NIST.	Revisión por pares y evaluación continua de la efectividad de las estrategias de seguridad aplicadas.	Auditorías de seguridad, análisis de impacto, y pruebas de conformidad.	Confirmación de que las medidas de seguridad implementadas cumplen con los estándares internacionales y mejoran la seguridad global.	Auditorías de seguridad, entrevistas con expertos, y análisis de impacto.

---

Desarrollo de Recomendaciones	Generación de un conjunto de recomendaciones prácticas basadas en los resultados obtenidos y alineadas con ISO 27001 y NIST SP 800-53.	Análisis comparativo de mejores prácticas y adaptación de soluciones personalizadas para cada caso de uso.	Creación de guías de implementación y recomendaciones para desarrolladores y organizaciones.	Propuesta de un plan de acción detallado para la mejora continua de la seguridad en PWAs.	Revisión documental, análisis de resultados previos, y consulta con especialistas en seguridad.
-------------------------------	----------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------

---

## CONCLUSIONES

Se ha logrado contextualizar de manera efectiva los fundamentos teóricos sobre la seguridad en aplicaciones PWAs, tomando como referencia las normativas ISO 27001:2022 y NIST SP 800-53. Este enfoque teórico ha proporcionado una base sólida para la posterior evaluación y análisis de las vulnerabilidades, permitiendo comprender la importancia de un marco normativo riguroso en el desarrollo de aplicaciones seguras.

A través de un conjunto de pruebas a ser diseñadas específicamente para las PWAs, se ha evaluado el nivel de cumplimiento de estas aplicaciones con respecto a los requisitos de seguridad establecidos por ISO 27001:2022 y NIST SP 800-53. Indicarán áreas críticas de vulnerabilidad, destacando la necesidad de mejorar la implementación de controles de seguridad en varios aspectos clave, como el control de acceso y la gestión de incidentes.

Se ha desarrollado un conjunto de estrategias de mitigación basadas en las normativas ISO y NIST, enfocadas en corregir las vulnerabilidades identificadas. Estas estrategias no solo buscan cumplir con los requisitos normativos, sino también fortalecer la seguridad general de las PWAs, asegurando una protección robusta contra amenazas potenciales.

La validación de las estrategias desarrolladas, a través de la evaluación por parte de especialistas, ha demostrado que las soluciones implementadas son efectivas y no comprometen el rendimiento ni la experiencia del usuario de las PWAs. Esto confirma la viabilidad de las medidas propuestas para mejorar la seguridad sin afectar la usabilidad de las aplicaciones.

## RECOMENDACIONES

**Capacitación y Sensibilización:** Es crucial implementar programas de capacitación que aborden en detalle los controles de seguridad de ISO 27001:2022 y NIST SP 800-53. Esto mejorará la familiarización con estas normativas y garantizará una mejor aplicación en el desarrollo de PWAs.

**Adopción de Herramientas de Seguridad:** Las organizaciones deben invertir en herramientas de desarrollo que faciliten la implementación de estos estándares, como análisis automatizado de código y pruebas de penetración específicas para PWAs.


**Auditorías de Seguridad Regulares:** Establecer un calendario de auditorías de seguridad regular, como mínimo trimestral, para evaluar el cumplimiento continuo de ISO 27001:2022 y NIST SP 800-53. Esto garantizará que las medidas de seguridad se mantengan actualizadas y efectivas.

**Desarrollo Ágil y DevSecOps:** Incorporar prácticas de DevSecOps para integrar la seguridad en todas las fases del ciclo de vida de desarrollo de las PWAs, asegurando una respuesta rápida a nuevas amenazas y vulnerabilidades.

**Colaboración con Expertos:** Involucrar a especialistas en seguridad para revisar las implementaciones de controles y validar que las estrategias de mitigación sean efectivas y estén alineadas con las mejores prácticas del sector.



