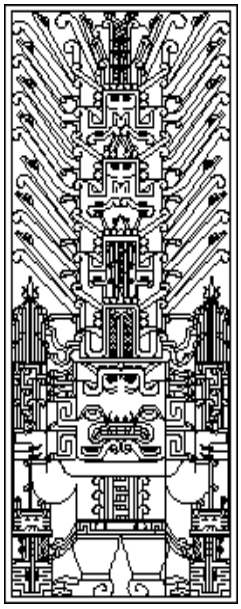
UNIVERSIDAD NACIONAL FEDERICO VILLARREAL

ESCUELA UNIVERSITARIA DE POSGRADO



TESIS

"TECNOLOGÍA WEB CON ENFOQUE OWASP EN LA AUTENTICACIÓN SEGURA DEL REGISTRO EN LÍNEA DE MENORES DEL PADRÓN NOMINADO COMO APORTE A LA REDUCCIÓN DE LA BRECHA SOCIAL DE LA PRIMERA INFANCIA"

PRESENTADO POR:

DANILO ALBERTO CHÁVEZ ESPÍRITU

PARA OPTAR EL GRADO ACADÉMICO DE:
MAESTRO EN INGENIERÍA DE SISTEMAS

LIMA- PERÚ

2018

DEDICATORIA

A mis queridos padres Tarcilo y Graciela, mi familia y a mis hijos por ser la fortaleza de mi vida.

AGRADECIMIENTO

A mis compañeros de RENIEC, a mis colegas de la UNI, a mis profesores y compañeros de clase de Escuela Universitaria de Posgrado de la UNFV y a mi asesor por su sus sabios consejos.

ÍNDICE

RESUMEN

La presente investigación tiene como objetivo autenticar de forma segura el registro en línea de menores en el Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia, considerando que la información que proporciona el RENIEC es una información que debe contar con altos niveles de seguridad, los cuales sin embargo no deben ser un obstáculo para acceder desde cualquier lugar más aun lugares alejados donde el Estado debe de tener presencia, en tal sentido se aplicó en registro en línea el proyecto abierto OWASP (Proyecto Abierto de Seguridad de Aplicaciones Web) que es referenciado por muchos estándares de seguridad, como resultado de esta implementación se logró autenticar de forma segura el registro en línea , reduciendo significativamente las vulnerabilidades en todas las fases de aplicación, lo cual ha permitido con alianzas estratégicas con el MEF y el MINSA llevar la tecnología de forma segura a las diferentes partes del Perú donde existía poca presencia del estado lo cual ha permitido que en el Padrón Nominal con el registro de los menores de la primera infancia se reduzca la brecha social en lo relacionado a la inclusión.

Palabras clave: OWASP, Tecnología Web, Padrón Nominal, Seguridad, Brecha social.

ABSTRACT

The objective of this research is to securely authenticate online registration of minors in the Nominee Register as a contribution to reducing the social gap in early childhood, considering that the information provided by RENIEC is information that must have high levels of security, which however should not be an obstacle to access from any place more distant places where the State should have a presence, in this sense the OWASP (Open Web Application Security Project), open project, which is referenced by many standards of security, as a result of this implementation it was possible to securely authenticate online registration, significantly reducing vulnerabilities in all application phases, which has enabled strategic alliances with MEF and MINSA to bring technology safely to the different parts of Peru where there was little presence of the state which has allowed in the Nominal Register with the registration of children from early childhood to reduce the social gap in relation to inclusion.

Keywords: OWASP, Web technology, Nominal Register, Security, Social gap.

INTRODUCCIÓN

Existen muchos menores de edad de la primera infancia de cero a cinco años, a los cuales el Estado no llega debido a diversas limitaciones, a pesar de los diversos programas de inclusión, esta investigación busca reducir indirectamente la brecha social de estos menores aplicando tecnología web segura y el registro e identificación en un Padrón Nominado que debe atender integralmente a estos menores de edad para sacarlos de una situación de riesgo, por lo que resulta importante recopilar toda la información que permita corregir el no contar con datos, indicadores y estadísticas reales y oportunas acerca de los diversos riesgos a la salud de menores de la primera infancia, así como también de educación que requieren la intervención del Estado. La falta de monitoreo y trazabilidad de la situación real del infante no permite evaluar el cumplimiento de metas, la evolución y evaluación del avance de lo realizado en favor de la infancia. Por otro lado, la no implementación de tecnologías seguras relacionadas a la identificación, impiden corregir los errores de falta de disponibilidad de información, que dificulta la posibilidad de mejorar la situación que atraviesan los menores de edad de la primera infancia, la ausencia de identificación no permite tener indicadores de atención de acceso a la salud.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1.- Antecedentes bibliográficos

1.1.1 Antecedentes nacionales:

Según Ñique (2016), la tecnología presenta nuevos entornos, pero también nos exponen a riesgos como la suplantación de identidad, porque carecen de robustez al momento de autenticar, facilitando que estas organizaciones sin protección sean fáciles de vulnerar, siendo necesario implementar sistemas de protección que consideren alternativas de autenticación por doble factor.

Urquizo (2016), por su parte identifica aquellos factores que afectan críticamente el registro adecuado, de esta manera propone aplicar programas de sensibilización que permita reducir errores al momento de registrar al ciudadano, la investigación también aborda la importancia de considerar las características socioculturales de las personas que registran a fin de proveer una metodología que considere lo necesario para asegurar su aprendizaje, esta investigación también busca identificar el potencial del registrador para mejorar el servicio al ciudadano.

1.1.2 Antecedentes internacionales:

Según Lay (2015), las nuevas teorías de sociología de la infancia, en su participación construye la infancia según la imagen que tienen los niños del adulto, la metodología empleada se enmarca una orientación interpretativa, en un enfoque que caracteriza abordar la participación del infante de forma inclusiva que agregue elementos experimentales y de conocimiento del entorno adulto como principios guías relacionados a la organización social que busca incluir e integrar al infante con una metodología que permita establecer acciones con una visión integral a fin de propiciar un enfoque colaborativo en busca de lograr el bienestar de la infancia.

Avella (2015), en su investigación en Colombia evalúa la política relacionada a la primera infancia en temas sociales de que implican los derechos de niños, y la falta de protección y abusos que reciben por lo que considera relevante propiciar programas que ayuden a proteger, prevenir y mejorar la educación del infante, con un enfoque en la calidad de vida del infante mediante procesos controlados.

1.2.- Planteamiento del problema

1.2.1.- Descripción de la realidad problemática

Existen muchos niños menores de cinco años comprendidos en la primera infancia, que presentan desnutrición crónica, a los cuales el Estado debe atender integralmente para sacarlos de una situación de riesgo, por lo que resulta importante recopilar toda la información que permita corregir el no contar con datos, indicadores y estadísticas reales y oportunas acerca de los diversos riesgos a la salud de los menores de la primera infancia, así como también de educación que requieren la intervención del Estado. La falta de monitoreo y trazabilidad de la situación real del infante no permite evaluar el cumplimiento de metas, la evolución y evaluación del avance de lo realizado en favor de la infancia. Por otro lado la no implementación de tecnologías seguras relacionadas a la identificación, impiden corregir los errores de falta de disponibilidad de información, que dificulta la posibilidad de mejorar la situación que atraviesan los niños de la primera infancia, la ausencia de identificación no permite tener indicadores de atención de acceso a la salud.

El RENIEC es la entidad responsable de registrar e identificar a todos los peruanos y de emitir el documento nacional que así lo acredite, el MINSA es el responsable de llevar un registro denominado Padrón Nominal que debe estar contener la data de los menores de edad hasta los 6 años que requieren ser atendidos en los centros médicos,

hospitales y postas medicas a nivel nacional que son vacunados principalmente (Resolución Ministerial 070-2011) y para ello es necesario conocer si los menores están registrados si tienen o no un DNI. Mediante el registro en el un Padrón Nominado se espera identificar a las personas documentadas y las no documentadas.

1.2.2- Formulación del problema.

Problema General:

¿De qué manera es posible autenticar de forma segura el registro en línea de menores de la primera infancia en el Padrón Nominado como aporte a la reducción de la brecha social?

Problemas Específicos:

a. ¿De qué manera es posible minimizar el riesgo del registro en línea de los menores del Padrón Nominado no identificados y no documentados?
b. ¿De qué manera es posible registrar en línea con tecnología web de forma segura a los menores del Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia?
c. ¿De qué manera es posible validar de forma segura el registro en línea de los menores del Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia?

1.3.- Objetivos

1.3.1.- Objetivo General:

Autenticar de forma segura el registro en línea de menores en el Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia.

1.3.2.- Objetivos Específicos:

a. Minimizar el riesgo del registro en línea de los menores del Padrón Nominado no identificados y no documentados.
b. Registrar en línea con tecnología web de forma segura a los menores del Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia.
c. Validar de forma segura el registro en línea de los menores del Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia.

1.4.- Justificación e importancia

1.4.1.- Justificación

Reducir la brecha de exclusión de los menores en la primera infancia, que por no estar identificados y que no pueden acceder a los servicios del Estado justifica la investigación porque además de aplicar tecnología de alto nivel como parte del conocimiento técnico permitirá aportar a la sociedad con tecnología de información, con datos confiables y líneas de transmisión de datos seguras para la identificación, registro y autenticación de los identificados para acceder a los servicios que ofrece el Estado.

1.4.2.- Importancia

La importancia se da porque permitirá incluir un nuevo conocimiento relacionado a implementar tecnología bajo nuevos enfoques de seguridad, toda vez que se conectara a bases de datos estratégicas y críticas para el Estado, con la finalidad de expandir su presencia en las zonas donde existen menores de edad no identificados y no documentados.

1.5.- Alcances, delimitación y limitaciones

1.5.1.- Alcances

La investigación es de alcance a nivel nacional, puesto que busca aportar un nuevo conocimiento para conectar a todas las regiones del país con un sistema seguro que permita registrar a los menores de la primera infancia que están no identificados y no documentados, a fin de acortar la brecha social.

1.5.2.- Delimitación

a. Espacial

Está circunscrita al espacio territorial del Perú, sin embargo, considerando que la investigación se enfoca en la aplicación de la tecnología para la inclusión de los niños de la primera infancia que no están identificados, el espacio inicial se enfocó en las regiones de Amazonas, Cajamarca y Huánuco y en la actualidad comprende a todos los lugares donde se encuentran las oficinas registrales del RENIEC.

b. Temporal

Abarca desde el año 2013 hasta el año 2017, tomando en cuenta que es un proceso continuo el registro de ciudadanos y de inclusión de los menores de la primera infancia en los proyectos sociales.

c. Temática y unidad de análisis

La temática corresponde a la seguridad en la tecnología web con la aplicación de los 10 componentes del marco de referencia OWASP para la autenticación segura del registro en línea de menores de la primera infancia del padrón nominado como aporte a la reducción de la brecha social

1.5.3.- Limitaciones

Las limitaciones que se han considerado son:

- Indisponibilidad del servicio de internet en las zonas alejadas a donde se pretende llegar para identificar y documentar a los menores de la primera infancia.
- Disponibilidad de personal para llegar a los lugares recónditos donde el Estado no llega con la tecnología y la brecha social se amplía.

CAPÍTULO II

MARCO TEÓRICO

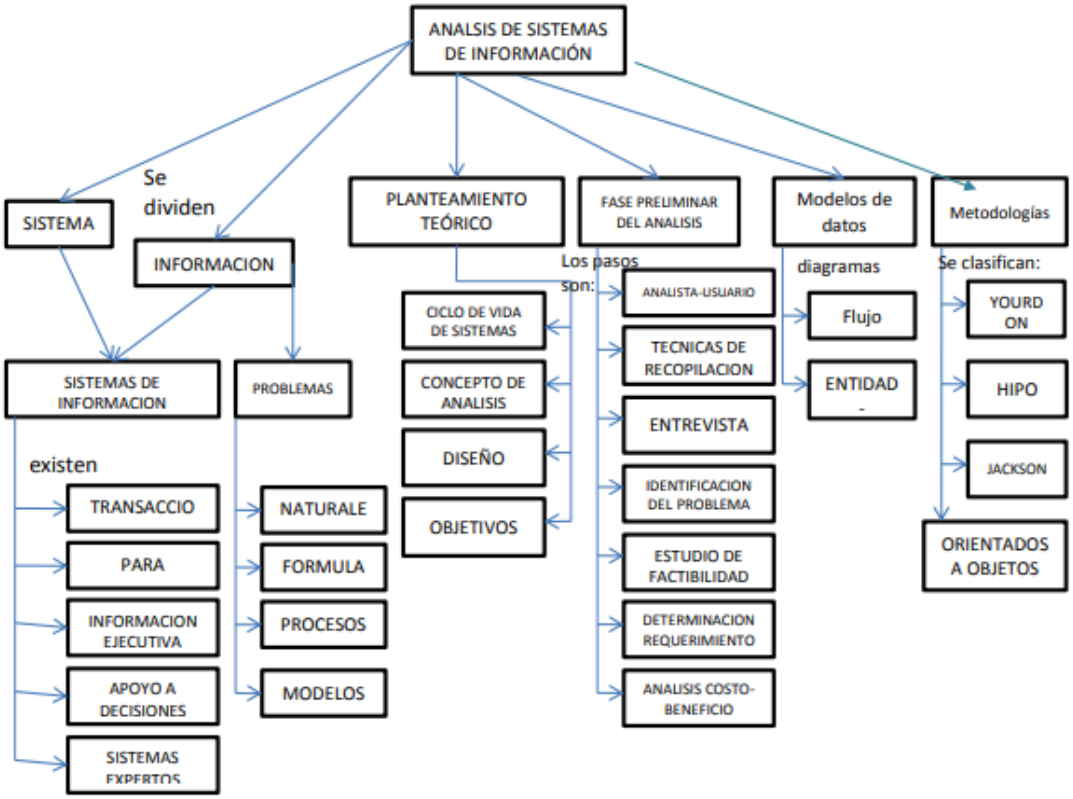
2.1.- Teorías generales

2.1.1- Teoría General de Sistemas

Según Dominguez (2012) "La teoría general de sistemas tiene su origen en los trabajos realizados por el biólogo alemán Von Bertalanffy, dados a conocer públicamente entre 1950 y 1968". Esta teoría a su vez genera formulaciones conceptuales para ser aplicadas empíricamente en el análisis de sistemas de información, Figura 1.

Figura 1: Sistemas de Información

Fuente: Luis Antonio Domínguez Coutiño 2008



Esta teoría nos permite:

- Integrar diversos conocimientos.

- Orientar a una sola teoría.
- Desarrollar otras áreas del conocimiento científico.
- Acercarnos a objetivos de investigación científica de aportar al conocimiento y a la sociedad.