## BIBLIOGRAFÍA

- Alomoto Galo. (2019). *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA APLICACIÓN DE LA NORMA INTERNACIONAL ISO/IEC 27001:2013 EN LA UNIDAD EDUCATIVA ADVENTISTA GEDEÓN*. <http://repositorio.uisrael.edu.ec/handle/47000/2159>
- Bukhtinova Kate. (2023). *10+ Great Progressive Web App (PWA) Examples in 2023*. 10+ Great Progressive Web App (PWA) Examples in 2023. <https://www.dizzain.com/blog/pwa-examples/>
- Chinprutthiwong, P., Vardhan, R., Yang, G. L., & Gu, G. (2020). Security Study of Service Worker Cross-Site Scripting. *ACM International Conference Proceeding Series*, 12(2020), 643–654. <https://doi.org/10.1145/3427228.3427290>
- Cortes Ruiz Ricardo Alfonso, & Herrera Herrera Manuel Hector. (2024). ANALYSIS OF VULNERABILITIES IN THE PHOENIX INVENTORY SYSTEM IN A LEVEL 1 IPS. *ANALYSIS OF VULNERABILITIES IN THE PHOENIX INVENTORY SYSTEM IN A LEVEL 1 IPS*.
- Databrackets. (2021). *ISO/IEC 27001 Compliance & Certification*. ISO/IEC 27001 Compliance & Certification. <https://databrackets.com/iso-27001/>
- Elle Houston. (2023). *9 PWA Security Practices to Safeguard From Cyber Threats | HackerNoon*. 9 PWA Security Practices to Safeguard From Cyber Threats. <https://hackernoon.com/9-pwa-security-practices-to-safeguard-from-cyber-threats>
- Gómez-Sierra, C. J. (2021). Design and development of a PWA-Progressive Web Application, to consult the diary and programming of a technological event. *Design and development of a PWA - Progressive Web Application, to consult the diary and programming of a technological event*. <https://doi.org/10.1088/1757-899X/1154/1/012047>
- Hacker Mentor. (2024).  *Triada*. Triada. <https://www.hacker-mentor.com/blog/triada>
- Kiuwan. (2021). *How NIST SP 800-53 Revision 5 Affects Application Security | Kiuwan*. How NIST SP 800-53 Revision 5 Affects Application Security | Kiuwan. <https://www.kiuwan.com/blog/how-nist-sp-800-53-revision-5-affects-application-security/>
- LePage Pete, & Richard Sam. (2020). *What are Progressive Web Apps? | Articles | web.dev*. What are Progressive Web Apps? . <https://web.dev/articles/what-are-pwas>
- Ley. (2021). LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES. *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. [www.lexis.com.ec](http://www.lexis.com.ec)
- Mozilla Developer Network. (2024). *Service Worker API - Web APIs | MDN*. Service Worker API. [https://developer.mozilla.org/en-US/docs/Web/API/Service\\_Worker\\_API](https://developer.mozilla.org/en-US/docs/Web/API/Service_Worker_API)
- Radu Pitis. (2023). *Why Progressive Web Apps Failed to Take Off: A Look at the Challenges and Barriers | by Pitis Radu | Medium*. Why Progressive Web Apps Failed to Take Off: A Look at the Challenges and Barriers. <https://medium.com/@pitis.radu/why-progressive-web-apps-failed-to-take-off-a-look-at-the-challenges-and-barriers-9718da21f87b>

- Rensema Dirk-Jan. (2020). *The Current State of Progressive Web Apps: A study on the performance, compatibility, consistency, security and privacy, and user and business impact of progressive web apps*. <https://urn.kb.se/resolve?urn=urn:nbn:se:kau:diva-78904>
- Thakur, P. (2018). *Evaluation and Implementation of Progressive Web Application*. <http://www.theseus.fi/handle/10024/142997>
- West Harry. (2023). *How to Implement ISO 27001 Annex A 8.26 [+ Examples]*. How to Implement ISO 27001 Annex A 8.26 [+ Examples]. <https://www.grcmana.io/blog/iso-27001-annex-a-8-26>
- Bell, J. (2017). *Exploring Progressive Web Applications*. <https://www.e-gineering.com/>.  
<https://www.e-gineering.com/2017/04/05/exploring-progressive-web-applications/>
- Gavilanes Quiroga, E. M. (2023). *Propuesta de controles de seguridad informática en la nube basados en NIST 800-53 E ISO-27000*. Repositorio Digital Universidad Israel. <http://repositorio.uisrael.edu.ec/handle/47000/3952>
- Melo Gamez, L., & León Ardila, J. (2024). *Metodología para el diagnóstico y cumplimiento de la norma ISO 27001:2022*. Universidad Cooperativa de Colombia, Facultad de Ingenierías, Maestría en Gestión de Tecnologías de la Información, Bucaramanga. <https://hdl.handle.net/20.500.12494/56717>
- NIST. (2022). *NIST SP 800-53 Rev. 5*. [csrc.nist.gov. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final](https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final)
- Nizo Mesa, D. S., & Molina Rubiano, A. J. (2023). *Propuesta para implementar el SGSI basada en la norma ISO 27001: 2022 para la empresa ARIA PSW*. [repository.libertadores.edu.co. https://repository.libertadores.edu.co/server/api/core/bitstreams/eaf053dd-160b-45f8-b613-8e510bbc9a7a/content](https://repository.libertadores.edu.co/server/api/core/bitstreams/eaf053dd-160b-45f8-b613-8e510bbc9a7a/content)

## ANEXOS

### ANEXO 1

#### FORMATO DE ENCUESTA

## Mejora de la Seguridad en Progressive Web Apps (PWAs) : Evaluación y Corrección de Puntos Débiles

El siguiente formulario es una encuesta acerca de la seguridad que se utiliza o no en los desarrollos de aplicaciones PWA, las Aplicaciones Web Progresivas actualmente tienen popularidad puesto que son de bajo costo y son escalables.

Agradecemos su ayuda con toda la sinceridad del caso en esta encuesta, no se requiere de sus datos personales. Muchas gracias.

EMPRESAS, FREELANCERS

De acuerdo a la situación de la empresa o negocio de desarrollo de software

¿Con qué frecuencia realiza auditorías de seguridad en sus PWAs?

	1: Nunca	2: Anualmente	3: Semestralmente	4: Trimestralmente	5: Mensualmente
Respuesta	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Los controles de ISO 27001:2022 se aplican de manera consistente en el desarrollo y mantenimiento de nuestras PWAs.

	1: Nada	2: En forma superficial	3: Parcialmente	4: En la mayoría	5: Completamente
Respuesta	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Conocemos y aplicamos los controles de seguridad definidos en NIST 800-53 en nuestras PWAs.

	1: No conocemos	2: Conocemos y aplicamos a baja escala	3: Conocemos y aplicamos a la mitad	4: Conocemos y aplicamos la mayor parte	5: Conocemos y aplicamos todos
Respuesta	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Consideramos que NIST 800-53 es un marco de referencia útil para la seguridad de nuestras PWAs.

	1: Totalmente en desacuerdo	2: Parcialmente en desacuerdo	3: Neutral	4: Parcialmente de acuerdo	5: Totalmente de acuerdo
Respuesta	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Nuestra organización realiza evaluaciones de conformidad con ISO 27001:2022 de manera regular.

	1: Nunca	2: Una vez al año	3: Una vez cada semestre	4: Una vez cada trimestre	5: Mensualmente
Respuesta	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Desarrolladores

Las siguientes preguntas ayudan a conocer el estatus de como se realizan los desarrollos

¿Cuántos años de experiencia tiene desarrollando PWAs?

1: 0 - 2 años    2: 3 - 5 años    3: 6 - 8 años    4: 8 - 10 años    5: Más de 10 años

Respuesta                   

¿Con qué frecuencia se mantiene actualizado sobre las últimas vulnerabilidades en PWAs?

1: Nunca    2: Una vez al año    3: Cada 6 meses    4: Cada mes    5: Diariamente

Respuesta                   

Estoy familiarizado con los conceptos básicos de ISO 27001:2022 y NIST 800-53.

1: Nada    2: Muy poco    3: Poco    4: Suficiente    5: Muy bien

Respuesta                   

Considero que ISO 27001:2022 y NIST 800-53 son marcos de referencia valiosos para la seguridad de las PWAs.

1: Totalmente en desacuerdo    2: Parcialmente en desacuerdo    3: Neutral    4: Parcialmente de acuerdo    5: Totalmente de acuerdo

Respuesta                   

Utiliza herramientas de desarrollo que facilitan el cumplimiento de estos estándares.