La Teoria General de Sistemas en su comprensión de los sistemas se manifiesta en el analisis general, considerando las relaciones de los sistemas en lo relacionado a que :

- Dentro de los sistemas hay sistemas, en el caso de esta investigación existe un sistema de registro de identificación que se incorporará a otro sistema que es el Padrón Nominado, así como incorporar el marco OWASP a la tecnología Web para asegurar el acceso al servicio Web.
- Los sistemas no son cerrados y permiten por su apertura incorporar sistemas o subsistemas para mejorar los sistemas.
- La estructura de los sistemas permite que sus funciones coadyuven al logro del objetivo para el cual están destinados.

En todo este proceso la administración fue la más fortalecida en su enfoque sistemático por el dominio de las ciencias, como por ejemplo como concebir un sistema de seguridad sin estar compuesto por un algoritmo matemático, lo que originó el dominio de las ciencias que trascendió por el concepto de sistema que especialmente impacto en la administración.

2.1.2- Teoría de la Identidad Social

Scandroglio, López, & San José, (2008) explican que la "Teoría de la Identidad Social (TIS) y la Teoría de la Auto-Categorización del Yo han tenido gran influencia en la Psicología Social contemporánea, proporcionando reseñables contribuciones a la comprensión de la dimensión social de la conducta".

La investigación revisa los componentes de la Teoría de la Identidad Social, y explica los esfuerzos de trabajos e interpretaciones que explican el comportamiento grupal considerando las dimensiones, el contexto y los procesos de identificación para analizar los eventos de grupo de una manera congruente a su complejidad.

2.2.- Bases teóricas

2.2.1- Seguridad en red:

Según Klooster (2016) en su investigación de "Aplicación de una metodología de prueba de seguridad: un estudio de caso" explica que la prueba de seguridad es una disciplina de prueba de software que tiene como objetivo verificar si está protegido y la resistencia de su funcionalidad contra los ataques a este y a los datos procesados. Los estándares de seguridad se publican para establecer requisitos comunes que debe cumplir el software. En esta investigación se describe y aplica un proceso necesario para verificar la seguridad de una aplicación web mediante un checklist de requerimientos de seguridad que combina el estándar de seguridad de aplicaciones web OWASP ASVS y OWASP Proyecto Top Ten. Se desarrollaron casos de prueba y se probó la aplicación web UXP Portal para verificar los requisitos de seguridad en la lista de verificación, se identifican numerosas vulnerabilidades de seguridad fueron identificadas por pruebas de seguridad así como las recomendaciones basadas en las lecciones aprendidas durante el estudio de caso presentados.

2.2.2- **Metodología de calificación de riesgo de OWASP**:

El descubrimiento de las vulnerabilidades es importante, pero ser capaz de estimar el riesgo asociado para el negocio es igualmente importante. Al principio del ciclo de vida, uno puede identificar problemas contra la seguridad tanto en la arquitectura como en el diseño por medio del modelamiento de amenazas. Más tarde, uno puede encontrar problemas de seguridad mediante la revisión del código o las pruebas de penetración. O

bien, es posible que los problemas no se descubran hasta que la aplicación esté en producción y en realidad esté comprometida.

Al seguir el enfoque, se proyecta el nivel de dificultad de los riesgos para la empresa al decidir qué acción tomar al momento que emergen los riesgos. Tener el sistema instituido permitirá analizar riesgos y optimizar el tiempo y eliminar discusiones sobre cual atacar primero. Lo importante aquí es la garantía que la organización no se enfoque en los riesgos menores como tampoco se ignoren lo de mayor impacto que siempre se comprenden menos.

Idealmente, habría un sistema de calificación de riesgo universal que calcularía con precisión todos los riesgos para todas las organizaciones. Pero una vulnerabilidad crítica para una organización puede no ser tan crítica para otra. Entonces se debe personalizar para la organización en particular.

Los autores han intentado hacer que este modelo sea fácil de usar, manteniendo al mismo tiempo los detalles suficientes para realizar estimaciones de riesgos precisos. Consulte la sección a continuación sobre personalización para obtener más información sobre cómo adaptar el modelo para su uso en una organización específica.

2.3 Marco tecnológico

2.3.1- Seguridad en la Web

Según Corona (2010) la seguridad informática aborda las debilidades del procesamiento de la información, considerando que en la actualidad el Internet es el vector principal en el procesamiento e intercambio de información, y la arquitectura basada en la web representa el estándar para acceder a los servicios de Internet. Es comprobado, que la debilidad de la seguridad es a través de Internet y está en: los usuarios que navegan en la Web y las aplicaciones web del lado del servidor que procesa la información, la investigación presenta dos enfoques de sistemas de seguridad, los cuales

contribuyen significativamente en la seguridad de los navegadores web y a las aplicaciones en los servidores web que son los típicos "puntos débiles".

Se analiza críticamente un sistema de detección de intrusos (IDS), el cual luego de implementado, debe aprender y operar en un ambiente adversarial y hostil ya que se convierte en un componente del sistema y de la red que debe estar protegido. Este aspecto es importante tener en cuenta, ya que, además de cualquier otro componente, el propio IDS puede ser atacado, lo cual es realmente complejo y la imagen general aún no está clara. Contrariamente, la conciencia de esta amenaza es una condición necesaria para mejorar las soluciones de IDS actuales (y futuras). Analizaremos críticamente las formas en que un atacante experto puede seguir para atacar un IDS, en cada componente de su diseño. Luego revisaremos y propondremos posibles soluciones para abordar estos problemas. Finalmente, le proporcionaremos al lector un esquema de referencia para apoyar el diseño de soluciones de IDS conscientes del adversario.

Thulin (2015) en su propuesta de “Evaluación de la aplicabilidad de las técnicas de prueba de seguridad en entornos de integración continua”, explica que las metodologías de desarrollo ágil son cada vez más populares, especialmente en proyectos que desarrollan aplicaciones web. Sin embargo, la incorporación de la seguridad del software en enfoques ligeros puede ser difícil. El uso de técnicas de prueba de seguridad a lo largo de un proceso de desarrollo ágil completo ejecutando pruebas automatizadas en entornos de integración continua es un enfoque que se esfuerza por mejorar la seguridad en proyectos ágiles. En lugar de realizar pruebas de seguridad al final del ciclo de desarrollo, dichos métodos permiten la detección temprana y continua de riesgos de seguridad y vulnerabilidades.

El propósito de la tesis es estudiar cómo funcionan las técnicas de prueba de seguridad existentes en entornos de integración continua y qué nivel de seguridad pueden ayudar a garantizar. El trabajo es un análisis cualitativo de diferentes técnicas de prueba de seguridad y evalúa cómo encajan técnicamente en un entorno de integración continua, así como también cómo se adhieren a principios ágiles. Estas técnicas también se analizan con el uso de OWASP Top Ten para determinar qué requisitos de seguridad pueden verificar. El resultado del análisis es que ninguna técnica de prueba de seguridad existente es perfecta para su uso en pruebas de integración continua. Cada técnica tiene sus ventajas y desventajas distintivas que deben tenerse en cuenta al elegir una técnica para trabajar

Singh Bisht (2011) en su investigación acerca de la mejora de la seguridad web por extracción automatizada de la intención de la aplicación web, explica que la última década, la Web se ha transformado en una plataforma informática compleja y distribuida, habilitada principalmente por aplicaciones web como lo demuestra el éxito de sitios como Facebook y YouTube. El objetivo es investigar formas fundamentales de mejorar la seguridad de las aplicaciones web existentes, con esfuerzos de investigación en dos direcciones complementarias: a) técnicas para descubrir fallas de seguridad y b) técnicas para corregir automáticamente fallas de seguridad.

Encontrar y corregir fallas de seguridad en una aplicación web heredada generalmente requiere un conocimiento detallado de su comportamiento. Este conocimiento es el resultado de comprender artefactos de diseño de alto nivel combinados con un análisis del código fuente de la aplicación web. Sin embargo, es bien sabido que el esfuerzo manual dedicado al análisis del código fuente es laborioso y costoso, y a menudo es propenso a errores, además, los artefactos de nivel de diseño a menudo no están disponibles para aplicaciones web heredadas y el único recurso disponible es el código fuente. Si bien el código fuente es la descripción más precisa del comportamiento de una aplicación web, esta descripción se expresa en declaraciones de programa de bajo nivel.

Debido a su naturaleza inherente de bajo nivel, el código fuente no ofrece fácilmente un alto nivel de comprensión del comportamiento previsto de una aplicación que es necesario para identificar y corregir fallas de seguridad.

Esta tesis desarrolla técnicas para calcular el comportamiento previsto de alto nivel de una aplicación web heredada directamente desde su descripción de código fuente de bajo nivel. La filosofía de descubrir intenciones para detectar vulnerabilidades y prevenir ataques descansa en dos simples observaciones: (a) las aplicaciones web se escriben implícitamente asumiendo entradas benignas, y codifican las intenciones del programador para lograr un cierto comportamiento en estas entradas, y (b) elaboradas de manera maliciosa las entradas subvierten el programa y se alejan de las conductas previstas, lo que lleva a ataques exitosos. Aprovechando estas observaciones, desarrollamos técnicas para inferir intenciones en el ámbito de descubrir fallas de seguridad y corregirlas. A través de dos resultados prácticos, demostramos que esta filosofía de inferir la intención es poderosa y es ampliamente aplicable para abordar los desafíos en la seguridad de las aplicaciones web.

El primer resultado en esta tesis presenta un enfoque sistemático para la detección de vulnerabilidades de alteración de parámetros. Estas vulnerabilidades surgen en el código de procesamiento de formularios cuando el lado del servidor no puede volver a validar las entradas que fueron rechazadas por la correspondiente validación del lado del cliente. Para detectar vulnerabilidades, nuestro enfoque explora sistemáticamente el espacio de las entradas que violan las restricciones previstas para encontrar las que el código del lado del servidor no puede aplicar. La evaluación de varias aplicaciones web de fuente abierta y comerciales revela graves problemas de seguridad, como transacciones monetarias no autorizadas en un banco y descuentos no autorizados en una sesión de compras. Estos resultados proporcionan una fuerte evidencia de que la extracción y verificación de

comportamientos deseados, ofrece un mecanismo efectivo para razonar sobre vulnerabilidades en aplicaciones web.

El segundo resultado de esta tesis ofrece un enfoque sólido para evitar las vulnerabilidades de inyección de SQL. Estas vulnerabilidades surgen cuando una aplicación no puede restringir la influencia de las entradas no confiables en las consultas SQL. Este enfoque primero extrae las consultas SQL de aplicaciones web mediante el análisis de su código fuente., la estrategia para corregir aplicaciones web vulnerables implica reescribir el código fuente para emplear sentencias, contra los ataques de inyección SQL.

La evaluación experimental demuestra la eficacia y la escalabilidad de su enfoque mediante la transformación exitosa de grandes aplicaciones de código abierto con una solución robusta incorporar ando declaraciones en aplicaciones web heredadas.

La filosofía de extraer y usar intenciones ofrece una forma sistemática y escalable de combatir los problemas de seguridad en aplicaciones web heredadas. Al presentar resultados extensos en los frentes de detección y prevención, esta tesis ofrece evidencia convincente de que el razonamiento de la intención de la aplicación permite el desarrollo de enfoques basados en principios para mejorar la seguridad de las aplicaciones web.

2.4 Marco Legal

Aquí se considera toda la normativa que constitucionalmente faculta al RENIEC con atribuciones de ser la organizadora y mantener el Registro Único de Identificación RUI y de registrar los hechos que modifican el estado civil así como de expedir el documento que acredita la identidad.

La normativa adicional de soporte es:

a. Declaración Universal de los Derechos Humanos, Artículo 6°.

b. Constitución Política del Perú (1993), Artículo 2°.

c. Ley Nº 26497 - Ley Orgánica del Registro Nacional de Identificación y Estado Civil, Artículo 2°, Artículo 5º.

d. Decreto Supremo Nº 015-98-PCM - Reglamento de Inscripciones del Registro Nacional de Identificación y Estado Civil, Artículo 3°.

e. Ley Nº 29733 - Ley de Protección de Datos Personales, Artículo 1°.

2.5.- Marco conceptual

2.5.1- Padrón Nominal

Es un registro homologado y actualizado que contiene los datos e información de niños menores de la primera infancia es considerado como parte de Modernización Municipal, es parte de la meta del Gobierno e integra a diversas instituciones estratégicas, como el MEF con el presupuesto, el MINSA como responsable de verificar y del RENIEC para el desarrollando del aplicativo informático

El propósito del padrón nominal es consolidar la información autenticada de los niños de la primera infancia y que sea actualizada constantemente, lo que permitirá al Estado promover el acceso del menor de edad a sus diferentes servicios como salud, educación, programas sociales, etc., analizar la brecha no cubierta, reducir las desigualdades, asimismo permitirá que el menor de edad mediante sus padres pueda ejercer sus derechos fundamentales.

La plataforma electrónica de RENIEC, contiene la lista o padrón nominal del registro de menores de edad de la primera infancia, la cual está actualizada con la información que proviene de diferentes fuentes y gobiernos locales que están interconectados, tales como: Nombres y apellidos del titular también del padre y la madre, DNI, Dirección, Programa Social, Seguros y otros.

Los beneficios de contar con el padrón nominal son muy amplios, un enfoque importante para los buenos resultados fue el enfoque de presupuesto por resultado y el cambio en

la manera de planificar, gestionar y monitorear los recursos para el logro de resultados y enfrentar de manera gradual los desafíos que implica la propuesta en sus diversas etapas, como la Planificación y la adecuación de la Normativa preparatoria (dispositivos legales para las modificaciones presupuestales y las directivas de formulación de presupuesto) la Prevención del cambio en la gestión institucional (capacitación activa de actores involucrados) y el Fomento del monitoreo y la evaluación de resultados (metas y objetivos) con el establecimiento de políticas de transparencia (publicación de metas de cada unidad ejecutora).

2.5.2- Brecha social

Se considera una brecha social a la separación, abertura o distancia en lo relacionado con la sociedad, la comunidad y los personas que interactúan entre sí compartiendo la misma cultura, la brecha supone una grieta de la sociedad, la brecha social es una forma de desigualdad social donde el grupo de personas no tienen posibilidades de acceso a los beneficios del Estado, lo que requiere mejorar las condiciones de los no incluidos en busca de un equilibrio social, los indicadores de medición de la brecha social pueden calcularse por nivel de ingresos, educación, calidad de empleo, vivienda, servicios, acceso a la salud y los programas sociales, reducir una brecha social contribuye a mejorar la dignidad del ser humano y ser parte de la inclusión del Estado (Pérez Porto, 2016).