1: No    2: Si

Respuesta       

Este formulario se creó en Universidad Israel.



## ANEXO 2

Guía de Programación Segura (Progressive Web Apps)		
Fecha de Vigencia: 29-08-2024	Fecha Última Revisión: 29-08-2024	Versión: 01

### Contenido

1. INTRODUCCIÓN .....	59
2. OBJETIVO .....	60
a. Objetivo General .....	60
b. Objetivos Específicos de la Descripción de Mejores Prácticas.....	60
3. ALCANCE .....	61
4. DESCRIPCION DE MEJORES PRÁCTICAS .....	62
6 CONTROL DE CAMBIOS .....	65

Aprobado por
Cargo: Gerencia de Seguridad de la Información
Fecha: 29-08-2024

## 1. INTRODUCCIÓN

Este manual se ha diseñado para proporcionar una guía detallada sobre cómo implementar y mantener prácticas de seguridad robustas en el desarrollo de Progressive Web Apps (PWAs). Se centra en la alineación con los estándares internacionales ISO 27001:2022 y NIST SP 800-53, asegurando que las aplicaciones sean seguras, confiables y cumplan con las regulaciones vigentes. La guía está dirigida a desarrolladores, arquitectos de software, equipos de seguridad y administradores que trabajan en el desarrollo y la gestión de PWAs.

## 2. OBJETIVO

### a. Objetivo General

Proporcionar las mejores prácticas de Programación Segura durante la etapa de Codificación del ciclo de Desarrollo de Aplicaciones.

### b. Objetivos Específicos de la Descripción de Mejores Prácticas.

- Proporcionar las mejores prácticas de programación segura para la implementación de Progressive Web Apps.
- Proporcionar un conjunto de prácticas y directrices para proteger las PWAs contra amenazas comunes.
- Alinear las estrategias de desarrollo de PWAs con los estándares internacionales ISO 27001 y NIST SP 800-53.
- Facilitar la identificación, mitigación y gestión de riesgos de seguridad en las aplicaciones web progresivas.



### **3. ALCANCE**

Las prácticas recomendadas de codificación segura que se describen en esta guía son aplicables tanto al desarrollo de nuevas aplicaciones como a las actividades de soporte y mejora de las aplicaciones existentes.

#### 4. DESCRIPCIÓN DE MEJORES PRÁCTICAS

##### 1. Control de Acceso (ISO 27001: A 5.15 y NIST 800-53: AC-3)

a. **Objetivo:** Garantizar que solo los usuarios autorizados tengan acceso a la información y funciones sensibles en la PWA.

b. **Buenas Prácticas:**

- **Implementación de RBAC (Control de Acceso Basado en Roles):** Asigne permisos de acceso basados en los roles de usuario, minimizando el riesgo de acceso no autorizado a funciones críticas. Defina claramente los roles y sus permisos correspondientes.
- **Autenticación Multi-Factor (MFA):** Requiere múltiples formas de verificación (contraseña, token de hardware, biometría) antes de conceder acceso a recursos sensibles.
- **Cifrado de Datos en Reposo y en Tránsito:** Asegure que los datos almacenados localmente en la PWA y transmitidos entre la PWA y el servidor estén cifrados para protegerlos de accesos no autorizados.
- **Revisión Regular de Accesos:** Establezca revisiones periódicas de los permisos de acceso para asegurarse de que solo los usuarios adecuados tengan acceso a los recursos necesarios.

##### 2. Seguridad en el Desarrollo (ISO 27001: A 8.25 y NIST 800-53: SI-7)

a. **Objetivo:** Asegurar que la seguridad sea una parte integral del proceso de desarrollo de la PWA.

b. **Buenas Prácticas:**

- **Desarrollo Seguro:** Utilice principios de codificación segura para prevenir vulnerabilidades comunes como Cross-Site Scripting (XSS) y ataques de inyección de código. Mantenga el software actualizado con los últimos parches de seguridad.
- **Revisiones de Código:** Realice revisiones de código regulares y análisis estáticos para identificar posibles vulnerabilidades antes de que el código sea implementado.

- **Pruebas de Penetración:** Lleve a cabo pruebas de penetración en la PWA para detectar y corregir vulnerabilidades antes del lanzamiento. Simule ataques reales para evaluar la resiliencia de la aplicación.
- **Automatización de la Seguridad:** Integre herramientas de seguridad automatizadas en el pipeline de desarrollo para detectar vulnerabilidades de manera continua.

### 3. Gestión de Incidentes de Seguridad (ISO 27001: A 5.24)

a. **Objetivo:** Prepararse para identificar, gestionar y mitigar incidentes de seguridad en la PWA.

b. **Buenas Prácticas:**

- **Plan de Respuesta a Incidentes:** Desarrolle y mantenga un plan de respuesta a incidentes que incluya procedimientos claros para la detección, análisis, contención, erradicación y recuperación de incidentes de seguridad.
- **Monitoreo Continuo:** Implemente sistemas de monitoreo continuo para detectar actividades sospechosas o inusuales que puedan indicar un incidente de seguridad.
- **Registro de Incidentes:** Mantenga un registro detallado de todos los incidentes de seguridad, incluyendo la fecha, hora, descripción, impacto y medidas tomadas. Utilice estos registros para mejorar continuamente el plan de respuesta.
- **Capacitación del Personal:** Capacite regularmente al personal en la detección de incidentes y la ejecución del plan de respuesta, asegurando que todos conozcan sus responsabilidades en caso de un incidente.

### 4. Transmisión Segura de Información (NIST 800-53: SC-8)

a. **Objetivo:** Proteger la confidencialidad e integridad de la información transmitida entre la PWA y el servidor.

b. **Buenas Prácticas:**

- **Uso de HTTPS y TLS:** Asegure que todas las comunicaciones entre la PWA y los servidores se realicen a través de HTTPS, utilizando TLS para cifrar los datos en tránsito.

- **Certificados de Seguridad:** Utilice certificados digitales válidos y actualizados para asegurar las conexiones entre la PWA y el servidor.
- **Evitar Protocolos Inseguros:** Deshabilite el uso de protocolos y algoritmos de cifrado obsoletos o inseguros, como SSL y versiones antiguas de TLS.
- **Verificación de Integridad de Datos:** Implemente mecanismos de verificación de integridad, como el uso de hash criptográfico, para asegurar que los datos no han sido alterados durante la transmisión.

**5. CONTROL DE CAMBIOS**

Fecha de Cambio	Resumen del Cambio Realizado	Autorizado por:
29-08-2024	Creación	Gerente de Seguridad de la información y Gerente de Tecnología

## ANEXO 3

### CONTROLES TECNOLÓGICOS ISO 27001:2022

<b>8</b>	<b>Controles tecnológicos</b>	
8.1	Dispositivos de punto final de usuario	<p><b>Control</b></p> <p>Se protegerá la información almacenada, procesada o accesible a través de los dispositivos finales del usuario.</p>
8.2	Derechos de acceso privilegiado	<p><b>Control</b></p> <p>La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará.</p>
8.3	Restricción de acceso a la información	<p><b>Control</b></p> <p>El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica del tema establecida sobre el control de acceso.</p>
8.4	Acceso al código fuente	<p><b>Control</b></p> <p>El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se gestionará adecuadamente.</p>
8.5	Autenticación segura	<p><b>Control</b></p> <p>Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.</p>
8.6	Gestión de capacidad	<p><b>Control</b></p> <p>El uso de los recursos se controlará y ajustará de acuerdo con los requisitos de capacidad actuales y previstos.</p>
8.7	Protección contra malware	<p><b>Control</b></p> <p>La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.</p>
8.8	Gestión de vulnerabilidades técnicas	<p><b>Control</b></p> <p>Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.</p>
8.9	Gestión de la configuración	<p><b>Control</b></p> <p>Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.</p>
8.10	Eliminación de información	<p><b>Control</b></p> <p>La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento será eliminada cuando ya no sea necesaria.</p>
8.11	Enmascaramiento de datos	<p><b>Control</b></p> <p>El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con el tema específico, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.</p>
8.12	Prevención de fuga de datos	<p><b>Control</b></p> <p>Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.</p>
8.13	Copia de seguridad de la información	<p><b>Control</b></p> <p>Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada.</p>
8.14	Redundancia de las instalaciones de procesamiento de información	<p><b>Control</b></p> <p>Las instalaciones de procesamiento de información se implementarán con suficiente redundancia para cumplir con los requisitos de disponibilidad.</p>
8.15	Inicio sesión	<p><b>Control</b></p> <p>Se producirán, almacenarán, protegerán y analizarán registros que registren actividades, excepciones, fallas y otros eventos relevantes.</p>