2.5.3- Tecnología Web

Es la tecnología que permite acceder a recursos disponibles en el Internet mediante un navegador para facilitar el acceso a datos e información así como desarrollos que gestionen el conocimiento, debido a su flexibilidad, facilidad de uso y despliegue permite la escalabilidad del sistema; así también propicia la interrelación de las personas, facilita la colaboración y difusión de los conocimientos, la tecnología web puede proporcionar

recursos estratégicos con el Internet, la Intranet o el extranet donde los usuarios pueden ir de explorando un recurso a otro con facilidad, hoy los agentes inteligentes, el chat, los motores de búsqueda y los navegadores facilitan la comunicación (Pérez Capdevila, 2018).

2.5.4- Proyecto OWASP (Proyecto Abierto de Seguridad de Aplicaciones Web)

Estándar con tareas con un plan definido con equipo, en el cual los que lideran un proyecto OWASP tienen la responsabilidad de definir la visión y misión del plan de trabajo del proyecto, el líder de proyecto promueve las actividades bajo un enfoque de seguridad y aunque cada proyecto tiene una lista de distribución asociada, examina sus archivos y se suscribe a cualquiera de ellas en las listas de distribución de proyectos OWASP (Proyectos OWASP)

2.5.5- La identidad e identificación

El solo nombre de las personas no es suficiente para identificarlas, pues ocurre que muchas personas, aún sin tener vínculo de parentesco, lleven el mismo nombre y el mismo apellido, es el caso de los homónimos. Esta confusión o falta de identificación puede crear una serie de perjuicios materiales o morales. Por lo cual, es necesario demostrar la identidad de la persona, está demostración se conoce con el nombre de identificación. Los procesos de identificación, según (Thornberry, 2015).

2.6.- Hipótesis

2.6.1- Hipótesis General

La tecnología web con enfoque OWASP permitirá autenticar de forma segura el registro en línea de menores del Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia.

2.6.2- Hipótesis Nula:

La tecnología web con enfoque OWASP no permitirá autenticar de forma segura el registro en línea de menores del Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia.

2.6.3- Hipótesis Específicas:

H_1) La tecnología Web con enfoque OWASP minimizar el riesgo del registro en línea de los menores del Padrón Nominado no identificados y no documentados.

H_2) La tecnología Web con enfoque OWASP permitirá registrar en línea de forma segura a los menores del Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia.

H_3) La tecnología Web con enfoque OWASP permitirá validar de forma segura el registro en línea de los menores del Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia.

CAPÍTULO III

MÉTODO

3.1.- Tipo y nivel de investigación

3.1.1- Tipo investigación

De acuerdo al propósito, parte de la identificación del problema, su naturaleza, los objetivos de la investigación y la propuesta de trabajo que congrega condiciones metodológicas para considerarla una investigación "aplicada", considerando que para su implementación se utilizan conocimientos relacionados a Tecnologías de Información, la cual es aplicada en los registros de identificación en el Perú; también es una investigación

cuantitativa porque procesara datos reales de los riesgos de la tecnología, así como los datos de los menores de la primera infancia.

3.1.2- Nivel de investigación

De acuerdo a la naturaleza del estudio, se considerada una investigación descriptiva de nivel III, predictivo I.

3.1.3- Método

Los métodos que serán utilizados en la investigación son: descriptivo, explicativo, analítico, sintético, deductivo, inductivo y estadístico, entre otros.

3.2.- Diseño de la investigación

Cuasi experimental porque no aleatoriza las variables con grupos de control no equivalente con valoración antes de aplicar la metodología OWASP y después de aplicarla para asegurar la autenticación y la seguridad de los datos e información según el diseño de (1) y (2).

GE (con OWASP) O_1 O_2 (1)

GC (sin OWASP) O_3 O_4 (2)

3.3.- Estrategia de prueba de hipótesis

Considerando que la investigación en su diseño es cuasi experimental y descriptiva establece hipótesis descriptivas, la muestra es tomada por conveniencia, considerando la Distribución T de Student, con datos obtenidos a partir de los resultados de las pruebas realizadas según el estándar OWASP y la cual se hizo efectiva en dos momentos: t1, al momento de la identificación de la situación actual pretest y t2, luego de aplicar el marco OWASP postest, con un Intervalo (nivel) de Confianza del 95%.

3.4.- Variables

a) Variable Independiente:

x1 : Niños primera infancia

x2 : Tecnología Web

b) Variable Dependiente:

y1 : Brecha social

c) Variable interviniente:

- Autenticación segura

3.4.1- Operacionalización de variables

La operacionalización se realiza considerando las variables independientes y dependientes, sus definiciones conceptual y operacional, sus dimensiones, indicadores e instrumentos de acuerdo a la Tabla 1.

Tabla 1 Operacionalización de variables

	Variable	Definición conceptual	Definición Operacional	Dimensiones	Indicadores	Instrumentos
Variable independiente	Niños de primera infancia	Individuo que su edad comprende entre "cero" y "cinco" años comprende la minoría de edad y toda la infancia.	Considera a los menores de la primera infancia que no han tenido acceso a los servicios del estado formando parte de la brecha social de excluidos	Niños de 0 a 1 Niños de 1 a 2 Niños de 2 a 3 Niños de 3 a 4 Niños de 4 a 5	Número de niños no identificados. Procedencia de niños Lengua de niños Condiciones de los padres	Entrevistas
	Riesgos Tecnología Web	Probabilidad de un suceso que impacte en la aplicación de la tecnología	Materialización de la amenaza que pueda vulnerar a los sistemas web que contienen información sensible de los ciudadanos	Riesgos Tecnología Web	Probabilidad Impacto.	Marco OWASP

Variable dependiente	Brecha social	Separación, abertura o distancia en lo social la comunidad y personas que interactúan entre sí compartiendo la misma cultura, supone una grieta social	Desigualdad social que afecta a la inclusión de los menores de edad en su participación de los programas en los cuales el Estado busca ampliar para el acceso a la salud y educación como parte de la inclusión.	Brecha de atención a salud Brecha de educación Brecha inclusión	-Nivel de alfabetización. -Acceso a Servicios públicos. -Participación en programas sociales	Registro de Indicadores en Padrón Nominal

Fuente: Elaboración propia.

3.5.- Población y muestra

3.5.1- Población

Se considera los menores de edad de la primera infancia que viven en determinado ámbito jurisdiccional de un distrito del Perú, en donde se prevé cerrar brechas de acceso a la identificación, condición básica para el acceso a derechos ciudadanos e intervenciones del Estado en salud, educación, alimentación como objetivo sectorial relacionado a la reducción de la desnutrición en la población infantil de niños de la primera infancia, a fin de hacer seguimiento.

3.5.2 Muestra

La muestra es la porción de niños menores de la primera infancia que representa a la población, los cuales serán empadronados y registrados en el Padrón Nominado en los municipios y distritos de las regiones del Perú en un principio en Amazonas, Huánuco y Cajamarca, para luego extenderse a las otras oficinas registrales a las cuales se pretende dotar de identificación para acceder a sus derechos en salud, educación y alimentación como objetivo sectorial relacionado a la reducción de la desnutrición en la población infantil de niños de la primera infancia, a fin de hacer seguimiento.

3.6.- Técnicas e instrumentos de recolección de datos

Las principales que serán consideradas son:

- Entrevistas (Personas)
- Análisis documental (Documentos)

Revisión documental, se utilizará para adquirir los datos de fuente primaria y secundaria que ayude a esclarecer y aumentar el conocimiento periódicos, reportes y trabajos de investigación.

- También se usaron herramientas de open source y de Denegación de Servicio.

3.7.- Instrumentos de recolección de datos

Guía de entrevista

Técnica para recoger información, una buena entrevista será planificar debidamente dicha entrevista.

El encuestador estará avalado por una carta institucional que lo presentó y señaló explícitamente los fines de la entrevista, afirmando su carácter reservado.

Se concertará una cita. Previamente acercándose donde el entrevistado y se coordinará la fecha en que se realizara la referida entrevista.

El entrevistador estará capacitado para ir sorteando las dificultades de dicha entrevista, como también tuvo las cualidades siguientes: capacidad de comunicación y de emplazarse en la posición del entrevistado con objetividad.

Instrumentos para Web

- Agileload para las pruebas de carga y stress en aplicaciones web,
- SoapUI para testear los webservices y monitorear su accionar
- Seleniun y XPATH también herramientas para probar las funcionalidades y seguridad de la web.

3.8.- Procesamiento y análisis de datos

En el procesamiento se realiza la recolección de datos a partir de los instrumentos establecidos en la matriz de operacionalización de variables los cuales serán luego establecidos en una matriz de indicadores que reflejaran las razones de evaluación de los riesgos y propiciar los programas sociales para la reducción de la brecha social.

CAPÍTULO IV

TECNOLOGÍA WEB CON ENFOQUE OWASP

Esta investigación se busca aplica el enfoque OWASP (Proyecto Abierto de Seguridad de Aplicaciones Web) sobre la plataforma tecnológica Web y de respaldo, bajo los estándares y criterios de seguridad establecidos.

4.1 Autenticación segura del registro en línea

4.1.1 Entorno de pruebas

Se consideran las pruebas de infraestructura en las que se incluyen las pruebas de Software y Hardware.

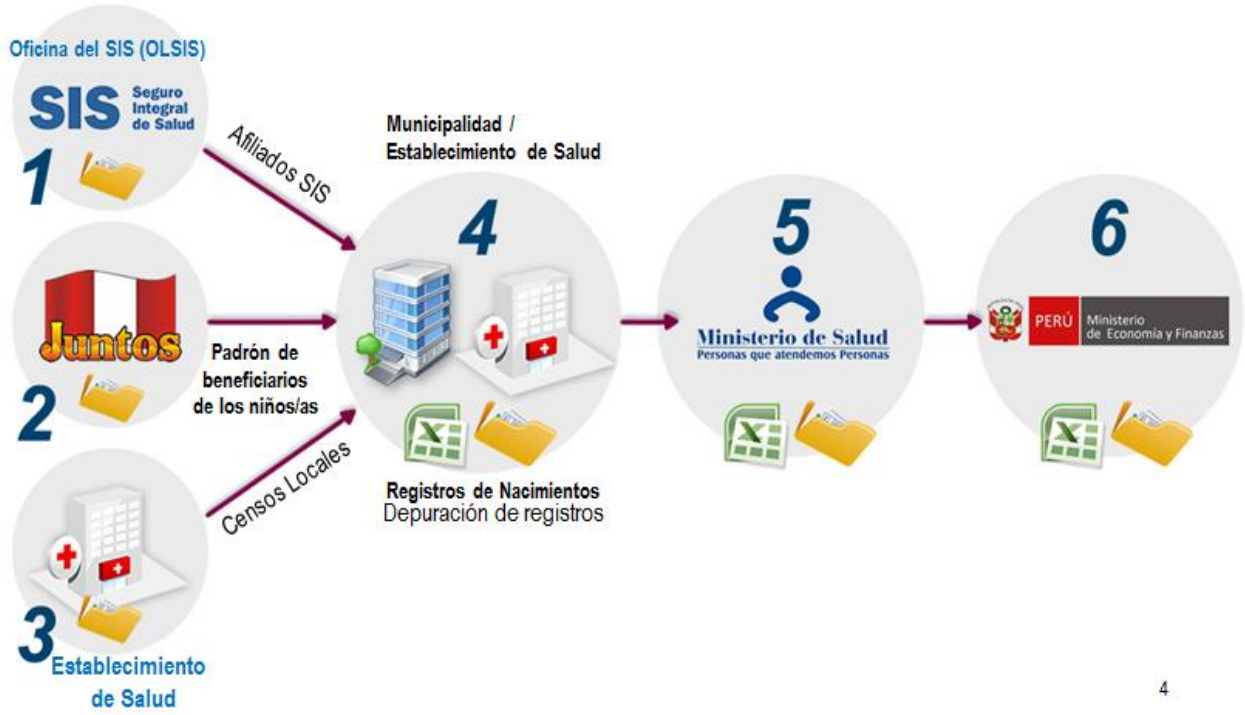
Para las pruebas de software se utilizaron:

- Sistema Operativo Windows
- Internet Explorer en las versiones 9, 10
- Mozilla Firefox version 39+
- Google Chrome version 43+

Para las pruebas de hardware se utilizaron:

Computadoras personales con las siguientes características mínimas de:

- Procesador: Intel Pentium IV
- Memoria RAM: superior a los 512 MB.

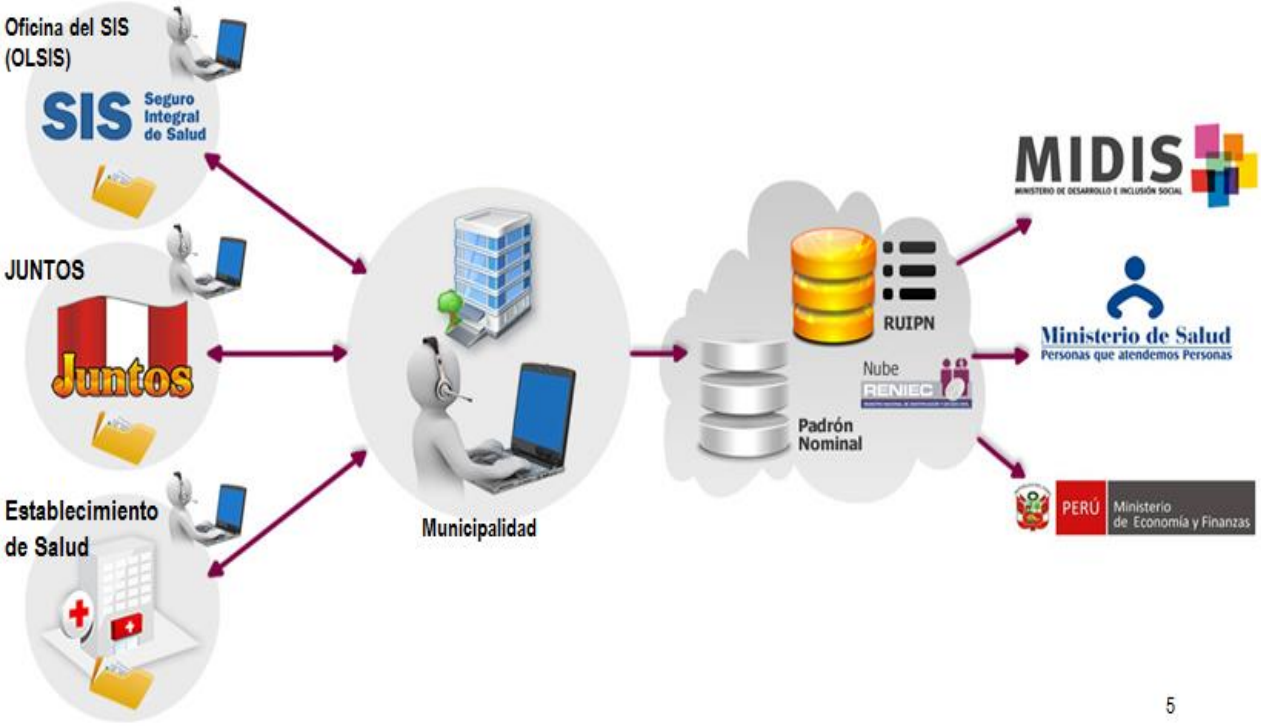


En la Figura Nº 2 se muestra el procedimiento inicial de cómo se administraba y suministraba la información en el padrón nominal, en el flujo del proceso se utilizaba el Excel para recoger la información y trasmitirla a través del sistema. En las municipalidades se registraba a los menores de la primera infancia, su paso era por el sistemas sin medidas de seguridad al MINSA y se reportaba al MEF para evaluar la inversión y hacer seguimiento al proyecto, todo con la información proporcionada por el RENIEC.