8.16	Actividades de seguimiento	<b>Control</b> Las redes, los sistemas y las aplicaciones deberán ser monitoreados por comportamiento anómalo y se tomarán las acciones apropiadas para evaluar posibles incidentes de seguridad de la información.
8.17	Sincronización de reloj	<b>Control</b> Los relojes de los sistemas de procesamiento de información utilizados por la organización deben estar sincronizados con las fuentes de tiempo aprobadas.
8.18	Uso de programas de utilidad privilegiados	<b>Control</b> El uso de programas de utilidad que puedan anular los controles del sistema y de la aplicación debe estar restringido y estrictamente controlado.
8.19	Instalación de software en sistemas operativos	<b>Control</b> Se implementarán procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.
8.20	Seguridad en redes	<b>Control</b> Las redes y los dispositivos de red se asegurarán, administrarán y controlarán para proteger la información en los sistemas y aplicaciones.
8.21	Seguridad de los servicios de red.	<b>Control</b> Se identificarán, implementarán y controlarán los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.
8.22	Segregación de redes	<b>Control</b> Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.
8.23	Filtrado web	<b>Control</b> El acceso a sitios web externos se gestionará para reducir la exposición a contenido malicioso.
8.24	Uso de criptografía	<b>Control</b> Se deben definir e implementar reglas para el uso efectivo de la criptografía, incluida la gestión de claves criptográficas.
8.25	Ciclo de vida de desarrollo seguro	<b>Control</b> Se establecerán y aplicarán reglas para el desarrollo seguro de software y sistemas.
8.26	Requisitos de seguridad de la aplicación	<b>Control</b> Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.
8.27	Principios de arquitectura e ingeniería de sistemas seguros	<b>Control</b> Se deben establecer, documentar, mantener y aplicar principios para la ingeniería de sistemas seguros en cualquier actividad de desarrollo de sistemas de información.
8.28	Codificación segura	<b>Control</b> Los principios de codificación segura se aplicarán al desarrollo de software.
8.29	Pruebas de seguridad en desarrollo y aceptación.	<b>Control</b> Los procesos de pruebas de seguridad se definirán e implementarán en el ciclo de vida del desarrollo.
8.30	Desarrollo subcontratado	<b>Control</b> La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.
8.31	Separación de los entornos de desarrollo, prueba y producción	<b>Control</b> Los entornos de desarrollo, prueba y producción deben estar separados y protegidos.
8.32	Gestión del cambio	<b>Control</b> Los cambios en las instalaciones de procesamiento de información y los sistemas de información estarán sujetos a procedimientos de gestión de cambios.
8.33	Información de prueba	<b>Control</b> La información de las pruebas se seleccionará, protegerá y gestionará adecuadamente.

8.34	Protección de los sistemas de información durante las pruebas de auditoría	<b>Control</b> Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deben planificarse y acordarse entre el evaluador y la gerencia correspondiente.
------	----------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



## ANEXO 4

### VALIDACIÓN DE ESPECIALISTAS



## UNIVERSIDAD TECNOLÓGICA ISRAEL

### ESCUELA DE POSGRADOS “ESPOG”

### MAESTRÍA EN SEGURIDAD INFORMÁTICA

#### INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital “Evaluación de la Seguridad en Aplicaciones PWAs conforme a ISO 27001:2022 y NIST SP 800-53: Un Enfoque Integral para la Identificación y Mitigación de Vulnerabilidades”. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

#### Datos informativos

<b>Validado por:</b> Ing. Luis Eduardo Pérez Díaz, MSc
<b>Título obtenido:</b> Máster Universitario en Seguridad de Tecnologías de la Información y de las Comunicaciones
<b>C.I.:</b> 1721731782
<b>E-mail:</b> du-perez@hotmail.com
<b>Institución de Trabajo:</b> NTTDATA
<b>Cargo:</b> Ingeniero de Seguridad Aplicativa
<b>Años de experiencia en el área:</b> 5

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Evaluación de la Seguridad en Aplicaciones PWAs conforme a ISO 27001:2022 y NIST SP 800-53: Un Enfoque Integral para la Identificación y Mitigación de Vulnerabilidades"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad	X				
Factibilidad	X				
Novedad		X			
Fundamentación pedagógica	X				
Fundamentación tecnológica	X				
Indicaciones para su uso	X				
<b>TOTAL</b>	<b>34</b>				

Observaciones:.....  
.....  
.....

Recomendaciones:.....  
.....  
.....

Lugar, fecha de validación: Quito, 29 de agosto de 2024

#### AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto [protecciondatospersonales@uisrael.edu.ec](mailto:protecciondatospersonales@uisrael.edu.ec) es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en

Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo [protecciondatospersonales@uisrael.edu.ec](mailto:protecciondatospersonales@uisrael.edu.ec).

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: [Política de Protección de Datos Personales | UISRAEL](#)

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.



---

Firma del especialista  
Ing. Luis Eduardo Pérez Díaz, MSc

## UNIVERSIDAD TECNOLÓGICA ISRAEL

### ESCUELA DE POSGRADOS "ESPOG"

#### MAESTRÍA EN SEGURIDAD INFORMÁTICA

#### INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital "Evaluación de la Seguridad en Aplicaciones PWAs conforme a ISO 27001:2022 y NIST SP 800-53: Un Enfoque Integral para la Identificación y Mitigación de Vulnerabilidades". Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

#### Datos informativos

Validado por: Edison G Diaz
Título obtenido: Bachelor's in Computer and Information Systems Farmingdale State College NY
C.I.: 1711507028
E-mail: edisond9@outlook.com
Institución de Trabajo: Catholic Health Services
Cargo: Sytems Analyst Service Desk/Operations
Años de experiencia en el área: 6

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Evaluación de la Seguridad en Aplicaciones PWAs conforme a ISO 27001:2022 y NIST SP 800-53: Un Enfoque Integral para la Identificación y Mitigación de Vulnerabilidades"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia	X				
Aplicabilidad	X				
Factibilidad		X			
Novedad		X			
Fundamentación pedagógica	X				
Fundamentación tecnológica		X			
Indicaciones para su uso	X				
TOTAL	20	12			

**Observaciones** El trabajo de investigación puede ser un punto de partida para la creación de políticas en una empresa

**Recomendaciones** Sería importante que se pueda entregar un mayor detalle en como realizar una prueba y validar una vulnerabilidad

Lugar, fecha de validación: Islip NY, 29 de Agosto del 2024

#### AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto [protecciondatospersonales@uisrael.edu.ec](mailto:protecciondatospersonales@uisrael.edu.ec) es la entidad responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

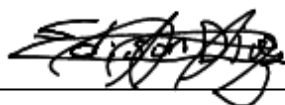
En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo [protecciondatospersonales@uisrael.edu.ec](mailto:protecciondatospersonales@uisrael.edu.ec).

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: [Política de Protección de Datos Personales | UISRAEL](#)

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.



Firma del especialista  
Edison G Díaz Systems Analyst CHS

## UNIVERSIDAD TECNOLÓGICA ISRAEL

### ESCUELA DE POSGRADOS “ESPOG”

#### MAESTRÍA EN SEGURIDAD INFORMÁTICA

#### INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la calidad del siguiente contenido digital “Evaluación de la Seguridad en Aplicaciones PWAs conforme a ISO 27001:2022 y NIST SP 800-53: Un Enfoque Integral para la Identificación y Mitigación de Vulnerabilidades”. Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide que brinde su cooperación contestando las preguntas que se realizan a continuación.