Figura 2: Procedimiento inicial del padrón nominal y envío de información.

Fuente: Elaboración propia

En la Figura 3 se muestra el modelo la nueva estructura de comunicación aplicando la tecnología Web con un en foque OWASP, aquí se integran los programas sociales y se realiza el registro en línea autenticado en las municipalidades, la información



5

centralizada puede ser accesada ya procesada con los indicadores respectivos para la toma de decisiones en el MIDIS, MINSA y MEF, propiciando la llegada del Estado a los diferentes sectores no incluidos donde se encuentran los menores de la primera infancia.

Figura 3: Procedimiento actual del padrón nominal y envío de información

Fuente: Elaboración propia

4.2 Monitoreo social con el Padrón Nominal

La implementación de un padrón nominal autenticado de niños de la primera infancia en el padrón nominado está orientado a homologar y actualizar la información de niños que viven en determinado ámbito jurisdiccional de un distrito, de esta manera el padrón brinda la oportunidad de reducir la distancia para obtener la identificación, condición básica del derecho ciudadano y de intervención del Estado, en salud, educación, alimentación entre otros que confluye con el objetivo sectorial relacionado a la disminuir la desnutrición infantil, los resultados del Programa Articulado Nutricional - PAN se miden en la población infantil de niños de la primera infancia, y el padrón Nominal debe contribuir también a hacer seguimiento de la cobertura de educación inicial, la cual es considerablemente menor a la cobertura de educación primaria que es cercana al 100%.

La solución permitirá brindar información oportuna y confiable sobre la cantidad de niños a nivel distrital que contribuye a mejorar los procesos de programación y evaluación presupuestal de los productos y subproductos relacionados al Programa Articulado Nutricional - PAN y otras intervenciones de salud infantil ya que permite calcular con mayor precisión las metas físicas y necesidades de bienes y servicios en función de un dato certero dela población infantil , adicionalmente el padrón contribuye con la implementación del presupuesto por resultados con enfoque territorial en la medida en que permite planificar y monitorear las intervenciones de desarrollo infantil a nivel distrital, articulando esfuerzos intersectoriales y promoviendo la participación comunitaria a través del proceso de verificación y uso de la información a nivel local . La implementación del Padrón Nominal recoge los aprendizajes de esta experiencia.

Los registros electrónicos previos no están actualizados ni han sido homologados, en el nivel distrital, recién a partir del 2012 el MINSA solicito a las regiones que los datos del Padrón Nominado Sectorial sean procesados como condición para la segunda transferencia del presupuesto adicional a favor de los programas presupuestales prioritarios. El documento indica que se ha registrado diversos niveles de desarrollo

regional para la administración de BD de este padrón nominal el cual contaba con un registro electrónico de aproximadamente 1.4 millones de niños a partir de los datos de la Dirección Regional de Salud -DIRESA, el registro cuenta con una cantidad limitada de variables estándar y no está conectado en línea con las bases de datos de otras instituciones públicas. La DGPP del MEF contaba con información parcial de niños de la primera infancia en las regiones de Amazonas, Apurímac, Ayacucho, Cajamarca, Huancavelica y Huánuco gracias a la ejecución de convenios de apoyo presupuestario entre el MEF y los Gobiernos Regionales respectivos que se consolida en padrones nominales estándar.

La información contenida en los padrones será verificada a través de fuentes como la del Seguro Integral de Salud SIS, el Programa JUNTOS y el RENIEC, sin embargo al no contar con un sistema que conecte de manera automática estas bases de datos, el proceso toma cierta cantidad de tiempo que podría evitarse si se contara con un sistema de registro más eficiente.

El ministerio de salud a través de la Oficina General de Estadística e Informática OGEI como pliego responsabilizado técnico del Programa Articulado Nutricional PAN con el Registro Nacional de Identificación y Estado Civil RENIEC y el Ministerio de Economía y Finanzas MEF, acordaron promover e implementar el Padrón Nominal con los siguientes objetivos.

- Registro actualizado y homologado de niños de la primera infancia a nivel distrital
- Identificar a los niños de la primera infancia sin Documento Nacional de Identidad - DNI o Código Único de Identificación CUI.
- Dotar de una herramienta para la gestión de intervenciones a los gobiernos locales regionales para mejorar la salud de los niños de la primera infancia.

El padrón nominal homologado y actualizado fue una meta al 2013 por municipios en regiones y ciudades con más de 500 viviendas urbanas y por las municipalidades con menos de 500 viviendas, esta meta se establece sobre la base de la propuesta que hiciera

la Dirección General de Promoción de la Salud - DGPS y la Oficina General de Estadística e Informática OGEI del Ministerio de Salud responsable de evaluar los resultados de esa meta.

En la construcción del Padrón Nominal se utilizan como insumos las fuentes de información que se han descrito en los párrafos anteriores, así como otras fuentes de información existentes, entre las que cabe destacar la Focalización de Hogares - SISFOH, que a través de las Unidades Locales de Focalización tiene el objetivo de identificar a los posibles beneficiarios de los programas sociales a nivel distrital. El SISFOH guarda un registro de las características socioeconómicas de las personas que son potenciales usuarios en el Padrón General de Hogares - PGH, instrumento que es complementario al Padrón Nominal, ya que proveerá información sobre las características socioeconómicas de un subconjunto de niños de la primera infancia que viven en el distrito.

La OGEI del MINSA conjuntamente con el RENIEC, definirá las características técnicas del padrón Nominal, la Dirección General de Presupuesto Público DGPP designa un consultor individual quien acompañara el proceso de diseño desarrollo e implementación del padrón nominal autenticado y articulara los esfuerzos de las instancias antes mencionadas. La solución informática deberá ser diseñada, desarrollada y validada por RENIEC de modo que sea posible establecer su cobertura a todo el país

La OGEI del ministerio de salud podrá administrar la base de datos completa del padrón, definirá los campos a ser registrados en él y propondrá el nivel de acceso a la información de las entidades involucradas. El RENIEC se encargara de la implementación del Padrón en los distritos seleccionados de amazonas Cajamarca y Huánuco según el anexo 1 del presente documento, y coordinara las actividades con OGEI del MINSA y DGPP del MEF. Finalmente, en el marco del plan de incentivos municipales, las municipalidades de los distritos en donde se implementara el Padrón Nominal serán las únicas instancias responsables de verificar la confiabilidad de los datos consignados y su

actualización periódica, a través de su revisión en línea con otras bases de datos a nivel nacional y su comparación con otras fuentes de información, en estrecha colaboración con otras instancias locales como por ejemplo las Oficinas Registrales de Estado Civil OREC , a fin de mantener un padrón nominal homologado y actualizado. Los Gobiernos locales , regionales , otras instituciones públicas , organizaciones no gubernamentales , u otras personas naturales o jurídicas que lo soliciten , tendrán acceso a los reportes públicos que se puedan generar a partir de la información registrada en el Padrón , de tal forma que se respeten las cláusulas de confiabilidad que el RENIEC cautela por mandato legal.

El objetivo del proyecto es implementar un padrón nominal autenticado, que permita identificar de manera confiable y oportuna a los niños de la primera infancia que viven en determinado ámbito distrital, a través de un instrumento nuevo que haga posible la verificación en línea y en tiempo real su identidad, mantener su registro actualizado y facilitar su verificación a nivel local, para así poder determinar las brechas de acceso a la identificación y a las diferentes intervenciones del Estado de la población infantil del país en relación al cierre de brechas en productos priorizados del Programa Articulado Nutricional PAN.

Los objetivos específicos del proyecto son:

- Diseñar y desarrollar la solución informática que permita implementar y autenticar el padrón nominal distrital de niños de la primera infancia homologado y actualizado en todo el país.
- Implementar el padrón nominal en coordinación con las municipalidades que correspondan, en los distritos seleccionados de Amazonas , Cajamarca y Huánuco
- Proporcionar una herramienta que le permita determinar oportunamente que niño está identificado

- Brindar al MINSA para su administración la base de datos de un padrón nominal que cuente con criterios de autenticidad, integridad , seguridad y conservación indefinida de la información
- Proporcionar la documentación detallada y el respaldo de la solución informática que permita implementar el padrón nominal, describa los procesos metodológicos de análisis diseño desarrollo e implementación y contenga las conclusiones y recomendaciones que el RENIEC considere pertinentes a fin de proveer los insumos necesarios para extender su cobertura en todo el país
- Alcances de servicios / productos del proyecto se complementan con la DGPP otorga la conformidad a los productos entregados por RENIEC y descritos a continuación, previa coordinación con la OGEI del MINSA, pliego responsable del PAN. El Plan de Trabajo que presenta el planeamiento, programación y calendarización de las actividades y tareas que se desarrollaran para el cumplimiento de los productos y resultados establecidos, contiene:
- Descripción detallada de las actividades y tareas, recursos requeridos para la organización, programación, operación de campo, control de calidad, digitación y procesamiento requerido delos datos para la obtención de la base de datos depurada y de la estimación de los indicadores.
- Cronograma de actividades elaborado para coordinar con la DGPP y la OGEI. La DGPP aprobara la versión final de la propuesta, previa coordinación con la OGEI del MINSA.
- Documentos de Análisis Diseño, desarrollo y validación de la solución informática.
- Documentos que contengan la descripción de la solución informática que permita implementar un Padrón Nominal distrital de niños homologado, actualizado y con sus respectivos informes de validación EL RENIEC asegura la alta disponibilidad

y la operatividad de la plataforma informática, que permita evitar la duplicidad de registro de datos y minimizar los tiempos en la elaboración del padrón nominal.

Además se debe contar con la siguiente información:

- Análisis y diseño de la solución informática
- Análisis de requisitos
- Estudio de viabilidad
- Diseño y prototipo del sistema

Y, el aplicativo debe permitir

- Editar los datos de los niños, ej. Domicilio habitual. Control de edición con perfiles de usuarios y los campos necesarios señalando el motivo.
- Registro de datos de los niños con las siguientes consideraciones
- Identificar la procedencia de la entidad que lo reporta
- Identificar la procedencia del CUI, posesión de DNI y el número de Certificado Nacido Vivo - CNV, si es que se encuentran registrados en la BD de RENIEC. En el caso de los niños de la primera infancia sin identificación o registro poseeran un código para su identificación o el CUI registrado en la oficina registral de Estado Civil respectiva para su posterior validación cuando este sea registrado en la BD de RENIEC.
- Validar que el registro del niño sea único, y anotar las veces que ha sido remitido para su registro a través de avisos de alerta.
- Notificación sobre cuántos niños han nacido en el distrito durante el último mes.
- Cancelación del registro y o desactivación de datos de los niños. Control de cancelación con perfiles de usuario, señalando el motivo para ello.

4.3 Desarrollo del aplicativo:

Se desarrollará la interfaz de comunicación para acceder a los datos del padrón según corresponda. la solución debe considerar que el personal autorizado de la municipalidad respectiva es el único responsable del registro. Debe permitir que todo cambio o alteración del mismo sea guardado, para poder ser presentado ante posibles auditorias.

La validación de la solución Informe de prueba piloto: operaciones de validación que permitan concluir sobre la funcionalidad y acceso al aplicativo desde la municipalidad distrital y sobre el procedimiento de uso y consulta de datos.

La actividad incluye:

- Precarga de los datos en el Padrón Nominal sobre la base de la información provista y o gestionada por el MINSA.
- La documentación sobre las pruebas de validación del aplicativo en distritos de Margos y Panao en el Departamento de Huánuco, en el marco de la implementación del piloto de articulación de programas presupuestales con enfoque en la primera infancia. La realización de las pruebas se desarrollaran en la misma municipalidad previa coordinación con el personal autorizado (acordando fechas, contactos locales, modalidad de inducción.
- El monitoreo de la pruebas piloto por representantes de la OGEI, la DGPP y el RENIEC
- Identificación de las principales dificultades en la operatividad del sistema de acuerdo a la EDT según la Figura 4.

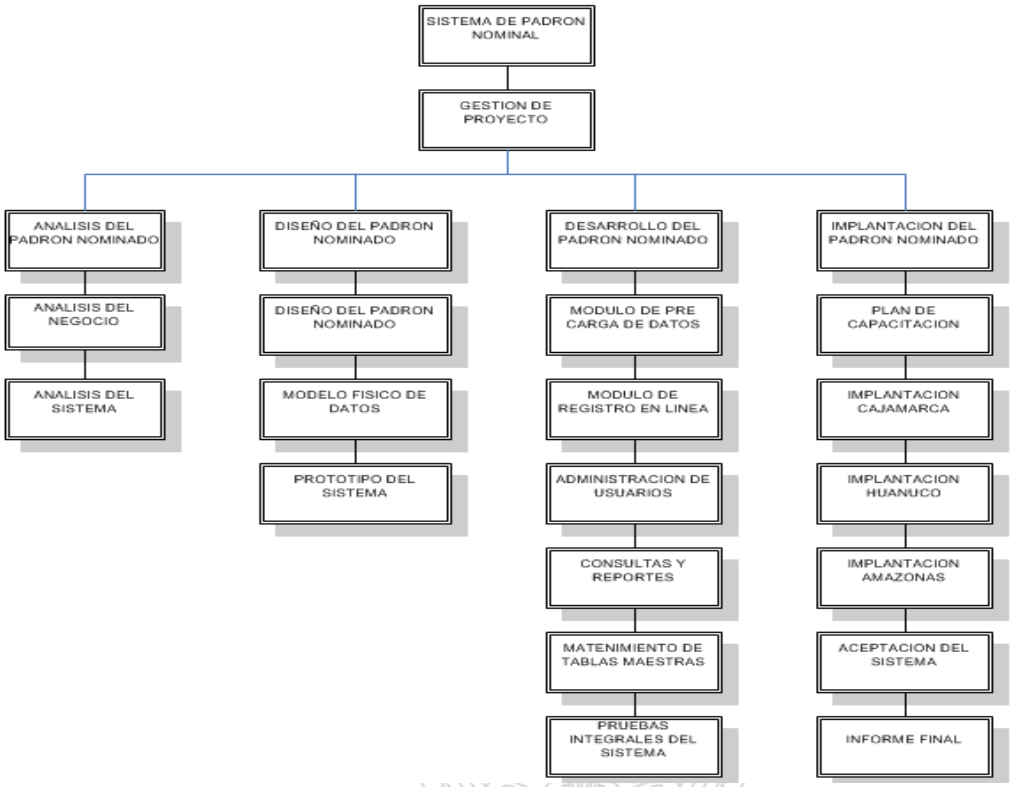


Figura 4

Estructura del Desglose del Trabajo – EDT del Padrón Nominal

Fuente: Elaboración propia

4.4 Plan de implantación:

Informe que describa la coordinación de RENIEC con las Municipalidades, y contiene los documentos metodológicos preparatorios para la implementación del padrón en coordinación con Municipalidades, comunicación con las municipalidades seleccionadas a fin de conocer la situación tecnológica y organización de los actores en el gobierno local, y la validación de las rutas de trabajo para la implementación del padrón, con la elaboración del plan de los distritos pilotos para:

- Mantener comunicación fluida vía correo electrónico, teléfono.
- Mantener comunicaciones formales, de ser necesario via documento entre instituciones.
- Documentos Metodológicos
- Procedimientos de aplicación del padrón Nominal. Esta actividad comprende :
    - Elaboración de documentos metodológicos y auxiliares
    - Elaboración del manual de usuario para su aplicación que contemple el instructivo que para tal efecto elabora el MINSA
    - Plan y programa de capacitación de personal de campo.
    - Documentación complementaria de validación de la solución informática y capacitación
    - Validación complementaria de la solución informática
    - Migración de datos provenientes de otros sistemas existentes, previa acreditación de la información a través del uso de firmas digitales. Incorpora la certificación de que los datos provienen de la fuente acreditada sin posibilidad de manipulación en el envío y recepción.
    - La base de datos se alojará en el servidor de RENIEC y se replicara en línea a la base de datos del MINSA con las variables que se determinen durante la etapa del análisis del aplicativo informático.

- Los Reportes de bases de datos transaccionales de los registros incluidos en el padrón según se acuerde con la OGEI y la DGPP en formatos amigables para los gobiernos locales, establecimientos de salud y otras entidades que se definan.
- El aplicativo debe permitir adjuntar las actas de reuniones de actualización del padrón en el nivel local, según se indica en el instructivo de la meta: Padrón Nominado distrital de niños menores de la primera infancia homologado y actualizado, publicado por el MEF a propuesta del MINSA.
- Control de acceso al sistema. Los accesos serán controlados con perfiles de usuario a los módulos correspondientes, según se coordine con el MINSA y se indique en la normatividad que se defina en la etapa de análisis para las altas y bajas de usuarios según la realidad nacional.

La validación de los reportes sugeridos por la OGEI.

- Modificación del Manual de usuario para su aplicación según instructivo de la meta: Padrón Nominal distrital de niños <6 años homologado y actualizado, con las opciones adicionales que allí se especifican.
- Capacitación e implementación del padrón nominal.
- Capacitación de los funcionarios responsables del registro de datos en el padrón nominal.
- Capacitación a facilitadores propuestos por el MINSA para replicar la implantación a Nivel Nacional.
- Desarrollo del procedimiento de uso y consulta de datos por parte de las instancias correspondientes y según el nivel de acceso a la información previamente acordado con el RENIEC.

- Informe de Avance de aceptación del Sistema del Padrón nominado en los distritos seleccionados.

Este producto está relacionado con la ejecución de la operación de campo así como el monitoreo del mismo, con el objetivo de realizar los ajustes necesarios, para garantizar la calidad de información y el cumplimiento de las actividades en los plazos establecidos. Incluye también la elaboración de las propuestas de los dispositivos normativos necesarios para que el padrón nominal funcione correcta y regularmente. Consiste en la presentación de un informe de avance de aceptación del sistema. Se debe considerar que la municipalidad será la única institución responsable de convalidar la información que reciba de las diferentes fuentes de datos. Designara a un responsable encargado de esta función de:

4.5 Implementación del padrón Nominal

El monitoreo de la operatividad del sistema en los distritos seleccionados está en función de:

- Normativa y respaldo a las soluciones que comprende las siguientes actividades:
  - Implementar la mesa de ayuda respectiva.
  - Iniciar el seguimiento y atención de mesa de ayuda.
  - Informe final
    - Debe contener un informe técnico que incluya
    - Informe de la implementación en los distritos seleccionados
    - Las conclusiones y recomendaciones que el RENIEC considere pertinentes, a fin de proveer los insumos necesarios para extender la cobertura del padrón de todo el país.

La metodología de trabajo comprende la selección de distritos, estos distritos pertenecen al primer quintil de la pobreza regional en las regiones de Amazonas, Cajamarca y Huánuco y son ámbito de intervención del programa JUNTOS son sujetos de medición y seguimiento según los convenios de apoyo presupuestario entre los gobiernos regionales respectivos, el MIDIS y el RENIEC con el MEF.

La coordinación Intersectorial fue fundamental, el RENIEC definió los ítems de coordinación con: la OGEI del MINSA, los campos a ser registrados en el padrón y su respectivo formato, el acceso a la información de los sectores involucrados, los formatos de reporte que arrojara el sistema para los diferentes usuarios, las Municipalidades de distritos seleccionados, el método o protocolo del uso del padrón.

4.6 Homologación y actualización del padrón

Para homologar los datos del patrón se debe contrastar las diferentes fuentes de información de donde provienen los datos y revisar criterios de validación para registrar información debidamente acreditadita. La actualización del padrón se realiza según se indique en el instructivo de la meta: Padrón nominal distrital de niños de la primera infancia homologado y actualizado, para actualizar el padrón, se realizaran reuniones mensuales entre el encargado municipal del padrón nominal y sus representantes de las instancias locales respectivas. Como producto de las reuniones, se elaboras y suscribe un acta en la que se describen los acuerdos tomados y los avances que se han realizado para completar los datos del padrón nominal. El RENIEC realiza la precarga de datos de los diferentes proveedores de información como los establecimientos de salud, el programa Juntos, la Oficina Registral de la Municipalidad, el SIS, el Ministerio de Educación, el programa vaso de leche, entre otros. Para ello se identifica a las fuentes de información

con las cuales se realiza la precarga (a qué nivel se produce dicha información y como se consolida a nivel distrital). Según los establecimientos se toma en cuenta la información provista por el establecimiento de salud de la capital del distrito o de mayor categoría resolutiva en el ámbito distrital.

La municipalidad validara la información precargada en línea desde donde se tenga acceso a internet. Si el registro cuenta con DNI, se hará una comparación automática, luego se verificara si los datos corresponden uno a uno para autenticar el registro. Si el registro no cuenta con DNI, la comparación se hará a través de otros datos como los nombre y apellidos, u otras comparaciones posibles para que se certifique que el niño existe. El registro se guardara con un código de identificación interno. La validación puede hacerse desde donde se pueda acceder a internet.

La municipalidad identifica a los niños que no estén con la información precargada. Y los registra manualmente en la base de datos del padrón nominal (a través del aplicativo del padrón). El registro se guardara con un código de identificación interno, si no se puede **registrar** a ningún niño del distrito, se deberá poder ver a través de una alerta si el niño está registrado en otro distrito , si lo está deberá actualizar el dato de la dirección habitual del niño, previa validación con algún documento que lo acredite.

La municipalidad pide periódicamente los registros de nuevos nacidos e información de nuevos niños captados por otras instituciones, según se indica en el instructivo de la meta: Padrón Nominal distrital de niños homologado y actualizado. Como producto de esta reunión, se elabora un acta certificando que se llevó a cabo esta reunión para intercambiar información sobre el registro de nuevos niños en el padrón nominado. Si hay algún inconveniente en el intercambio de información con el

establecimiento de salud o la municipalidad respectiva, se comunicara a la dirección regional de salud.

El responsable municipal del padrón ingresa los datos, autentica los registros verificando que los datos estén correctos: Comprueba que tengan DNI o CUI, verifica la información con los datos de los padres, o realiza otras comparaciones posibles según sea necesario. Si al autenticar el registro, se identifica que según el acta del mes anterior había niños cuyos datos no eran válidos, se deberá registrar el acta más reciente la razón por la cual no se pudo hacer ese registro.

CAPÍTULO V

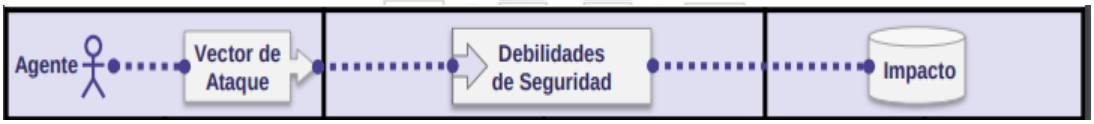
PRESENTACIÓN DE LOS RESULTADOS

5.1 Pruebas realizadas

Las pruebas realizadas fueron las siguientes:

Para todos los casos se siguió el siguiente esquema como se muestra en la Figura 5.

Figura 5 Esquema Ataque -Impacto



Fuente: OWASP top 10

5.1.1 A1 Inyección:

Inyección a SQL, NoSQL, OS o LDAP, se presentan como parte de una consulta, cuando el interprete recibe o envía datos que no son confiables, estos datos pueden o

engañan al intérprete induciendo a la ejecución de comandos para acceder a los datos sin la debida autorización.

Su explotabilidad (3) desde una aplicación específica de cualquier fuente como variables, parámetros, servicios web internos y externos, y a cualquier usuario.

La detectabilidad (3) se da respecto a la prevalecencia (2), los cuales son comunes, especialmente en aplicaciones con en código legacy, los ataques de inyección aprovechan las vulnerabilidades sobre todo en las consultas SQL, NoSQL, LDAP, XPath, en los analizadores XML, en los encabezados SMTP, lenguajes de expresión, parámetros y consultas ORM y hasta en los comandos del SO, la identificación de estas amenazas de inyección se realiza analizando el código y con la ayuda de escáneres y fuzzers.

Para el negocio en el nivel técnico la inyección puede tener un gran impacto en la organización y sus datos causando la divulgación de los datos, la pérdida de información y auditabilidad, así como la denegación de accesos.

5.1.2 A2 Pérdida de Autenticación

Cuando la autenticación y la gestión de sesiones no son implementadas correctamente, entonces se presenta la oportunidad de los atacantes para comprometer a los usuarios, las contraseñas, la implementación así como para suplantar la identidad.

Su explotabilidad (2) desde una aplicación específica se da cuando los atacantes tienen acceso a las combinaciones de usuario, contraseña y por defecto a cuentas administrativas, desde donde realizan ataques por fuerza bruta o de diccionarios.

La detectabilidad (2) en su prevalencia (2) se realiza por pérdida de autenticación en el diseño e implementación de los controles de acceso, aquí la gestión de sesiones es importante con los controles de autenticación presentes en las aplicaciones, puesto que los atacantes detectan lo defectuoso de esta para lo cual utilizan medios manuales y herramientas automáticas.

Respecto al negocio el nivel técnico (3) los atacantes obtienen el acceso a las cuentas o a la cuenta de administrador para comprometer el sistema propiciando el robo de identidad, y caer en el riesgo de divulgación de información sensible.

5.1.3 A3 Exposición de datos sensibles

Las aplicaciones web y los APIs no están exentos de ser violentados para exponer la data como información financiera, de salud o información personal. El robo o la modificación de datos no protegidos adecuadamente facilitan, fraudes o delitos mo son una oportunidad.

Su explotabilidad (2) desde una aplicación específica en lugar de atacar la criptografía, los atacantes roban claves, ejecutan ataques de "hombre en el medio" o roban datos del servidor, o desde el cliente. Se requiere un ataque manual pero pueden utilizase bases de datos con hashes que han sido hechas públicas para obtener las contraseñas originales utilizando GPUs.

La detectabilidad (2) en su prevalencia (3) en los últimos años, ha realizado el ataque de mayor impacto, siendo común no cifrar la data sensible. La criptografía, genera y gestiona claves, algoritmos, cifradores y protocolos. En particular algoritmos débiles de hashing para el almacenamiento de contraseñas. Para los datos en tránsito las debilidades son fáciles de detectar, mientras que para los datos almacenados es muy difícil. Ambos tienen una explotabilidad muy variable.

Para el negocio, los fallos comprometen datos desprotegidos, lo cual incluye información personal como registros de salud, datos personales, credenciales y tarjetas de crédito, que a menudo requieren mayor protección, según lo definido por las leyes o la reglamentación vigente.

5.1.4 A4 Entidades Externas XML (XXE)

Procesadores de XML antiguos o mal configurados evalúan referencias a entidades en documentos XML. Las entidades pueden utilizarse para revelar archivos

internos mediante o internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación.

Su explotabilidad (2) desde una aplicación en la que los atacantes pueden explotar procesadores XML vulnerables si cargan o incluyen contenido hostil en un documento XML, explotando código vulnerable, dependencias o integraciones.

La detectabilidad (3) en su prevalencia (2) es de forma predeterminada, muchos procesadores XML antiguos permiten la especificación de una entidad externa, una URI que se referencia y evalúa durante el procesamiento XML. Las herramientas SAST pueden descubrir estos problemas inspeccionando las dependencias y la configuración. Las herramientas DAST requieren pasos manuales adicionales para detectar y explotar estos problemas. Los testers necesitan ser entrenados para hacer estas pruebas, ya que no eran realizadas antes de 2017.

Para el negocio (3) estos defectos se pueden utilizar para extraer datos, ejecutar una solicitud remota desde el servidor, escanear sistemas internos, realizar un ataque de denegación de servicio y ejecutar otro tipo de ataques.

5.1.5 A5: Pérdida de control de acceso

No aplicar las restricciones establecidas a usuarios autenticados puede generar que los atacantes exploten las vulnerabilidades para acceder de forma no autorizada, a las funcionalidades, datos, cuentas, archivos, pudiendo cambiar derechos de acceso y permisos.

Su explotabilidad (2) desde una aplicación es la explotación del control de acceso es una habilidad esencial de los atacantes. Las herramientas SAST y DAST pueden detectar la ausencia de controles de acceso pero, en el caso de estar presentes, no pueden verificar si son correctos. Es detectable utilizando medios manuales o de forma automática en algunos frameworks que carecen de controles de acceso.

La detectabilidad (2) en su prevalencia (2) está en las debilidades del control de acceso son comunes debido a la falta de detección automática y a la falta de pruebas funcionales efectivas por parte de los desarrolladores de aplicaciones. La detección de fallas en el control de acceso no suele ser cubierto por pruebas automatizadas, tanto estáticas como dinámicas.