#### Datos informativos

Validado por: Eddy Fernando Granizo Cardenas
Título obtenido: Ingeniero en redes y telecomunicaciones
C.I.: 1722812771
E-mail: eddy_97f@hotmail.com
Institución de Trabajo: ProtelCotel SA
Cargo: Analista de redes
Años de experiencia en el área: 5 años



**Universidad  
Israel**

**ESPOG**

**Escuela de  
Posgrados**

Instructivo:

- Responda cada criterio con la máxima sinceridad del caso.
- Revisar, observar y analizar la propuesta de la plataforma virtual, blog o sitio web.
- Coloque una X en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Evaluación de la Seguridad en Aplicaciones PWAs conforme a ISO 27001:2022 y NIST SP 800-53: Un Enfoque Integral para la Identificación y Mitigación de Vulnerabilidades"

Indicadores	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Pertinencia		X			
Aplicabilidad		X			
Factibilidad			X		
Novedad			X		
Fundamentación pedagógica		X			
Fundamentación tecnológica	X				
Indicaciones para su uso		X			
<b>TOTAL</b>	<b>5</b>	<b>16</b>	<b>6</b>		

Observaciones:.....  
.....  
.....

Recomendaciones: Se recomienda utilizar el Common Vulnerabilities and Exposures (CVE) de la plataforma a utilizar como guía principal al crear la matriz de vulnerabilidad, ya que facilita la identificación de vulnerabilidades comunes y asegura la alineación con los estándares ISO 27001:2022 y NIST SP 800-53.

Lugar, fecha de validación: Quito, 30 de ago. de 2024

**AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES**

La Universidad Tecnológica Israel con domicilio en Francisco Pizarro E4-142 y Marieta de Veintimilla, Quito – Ecuador y dirección electrónica de contacto [protecciondatospersonales@uisrael.edu.ec](mailto:protecciondatospersonales@uisrael.edu.ec) es la entidad



responsable del tratamiento de sus datos personales, cumple con informar que la gestión de sus datos personales es con la finalidad de registrar el instrumento de validación de propuesta de la Maestría en Seguridad Informática, como requisito de titulación para los cursantes del programa de posgrados. Como consecuencia de este tratamiento sus datos estarán públicos en el repositorio donde reposan los trabajos de titulación.

La base legal para realizar dicho tratamiento es su consentimiento otorgado en este documento, el mismo que puede revocarlo en cualquier momento.

Los datos personales se publicarán en el repositorio de trabajos de titulación, no se comunicarán a terceros con otra finalidad distinta a la recogida, salvo cuando exista una obligación legal, orden judicial, de agencia o entidad gubernamental con facultades comprobadas, o de autoridad competente.

En algunos casos este tratamiento puede implicar transferencias internacionales de datos, para lo cual garantizamos el cumplimiento de la Ley Orgánica de Protección de Datos Personales y el Reglamento a la ley. La UISRAEL conservará sus datos durante el tiempo necesario para que se cumpla la finalidad indicada, mientras se mantenga la relación comercial o contractual, Ud. no revoque su consentimiento o durante el tiempo necesario que resulten de aplicación por plazos legales de prescripción.

La UISRAEL ha adoptado diversas medidas organizativas, legales y tecnológicas para proteger sus datos personales. Estas medidas están diseñadas para garantizar un nivel razonable de seguridad y cumplir con las exigencias conforme a la normativa aplicable en materia de protección de datos personales.

La UISRAEL le informa que tiene derechos sobre sus datos personales conforme lo establecido en la Ley Orgánica de Protección de Datos Personales, para su ejercicio puede hacerlo mediante envío de una solicitud al correo [protecciondatospersonales@uisrael.edu.ec](mailto:protecciondatospersonales@uisrael.edu.ec).

Para obtener más detalles de cómo se manejan sus datos personales, la UISRAEL pone a su disposición la política de Privacidad y Protección de Datos Personales disponible en el siguiente link: [Política de Protección de Datos Personales | UISRAEL](#)

Por lo expuesto, declaro haber sido informado sobre el tratamiento de los datos personales que he entregado a la UISRAEL.



firmado electrónicamente por:  
EDDY GRANIZO  
GRANIZO CARDENAS

---

Firma del especialista  
Eddy Granizo