En el negocio el impacto técnico incluye atacantes anónimos actuando como usuarios o administradores; usuarios que utilizan funciones privilegiadas o crean, acceden, actualizan o eliminan cualquier registro.

5.1.6 A6: Configuración de Seguridad Incorrecta)

Es un problema muy común y se debe en parte a establecer la configuración de forma manual, ad hoc o por omisión (o directamente por la falta de configuración). Son ejemplos: S3 buckets abiertos, cabeceras HTTP mal configuradas, mensajes de error con contenido sensible, falta de parches y actualizaciones, frameworks, dependencias y componentes desactualizados, etc.

Su explotabilidad (3) desde una aplicación (2) en donde los atacantes a menudo intentarán explotar vulnerabilidades sin parchear o acceder a cuentas por defecto, páginas no utilizadas, archivos, directorios desprotegidos, para acceder al sistema o el negocio.

La detectabilidad (3) en su prevalencia (3) está en las configuraciones incorrectas de seguridad pueden ocurrir en cualquier nivel del stack tecnológico, incluidos los servicios de red, el servidor web y de aplicaciones, la BD, los frameworks, el código y las máquinas virtuales preinstaladas, contenedores, etc. Los escáneres automatizados son útiles para detectar configuraciones erróneas, el uso de cuentas o configuraciones predeterminadas, servicios innecesarios, opciones heredadas, etc.

Para el negocio las vulnerabilidades facilitan a los atacantes el acceso a los datos y las funciones de los sistemas. Ocasionalmente, estos errores resultan en un completo compromiso del sistema.

5.1.7 A7: Cross-Site Scripting (XSS)

Ocurren cuando se ingresan datos no confiables y envían a la web sin validación y la adecuada codificación; o se actualiza la web existente con datos suministrados por usuarios con una API que ejecuta scripts en el navegador. Permiten ejecutar comandos para secuestrar una sesión, realizar un defacement en la web, o redireccionar

En la explotabilidad (3) de una aplicación específica existen herramientas automatizadas que permiten detectar y explotar las tres formas de XSS, y también se encuentran disponibles kits de explotación gratuitos.

En la detectabilidad (3) de la prevalecencia (3), la XSS es la segunda vulnerabilidad más frecuente en OWASP Top 10, y se encuentra en alrededor de dos tercios de todas las aplicaciones. Las herramientas automatizadas pueden detectar algunos problemas XSS en forma automática, particularmente en tecnologías maduras como PHP, J2EE / JSP, y ASP.NET.

En el negocio el impacto de XSS es moderado para el caso de XSS Reflejado y XSS en DOM, y severa para XSS Almacenado, cuando ejecuta instrucciones en el lado que buscan victimizar, para robar credenciales, secuestrar sesiones, o la instalación de software malicioso en el equipo de la víctima.

5.1.8 A8: Deserialización Insegura

Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos y estos objetos pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor.

En la explotabilidad de una aplicación específica se busca lograr la explotación de deserialización que es difícil, ya que los exploits distribuidos raramente funcionan sin cambios o ajustes en su código fuente.

En la detectabilidad (2) de la prevalecencia (2), este ítem se incluye en el Top 10 basado en una encuesta a la industria y no en datos cuantificables. Algunas herramientas pueden descubrir defectos de deserialización, pero con frecuencia se necesita ayuda humana para validarlo. Se espera que los datos de prevalencia de estos errores aumenten a medida que se desarrollen más herramientas para ayudar a identificarlos y abordarlos.

En el negocio no se debe desvalorizar el impacto de los errores de deserialización, pues pueden llevar a la ejecución remota de código, uno de los ataques más serios posibles con gran impacto a los datos y al negocio.

5.1.9 A9: Uso de componentes con vulnerabilidades conocidas

Componentes se ejecutan con privilegios asignados en la aplicación. Si se vulnera un componente, el ataque tomará los datos o el control del servidor, por lo tanto las vulnerabilidades de la aplicación y APIs debilitaran las defensas de las aplicaciones con diversos ataques e impactos.

La explotabilidad Es sencillo obtener exploits para vulnerabilidades ya conocidas pero la explotación de otras requieren un esfuerzo considerable, para su desarrollo y/o personalización

La detectabilidad (2) de la prevalencia (3) con los defectos difundidos. El desarrollo basado fuertemente en componentes de terceros, puede llevar a que los desarrolladores no entiendan qué componentes se utilizan en la aplicación o API y, mucho menos, mantenerlos actualizados. Esta debilidad es detectable mediante el uso de analizadores tales como retire.js o la inspección de cabeceras. La verificación de su explotación requiere de la descripción de un posible ataque.

En el negocio mientras ciertas vulnerabilidades conocidas conllevan impactos menores, algunas de las mayores brechas registradas han sido realizadas explotando

vulnerabilidades conocidas en componentes comunes. Dependiendo del activo que se está protegiendo, este riesgo puede ser incluso el principal de la lista.

5.1.10 A10: Registro y Monitoreo Insuficientes

Es la carencia de respuesta ante ataques que se pueden dar en el tiempo y que intenten manipular, extraer o destruir datos, hoy en día hay una brecha entre el tiempo de detección de una amenaza, siendo típicamente detectado por terceros en lugar de por procesos internos

La explotabilidad (2) de la aplicación específica muestra el registro y monitoreo insuficientes es la base de casi todos los grandes y mayores incidentes de seguridad. Los atacantes dependen de la falta de monitoreo y respuesta oportuna para lograr sus objetivos sin ser detectados.

En la detectabilidad (1) y prevalencia (3) se incluye basado en la encuesta a la industria. Una estrategia para determinar si no se posee suficiente monitoreo al examinar los registros después de las pruebas de penetración. Las acciones de los evaluadores deben registrarse lo suficiente como para comprender los daños que podrían haber causado.

En el negocio los ataques más exitosos comienzan con la exploración de vulnerabilidades. Permitir que el sondeo de vulnerabilidades continúe puede aumentar la probabilidad de una explotación exitosa. En 2016, la identificación de brechas tardó una media de 191 días, un tiempo más que suficiente para infligir daño.

La siguiente Figura 6 resume el resultado de los casos de prueba de vulnerabilidad con la aplicación de OWASP según lo evaluado en un ambiente de desarrollo y pruebas.

Figura 6 Caso de prueba Falla por inyección SQL: A1 Inyección

Fuente: Elaboración propia

Las URL comprometidas que se identificaron y sometieron a las pruebas correspondientes fueron:

http://weblogdev7.reniec.gob.pe:7001/padronn/registromanual/buscarmenor.do?dni=63439104

http://weblogdev7.reniec.gob.pe:7001/padronn/registromanual/formulario.do?coPadronNominal=81243825&_=1442876678835

http://weblogdev7.reniec.gob.pe:7001/padronn/registromanual/guardar.do

De los resultados obtenidos se identificó que no hay confianza en la data de ingreso cliente, requiriéndose

- Comprobar la data de ingreso al servidor.
- Identificar el uso de JDBC, y de ser así usar los métodos PreparedStatement, CallableStatement con parámetros pasados por '?'
- Es preferible usar procedimientos almacenados en la BD.

Caso de Prueba:		CP_001: Falla por Inyección SQL			
Requisitos:		El aplicativo no debe permitir ataques de tipo Inyección SQL			
Propósito de Prueba:		Los datos de RENIEC deben permanecer inalterables y seguros.			
Naturaleza de la prueba:		Positiva			
Modo de prueba:		Sistemático			
Pre-Condiciones:		Usuario registrado, activo y logueado en el sistema.			
Datos de entrada:		• Usuario:			
Descripción de la prueba:		1. Acceder al sistema 2. Ingresar un modulo 3. Ingresar al software OWASP ZAP 4. Aplicar un Escaneo Activo (Nivel Alto) 5. Analizar las Alertas mostradas			
Criterios de éxito		Los pasos se han ejecutado correctamente.			
Post- condiciones:					
Fecha	**Encargado**	**Pruebas**	**Riesgos hallados**	**Nivel de riesgo**	**Comentario**
		1	13	Alto	Inyección SQL puede ser posible. Los resultados de la página se manipularon con éxito utilizando las condiciones booleanas.

- Las cadenas no deben ser concatenadas cadenas en las consultas y en los procedimientos almacenados.

Nivel de riesgo	Número de alertas	Color según nivel
Alto Riesgos con probabilidad de ocurrencia alta	13	Rojo
Medio Riesgos con probabilidad de ocurrencia media	8	Naranja
Bajo Riesgos con probabilidad de ocurrencia baja	2	Amarillo
Informativo	0	-

- Utilizar ejecutar o ejecutar inmediato o funcionalidad equivalente.
- Evitar crear concatenación de cadenas débiles en consultas dinámicas con SQL.
- Considerar una lista blanca o lista negra de caracteres permitidos y no, en lado de ingreso de usuarios.
- Implementar el control de privilegio con restricciones y necesarios a usuarios de la BD.
- Minimizar el impacto por inyección SQL evitando que los usuarios de la BD usen 'sa' o 'db-owner'.

Figura Nº 7 CP_003:X-Frame-Opcions No Set Header : A3 Exposición de datos

Fuente: Elaboración propia

En la Figura 8 la matriz de nivel de riesgo que muestra el número de alertas con una alta probabilidad de ocurrencia.

Figura 8 Matriz de Nivel de Riesgos

Fuente: Elaboración propia

Las alertas identificadas son evaluadas en la matriz de probabilidad e impacto

Caso de Prueba:		CP_003: X-Frame-Options No Set Header			
Requisitos:		El aplicativo no debe permitir ataques de tipo 'ClickJacking', del lado del cliente y del lado del servidor.			
Propósito de Prueba:		Los datos de RENIEC deben permanecer inalterables y seguros.			
Naturaleza de la prueba:		Positiva			
Modo de prueba:		Sistemático			
Pre-Condiciones:		Usuario registrado, activo y logueado en el sistema.			
Datos de entrada:		▪ Usuario:			
Descripción de la prueba:		1. Acceder al sistema 2. Ingresar un modulo 3. Ingresar al software OWASP ZAP 4. Aplicar un Escaneo Activo (Nivel Alto) 5. Analizar las Alertas mostradas			
Criterios de éxito		Los pasos se han ejecutado correctamente.			
Post- condiciones:					
Fecha	**Encargado**	**Pruebas**	**Riesgos hallados**	**Nivel de riesgo**	**Comentario**
		1	1	Medio	La cabecera X-Frame-Options no está incluida en la respuesta HTTP para proteger contra ataques 'ClickJacking'.

Tabla 2 Cálculo de la probabilidad y el impacto para riesgos con OWASP

Probabilidad								
Factores del agente amenaza					Factores de vulnerabilidad			
Nivel de habilidad	Motivo	Oportunidad	Tamaño		Facilidad de des cubrimiento	Facilidad de explotación	Conciencia	Detección de intrusos
5 - Usuario avanzado de computadora	1 - Recompensa baja o nula	4 - Acceso especial o recursos requeridos	5 - Socios		3 - Difícil	3 - Difícil	4 - Oculto	3 - Registrado y revisado
Probabilidad general:				3.500	MEDIO			

Impacto Tecnico					Impacto del Negocio			
Pérdida de con fidencialidad	Pérdida de integridad	Pérdida de disponibilidad	Pérdida de res ponsabilidad		Daño financiero	Daño de reputación	In cumplimiento	Violación de la privacidad
2 - Datos mínimos no sensibles divulgados	0 -	0 -	9 - Completamente anónimo		1 - Menos que el costo de arreglar la vulnerabilidad	1 - Daño mínimo	0 -	5 - Cientos de personas
Impacto técnico general:		2.750	BAJO		Impacto general del negocio:		1.750	BAJO
Impacto general:				2.250	BAJO			

Severidad Global del Riesgo = Probabilidad x Impacto				
Impacto	ALTO	Medio	Alto	Critico
	MEDIO	Bajo	Medio	Alto
	BAJO	Note	Bajo	Medio
		BAJO	MEDIO	ALTO
	Probabilidad			

Niveles de probabilidad e impacto	
0 to <3	BAJO
3 to <6	MEDIO
6 to 9	ALTO

Fuente: Metodología OWASP

Tabla 2 Cálculo de la probabilidad y el impacto para riesgos según OWASP

Fuente: Elaboración propia

Riesgo OWASP	Probabilidad e impacto	Resultados					
		Pruebas pretest sin OWASP			Pruebas postest con OWASP		
A1	Probabilidad	ALTO	7.875	3.500	BAJO	0.910	1.300
	Inpacto			2.250			0.700
A2	Probabilidad	CRITICO	12.160	4.000	BAJO	0.006	1.070
	Inpacto			3.040			0.006
A3	Probabilidad	ALTO	7.343	3.575	BAJO	2.268	2.257
	Inpacto			2.054			1.005
A4	Probabilidad	ALTO	6.241	2.051	BAJO	1.376	1.345
	Inpacto			3.043			1.023
A5	Probabilidad	MEDIO	4.252	2.067	BAJO	1.004	1.003
	Inpacto			2.057			1.001
A6	Probabilidad	ALTO	6.150	3.075	BAJO	2.545	1.777
	Inpacto			2.000			1.432
A7	Probabilidad	ALTO	6.027	3.003	BAJO	1.900	1.324
	Inpacto			2.007			1.435
A8	Probabilidad	ALTO	7.585	2.957	BAJO	2.757	1.650
	Inpacto			2.565			1.671
A9	Probabilidad	ALTO	8.974	3.654	BAJO	1.009	1.004
	Inpacto			2.456			1.005
A10	Probabilidad	ALTO	8.467	3.446	BAJO	2.916	1.763
	Inpacto			2.457			1.654

Tabla 3 Clasificación de Riesgos según OWASP

	Probabilidad										Impacto									
	Factores del agente amenaza				Factores de vulnerabilidad						Impacto Tecnico						Impacto del Negocio			
	Nivel de habilidad	Motivo	Oportunidad	Tamaño	Facilidad de descubrimiento	Facilidad de explotación	Conciencia	Detección de intrusos	Pérdida de confidencialidad	Pérdida de integridad	Pérdida de disponibilidad	Pérdida de responsabilidad	Daño financiero	Daño de reputación	Incumplimiento	Violación de la privacidad
0			Acceso total o recursos costosos requeridos													
1	Sin habilidades técnicas	Recompensa baja o nula			Prácticamente imposible	Teórico	Desconocido	Detección activa en la aplicación		Datos mínimos ligeramente corruptos	Servicios secundarios mínimos interrumpidos	Totalmente rastreable	Menos que el costo de arreglar la vulnerabilidad	Daño mínimo		
2				Desarrolladores, administradores de sistemas					Datos mínimos no sensibles divulgados						Violación menor	
3	Algunas habilidades técnicas				Difícil	Difícil		Registrado y revisado		Datos mínimos seriamente corruptos			Efecto menor sobre el beneficio anual			Un individuo
4		Posible recompensa	Acceso especial o recursos requeridos	Usuarios de la intranet			Oculto		Se revelaron datos críticos mínimos, se divulgaron datos extensos no sensibles					Pérdida de cuentas principales		
5	Usuario avanzado de computadora			Socios		Fácil			Se divulgaron datos críticos extensos	Extensos datos ligeramente corruptos	Servicios primarios mínimos interrumpidos, extensos servicios secundarios interrumpidos			Pérdida de buena voluntad	Violación clara	Cientos de personas
6	Habilidades de red y programación		Algunos accesos o recursos requeridos	Usuarios autenticados			Obvio						Efecto significativo sobre el beneficio anual			
7				Fácil					Extensos datos seriamente corruptos		Extensos servicios primarios interrumpidos	Posiblemente trasable			Violación de alto perfil	Miles de personas
8			Sin acceso o recursos requeridos	Usuarios de internet anónimos	Herramientas automatizadas disponibles	Herramientas automatizadas disponibles	Conocimiento público	No registrado	Todos los datos revelados	Todos los datos totalmente corruptos	Todos los servicios completamente perdidos	Completamente anónimo	Bancarrota	Daño de marca		Millones de personas
9	Habilidades de penetración de seguridad	Recompensa alta						Registrado sin revisión								

Fuente: OWASP

5.2 Prueba de Hipótesis

De acuerdo al procesamiento de datos realizado, respecto a la hipótesis nula se tiene que:

H_0: No existe diferencia entre la prueba Pre test sin OWASP y la prueba Pos test con OWASP, se rechaza la hipótesis nula

H_1: Existe diferencia entre la prueba Pre test sin OWASP y la prueba Pos test con OWASP, se acepta la hipótesis

Se consideró el nivel de significancia 5%

Tabla *Estadísticas de muestras emparejadas*

	Media	N	Desviación estándar	Media de error estándar
Pos test	1,6700	10	0,95581	0,30225
Pre test	7,5070	10	2,13767	0,67599

Se comprobó la normalidad de las variables pre test y pos test

5.2.1 Estadístico de Prueba

T-student para muestras relacionadas o emparejadas

Prueba de muestras emparejadas

	Diferencias emparejadas					t	gl	Sig. (bilateral)
	Media	Desviación estándar	Media de error estándar	95% de intervalo de confianza de la diferencia Inferior	Superior			
Pos test – Pre test	-5,837	2,64302	0,83580	-7,72771	-3,94629	-6,984	9	0,000

Decisión: p-valor = 0,000 < 0.05 se rechaza la hipótesis H_0

Conclusión: Existe diferencia significativa entre la prueba Pre test sin OWASP y la prueba Pos test con OWASP, con un nivel de significancia de 0,05

Anexo 1

Prueba de Kolmogorov-Smirnov para una muestra

		Pretest	Postest
N		10	10
Parámetros normales	Media	7,5070	1,6700
	Desviación estándar	2,13767	,95581
Máximas diferencias	Absoluta	,147	,155
extremas	Positivo	,147	,155
	Negativo	-,145	-,135
Estadístico de prueba		,147	,155
Sig. asintótica (bilateral)		**0,200**	**0,200**

Las dos variables siguen una distribución normal

5.3 Resultados de la variable Brecha social

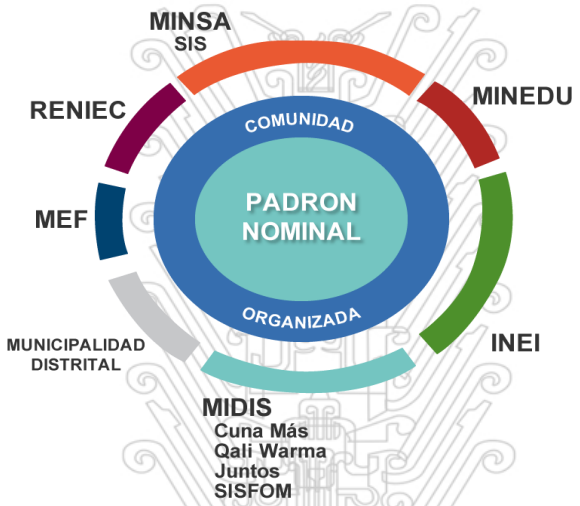
Tabla 4 Indicadores de Padrón Nominal distrital homologado y actualizado de niños de la Primera Infancia

Fuente: Elaboración propia

Nº	Indicador	Definición operacional del indicador	Fórmula		Periodo de medición	Fuente de información	Unidad de análisis	Forma de presentación	Rango de valores semáforos	Variable de corte
			Numerador	Denominador						
1	Porcentaje de niños menores de 6 años de edad que cuentan con DNI.	Niños menores de 6 años de edad que cuentan con DNI.	Nº de niños y niñas registrados en la base de datos del Padrón Nominado con identificación mediante DNI que a la fecha de medición son menores de 6 años	Total de niños y niñas registrados en la base de datos del Padrón Nominado con identificación mediante DNI o con CNV o sin identificación que a la fecha de medición son menores de 6 años	Mensual	Numerador: Base de datos del Padrón Nominado. Denominador: Base de datos del Padrón Nominado	Centro poblado, distrito, provincia, departamento de residencia del menor, establecimiento de salud de atención o adscripción. Distritos priorizados por quintiles regionales y distritales. Grupos de edad: (< 1 año; 1, 2, 3, 4, 5 años) Sexo: varón, mujer.	Tablas, gráficos, mapas.	Verde: igual o mayor del 95% Amarillo: 80 a 94% Rojo: menor de 80%	Fecha de nacimiento del menor y fecha de cierre o fecha de corte (mensual).
2	Porcentaje de niños y niñas menores de 1 año de edad que cuentan con DNI emitido hasta los 30 días de nacido.	Niños y niñas menores de 1 año de edad que cuentan con DNI emitido hasta los 30 días de nacido. Se tomará la fecha de emisión del primer trámite realizado para la obtención del DNI.	Nº de niños y niñas registrados en la base de datos del Padrón Nominado con identificación mediante DNI que a la fecha de medición son menores de 1 año y tuvieron DNI emitido hasta los 30 días de nacido	Total de niños y niñas registrados en la base de datos del Padrón Nominado con identificación mediante DNI que a la fecha de medición son menores de 1 año	Mensual	Numerador: Base de datos Padrón Nominado. Denominador: Base de datos Padrón Nominado.	Centro poblado, distrito, provincia, departamento de residencia del menor, Distritos priorizados por quintiles regionales y distritales. Establecimientos de salud de atención o adscripción.	Tablas, gráficos, mapas.	Verde: igual o mayor del 80% Amarillo: 70 a 79% Rojo: menor de 70%	Fecha de nacimiento del menor y fecha de cierre o fecha de corte (mensual).
3	Proporción de niños y niñas registrados en el Padrón Nominado que tienen menos de 1 año respecto a niños de 1 año de edad.	Niños y niñas menores de 1 año de edad registrados en la base de datos del Padrón Nominado con identificación mediante DNI o con CUI o con CNV o sin identificación respecto a las niñas y niños de 01 año de edad.	Nº de niños y niñas registrados en la base de datos del Padrón Nominado con identificación mediante DNI o con CUI o con CNV o sin identificación que a la fecha de medición son menores de 1 año.	Total de niños y niñas registrados en la base de datos del Padrón Nominado con identificación mediante DNI o con CUI o con CNV o sin identificación que a la fecha de medición tienen 1 año de edad.	Mensual	Numerador: Base de datos del Padrón Nominado. Denominador: Base de datos del Padrón Nominado	Centro poblado, distrito, provincia, departamento de residencia del menor. Distritos priorizados por quintiles regionales y distritales. Sexo: varón, mujer.	Tablas, gráficos, mapas.	Sin rangos	Fecha de nacimiento del menor y fecha de cierre o fecha de corte (mensual).
4	Proporción de niños y niñas con DNI emitido hasta los 30 días de edad cuyo Certificado de Nacido Vivo fue electrónico.	Niñas y niños que nacieron en los últimos 12 meses que tuvieron su DNI hasta los 30 días de edad cuyo Certificado de Nacido Vivo fue electrónico. Se tomará la fecha de emisión del primer trámite realizado para la obtención del DNI.	Niñas y niños que nacieron en los últimos 12 meses cuyo nacimiento fue certificado mediante el sistema de Certificado Nacido Vivo Electrónico (CNVe) cuyo DNI fue emitido hasta los 30 días de edad calculada según la fecha de emisión del DNI que se encuentran registrados en el Padrón Nominal.	Total de niñas y niños que nacieron en los últimos 12 meses previos a la medición del indicador cuyo nacimiento fue certificado mediante el sistema de Certificado Nacido Vivo Electrónico (CNVe) y que se encuentran registrados en el Padrón Nominado.	Mensual	Numerador: Base de datos Padrón Nominado. Denominador: Base de datos Padrón Nominado.	Centro poblado, distrito, provincia, departamento de residencia del menor, Distritos priorizados por quintiles regionales y distritales. Tipo de establecimientos de salud (públicos privados, EsSalud).	Tablas, gráficos, mapas.	Verde: igual o mayor del 90% Amarillo: 80 a 89% Rojo: menor de 80%	Fecha de nacimiento del menor y fecha de cierre o fecha de corte (mensual).
5	Porcentaje de niños y niñas mayores de 3 años y menores de 6 años de edad matriculados en instituciones educativas de nivel inicial.	Niños y niñas mayores de 3 años y menores de 6 años de edad matriculados en instituciones educativas de nivel inicial.	Nº de niños y niñas registrados en la base de datos del Padrón Nominado con identificación mediante DNI o con CUI o con CNV que a la fecha de medición son mayores de 3 años y menores de 6 años de edad que se encuentran matriculados en instituciones educativas de nivel inicial según la base de datos del MINEDU.	Total de niños y niñas registrados en la base de datos del Padrón Nominado con identificación mediante DNI o con CUI o con CNV que a la fecha de medición son mayores de 3 años y menores de 6 años de edad que forman parte del Padrón Nominal	Mensual	Numerador: Base de datos del Padrón Nominado. Denominador: Base de datos del Padrón Nominado	Centro poblado, distrito, provincia, departamento de residencia del menor. Distritos priorizados por quintiles regionales y distritales. Grupos de edad 3, 4 y 5 años.	Tablas, gráficos, mapas.	Verde: igual o mayor del 95% Amarillo: 80 a 94% Rojo: menor de 80%	Fecha de nacimiento del menor y fecha de cierre o fecha de corte (mensual).

Como resultado de la integración de los diversos sectores MINSA (SIS), MINEDU, MEF, INEI, Municipalidades distritales, MIDIS (proyecto Cuna Mas, Qali Warma, Juntos, SISFOM) y RENIEC alrededor del Padrón Nominal, se obtuvo como resultado la participación de la comunidad de forma organizada y como consecuencia abordar la reducción de la Brecha social

Figura de sectores intervinientes en la reducción de la brecha



Fuente: Elaboración propia

Porcentaje de niños de la primera infancia beneficiarios del Programa Juntos.

Para la variable dependiente, tenemos los indicadores que registran la reducción de la brecha social

Niños de la primera infancia que cuentan con DNI por procedencia.

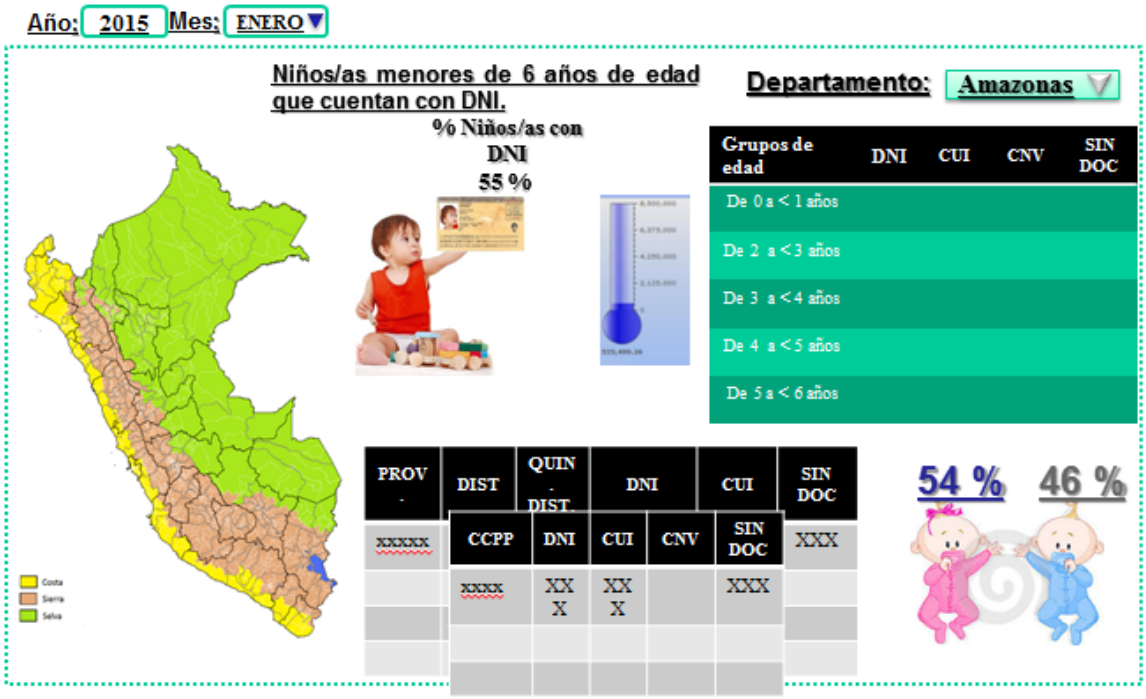
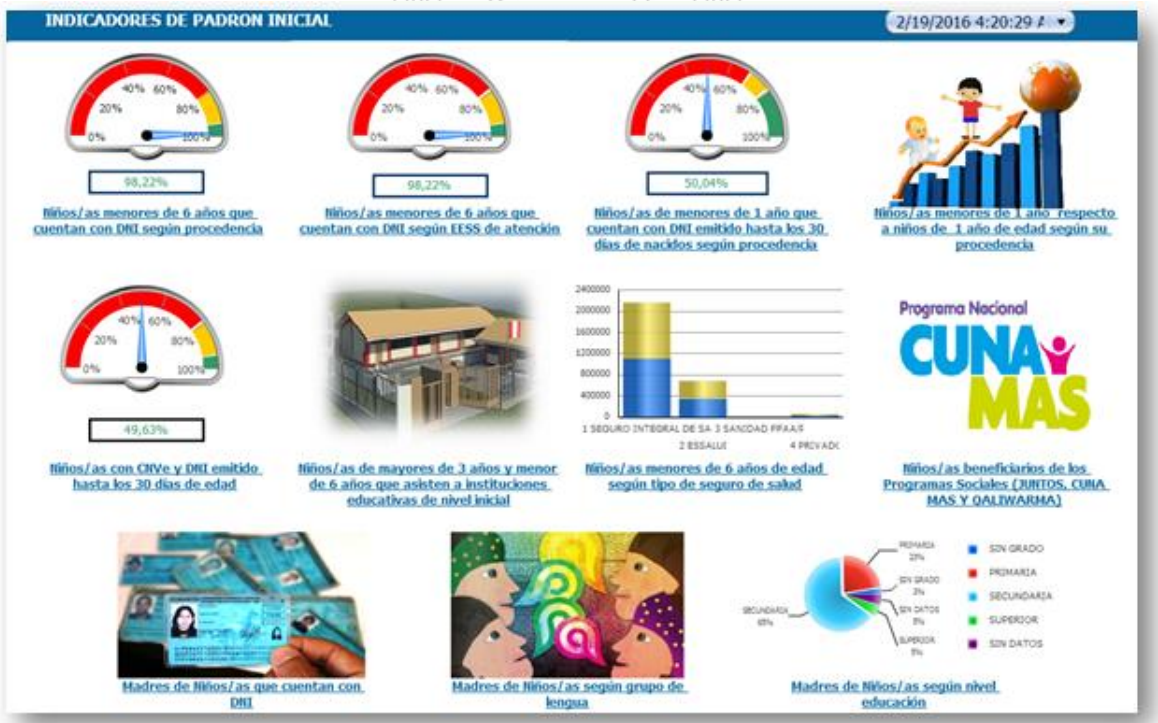


Figura Indicadores de Padrón Nominal



Metas del Plan de Incentivos Municipales

Fuente : Website de RENIEC

La reducción de la brecha social se muestra con los niveles de los indicadores de acceso a los servicios de los niños menores de la primera infancia, que ha sido posible por el monitoreo y la toma de decisiones con aplicación de los programas

CAPÍTULO VI

DISCUSIÓN

5.1 Discusión

De acuerdo a los resultados obtenidos y según Dominguez (2012), la teoría sistemas genera formulaciones conceptuales para ser aplicadas empíricamente en el análisis de sistemas de información que permiten integrar diversos conocimientos, aquí el sistema de información está representada por los diversos sistemas que cumplen la función de generar información, como es el caso del sistema de registro de identificación que se incorporará al Padrón Nominado, así como también incorpora el marco OWASP a la tecnología Web para asegurar el acceso al servicio Web.

Respecto a la teoria de Scandroglio, López, & San José, (2008) en la que explican que la Teoría de la Identidad Social (TIS) tienen gran influencia en la Psicología Social, es importante resaltar que todo ciudadano tiene derecho a la identificación, como también es un deber del Estado tener registrado a toda su población, en tal sentido los proyectos sociales como resultado de esta identificación influye en el comportamiento grupal considerando las dimensiones, el contexto y los procesos de identificación, especialmente para los niños menores de la primera infancia.

Luego obtenidos los resultados de la prueba de hipótesis, y contrastando los resultados con la posición de Klooster (2016) se coincide en que la aplicación de una metodología de prueba de seguridad verifica si está protegida y es resistente la funcionalidad contra los posibles ataques al registro de los datos y a los datos procesados del Padrón Nominado, es importante destacar que los estándares de seguridad como el de OWASP establece los requisitos que debe cumplir el software como un proceso necesario para verificar la seguridad de una aplicación web mediante un checklist de seguridad.

Es importante considerar en esta discusión que el descubrimiento de vulnerabilidades es importante, pero también muy importante es estimar el riesgo asociado para el negocio y que seguir el enfoque OWASP proyecta el nivel de dificultad de los riesgos para la organización al decidir qué acción tomar al momento que emergen los riesgos y analizar riesgos, lo importante aquí es el enfoque que se de a los riesgos.

La implementación de tecnología web con enfoque OWASP para asegurar el registro en línea de menores de la primera infancia en el Padrón Nominado se refuerza con la posición de Corona (2010) en cuanto a que las debilidades del procesamiento de la información limitan la exposición de los datos sensibles en la web considerando que Internet es el vector principal en el procesamiento e intercambio de información, así como también está comprobado, que la debilidad de la seguridad está en los usuarios que navegan en la Web y en las aplicaciones web que procesan la información que son los "puntos débiles" lo que a su vez trae como consecuencia no exponer los datos para evitar los riesgos , lo que a su vez implica no llegar a los sectores no incluidos de niños de la primera infancia para un significativo aporte a la reducción de la brecha social.

La posición de Thulin (2015) en su propuesta de la aplicabilidad de las técnicas de prueba de seguridad se confirma con los resultados obtenidos en esta investigación, respecto a la importancia de las técnicas y marcos de seguridad como OWASP Top Ten para determinar los requisitos de seguridad, y a pesar de que ninguna técnica de prueba de seguridad existente es perfecta cada técnica tiene el mismo objetivo, como también lo aborda Singh Bisht (2011) en su investigación acerca de la mejora de la seguridad web por extracción de la aplicación web apoyándose como ya lo hemos visto anteriormente en las técnicas para descubrir fallas de seguridad y corregir automáticamente esas fallas de seguridad y atacar las vulnerabilidades como el de inyección de SQL.

5.2 Conclusiones

- Se logró el objetivo de autenticar de forma segura el registro en línea de menores de la primera infancia en el Padrón Nominado, asimismo se comprobó la hipótesis de que la implementación de tecnología web con enfoque OWASP permite autenticar, lo que significa acreditar , asegurar y certificar la veracidad de los datos a procesar en las transacciones y procesamiento del registro en línea de menores de la primera infancia del Padrón Nominado se realiza segura habiéndose reducido los riesgos con los 10 estándares OWASP de un nivel alto a un nivel bajo, permitiendo llegar con tecnología web a las más alejadas oficinas registrales proporcionando indicadores para reducir la brecha social.

- Se logró el objetivo de minimizar el riesgo del registro en línea de menores de la primera infancia en el Padrón Nominado no estaban identificados y tampoco documentados comprobándose la hipótesis de que la implementación de tecnología web con enfoque OWASP permite minimizar el riesgo del registro en línea de los menores del Padrón Nominado no identificados y no documentados, la minimización del riesgo se determina al reducir el riesgo de un nivel de alto a un nivel bajo, propiciando no solo identificar y registrar, sino también documentar a los menores de la primera infancia quienes pueden ya ser incluidos y beneficiarios de los programas sociales.

- Se logró el objetivo de registrar en línea con tecnología web de forma segura a los menores de la primera infancia del Padrón Nominado asimismo la implementación de tecnología Web con enfoque OWASP ha permitido registrar a los menores de la primera infancia, por medio de los indicadores que muestran

resultados favorables en los principales sectores como economía y salud para la reducción de la brecha social de los niños de la primera infancia.

- Se logró el objetivo de validar de forma segura el registro en línea de los menores del Padrón Nominado asimismo la implementación de la tecnología Web con enfoque OWASP con los resultados obtenidos en el periodo de delimitación temporal valida de forma segura y con información confiable el registro de los menores lo cual ha permitido tener un conocimiento de la situación real, así como planificar las actividades de proyección social del MEF, MINSA, MINEDU como aporte a la reducción de la brecha social de la primera infancia.

5.3 Recomendaciones

- Las técnicas, estándares, marcos y metodologías de seguridad como el OWASP aplicados a la tecnología web deben ser considerados a las diferentes instituciones del Estado a fin de propiciar una mayor llegada al ciudadano mediante el Gobierno Electrónico, hoy llamado Gobierno Digital.

- La tecnología web debería estar integrada a fin de generar una convergencia tecnológica, siempre bajo estándares de seguridad de la información y de ciberseguridad, considerando que muchos datos o información tienen que ser expuestos a los ciudadanos para fomentar su participación y agilización de servicios.
- La adopción del marco y su estándares OWASP debe de considerarse como una alternativa de seguridad, considerando que es abierto y colaborativo, y que además recoge diversas experiencias que son actualizadas constantemente.

VII.- REFERENCIAS BIBLIOGRÁFICAS

Avella Villamil, A. M. (2015). *¿QUE EFICACIA HA TENIDO LA POLÍTICA PÚBLICA COLOMBIANA DE PRIMERA INFANCIA "DE CERO A SIEMPRE"?* Tesis, UNIVERSIDAD MILITAR NUEVA GRANADA, RELACIONES INTERNACIONALES Y ESTUDIOS POLÍTICOS, Bogotá. Colombia.

Corona, I. (2010). *Deteccion de ataques a la Web.* Universidad de Cagliari, Departamento de Ingenieria Electrica y Electronica. Cagliari: Universidad de Cagliari.

Dominguez, L. A. (2012). *Análisis de Sistemas de Información* (Primera ed.). (R. T. MILENIO, Ed.) Tlalnepantla: RED TERCER MILENIO. doi:978-607-733-105-6

Klooster, K. (2016). *Applying a Security Testing Methodology: a Case Study.* UNIVERSITY OF TARTU, Institute of Computer Science. Tartu: UNIVERSITY OF TARTU.

Lay Lisboa, S. L. (2015). *LA PARTICIPACIÓN DE LA INFANCIA DESDE LA INFANCIA La Construcción de la Participación Infantil a Partir del Análisis de los Discursos de Niños y Niñas.* Tesis Doctoral, Universidad de Universidad de Valladolid, Facultad de Educación y Trabajo Social Departamento de Pedagogía, Segovia, España.

MINSA. (2018). *Ministerio de Salud.* Recuperado el 14 de Enero de 2018, de http://www.minsa.gob.pe/portalweb/02estadistica/estadistica_26.asp

Ñique Morazzani, V. A. (2016). *IMPLEMENTACIÓN DE SOLUCIÓN DE AUTENTICACIÓN SEGURA BASADA EN DOBLE FACTOR EN UNA ENTIDAD DEL ESTADO.* Tesis, Universidad San Ignacio de Loyola, FACULTAD DE INGENIERÍA, Carrera de Ingeniería Informática y de Sistemas, Lima, Perú.

OWASP. (s.f.). Recuperado el 14 de Enero de 2018, de https://www.owasp.org/index.php/Proyectos_OWASP

Pérez Capdevila, J. (2018). *Tecnoweb2.* Recuperado el 14 de Enero de 2018, de http://tecnoweb2.com/tecnologias-web

Pérez Porto, J. (2016). *Definicion.* Recuperado el 14 de Enero de 2018, de https://definicion.de/brecha-social/

Scandroglio, B., López, J., & San José, C. (2008). *La Teoría de la Identidad Social: una síntesis crítica de sus fundamentos, evidencias y controversias.* Paper, Universidad Autónoma de Madrid, Madrid. Obtenido de http://www.psicothema.es/pdf/3432.pdf

Singh Bisht, P. P. (2011). *Improving Web Security by Automated Extraction of Web Application Intent.* University of Illinois, Computer Science. Chicago: University of Illinois.

Thornberry, G. (2015). *PALESTRA PORTAL DE ASUNTOS PÚBLICOS DE LA PUCP.* (PUCP, Ed.) Recuperado el 14 de Enero de 2018, de http://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/11954/quien_soy_yo_Thornberry.pdf?sequence=1

Thulin, P. (2015). *Evaluation of the applicability of security testing.* Linköpings universitet, Department of Computer and Information Science. Linköping: Institutionen för datavetenskap.

Urquizo Limache, G. R. (2016). *La capacitación de los registradores civiles impartida por el Registro Nacional de Identificación y Estado Civil (RENIEC) y su eficiencia en la función registral.* Tesis de magister en Gerencia Social, PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ, ESCUELA DE POSGRADO, Lima, Perú.

ANEXOS

ANEXO 1 : MATRIZ DE CONSISTENCIA

TÍTULO: "TECNOLOGÍA WEB CON ENFOQUE OWASP EN LA AUTENTICACIÓN SEGURA DEL REGISTRO EN LÍNEA DE MENORES DEL PADRÓN NOMINADO COMO APORTE A LA REDUCCIÓN DE LA BRECHA SOCIAL DE LA PRIMERA INFANCIA"

GRADUANDO: DANILO ALBERTO CHÁVEZ ESPÍRITU

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	INDICADORES	METODOLOGÍA
Problema General ¿De qué manera es posible autenticar de forma segura el registro en línea de menores de la primera infancia en el Padrón Nominado como aporte a la reducción de la brecha social? **Problemas Específicos** a) ¿De qué manera es posible minimizar el riesgo del registro en línea de los menores del Padrón Nominado no identificados y no documentados? b) ¿De qué manera es posible registrar en línea con tecnología web de forma segura a los menores del Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia? c) ¿De qué manera es posible validar de forma segura el registro en línea de los menores del Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia?	**Objetivo General** Autenticar de forma segura el registro en línea de menores en el Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia. **Objetivos Específicos** a) Minimizar el riesgo del registro en línea de los menores del Padrón Nominado no identificados y no documentados. b) Registrar en línea con tecnología web de forma segura a los menores del Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia. c) Validar de forma segura el registro en línea de los menores del Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia.	**Hipótesis General** La tecnología web con enfoque OWASP permitirá autenticar de forma segura el registro en línea de menores del Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia. **Hipótesis Especificas** H1) La tecnología Web con enfoque OWASP minimizar el riesgo del registro en línea de los menores del Padrón Nominado no identificados y no documentados. H2) La tecnología Web con enfoque OWASP permitirá registrar en línea de forma segura a los menores del Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia. H3) La tecnología Web con enfoque OWASP permitirá validar de forma segura el registro en línea de los menores del Padrón Nominado como aporte a la reducción de la brecha social de la primera infancia.	**Variable independiente** • x1 : Niños primera infancia • x2 : Tecnología Web **Variable dependiente** • Brecha social **Variable interviniente** • Autenticación segura • a) Variable Independiente: • x1 : Niños primera infancia • x2 : Tecnología Web	Número de niños no identificados. Procedencia de niños Lengua de niños Condiciones de los padres Niños que estudia. Niños que cuentan con seguro de salud. Nivel de alfabetización. -Acceso a Servicios públicos. -Participación en programas sociales	**Tipo y nivel investigación** a) Tipo de Investigación Aplicada, cuantitativa b) Nivel de Investigación Descriptiva. Explicativa **Población y Muestra** a) Población Grupo de menores no identificados. b) Muestra Menores de 6 años de los departamentos de Amazonas, Huánuco y Cajamarca. **Métodos** Descriptivo, explicativo, analítico, síntesis, deductivo, inductivo y estadístico.
