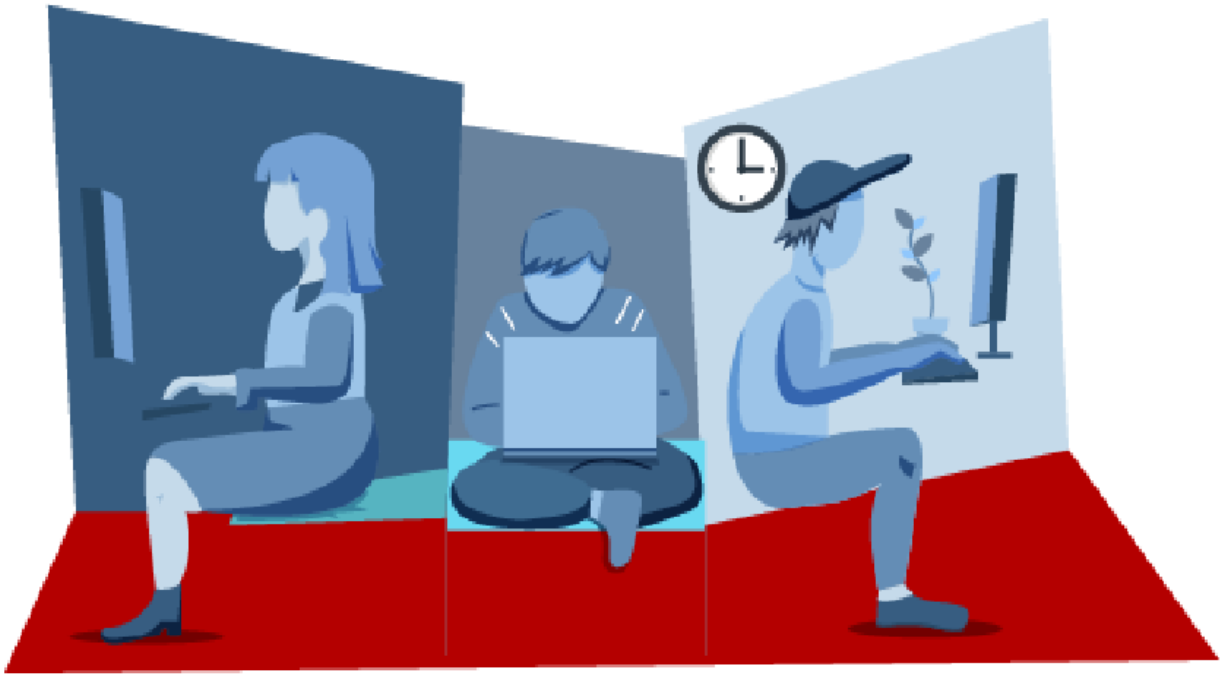
Análisis de SDLC considerando normativa vigente



Módulo PRO203 – 9003 – 2021 Programación Segura
Semana 2
Docente Daniela Salinas Casas
Estudiante Camilo Villavicencio Garrido

Índice

Introducción

En el presente documento se analizará la formulación de un sistema desarrollado para la gestión de entrega de subsidios para SERVIU. El análisis contempla la identificación de los procesos que se necesitan desarrollar, la determinación de qué metodología aplicar para producirlo, un diagrama de casos de uso y, finalmente, un diagrama de amenazas acompañado del análisis del reporte generado por el software Microsoft Threat Modeling Tool 2016, que contemplara una revisión a las amenazas que enfrenta el sistema, siguiendo la metodología de modelado de amenazas STRIDE.

Caso propuesto

El SERVIU, para el año 2021 necesita implementar un sistema que permita gestionar el nuevo subsidio de compra de casas usadas, dirigido a las clases sociales. Las reglas del negocio de este nuevo Subsidio son explicadas por Roxana Recabarren, encargada de la puesta en marcha del nuevo subsidio, ella explica lo siguiente:

Cada año, entre marzo y mayo, los ciudadanos que ganan un sueldo líquido menor a $880.000.- pesos, pueden postular al subsidio habitacional de la clase media, inscribiéndose en la Oficina Regional de SERVIU de su región. Al inscribirse debe señalar todos los datos personales. Si el postulante es casado, además debe señalar el nombre completo de su cónyuge. En cambio, si el postulante es soltero, debe señalar los años que lleva trabajando y su fecha de nacimiento. Un postulante debe presentarse como casado o soltero no ambas situaciones

Cada ciudadano puede inscribirse sólo una vez en su vida. La inscripción debe señalar, además de todos los datos del ciudadano relacionado, el número correlativo único, la fecha de inscripción, debe adjuntar las fotos del ciudadano al momento de inscribirse.

Luego de la inscripción, SERVIU le entregará al ciudadano una libreta de ahorro del banco que lleva registrado en la carátula su número, fecha de creación y vigencia, además de la foto y firma del postulante. Este instrumento es intransferible, frente a su pérdida el banco podrá entregarle otra, dejando no vigente la original. Cada libreta se asocia sólo a una cuenta corriente del banco. De esta cuenta se conoce su número único, monto Inicial de apertura y fecha de apertura. Cada cuenta corriente está asociada obligatoriamente a una libreta de ahorro.

Al postular a este subsidio, el ciudadano se compromete a realizar depósitos mensuales a la cuenta corriente, por un monto mínimo correspondiente al 2% de su sueldo mensual. Cuando se ha alcanzado un ahorro mayor o igual a $500.000, debe acercarse a la oficina regional de Serviu con su libreta donde se detallan todos los depósitos que ha efectuado, monto, fecha y sucursal bancaria en donde se realizó. La lista de todos sus depósitos ordenados por fecha se va imprimiendo en las hojas de la libreta de ahorro.

Llegado a este punto, podrá llenar una solicitud de subsidio, donde se indican los datos de la vivienda que el ciudadano postulante quiere comprar, incluyendo: identificador o número fiscal de la vivienda, la dirección, fecha de construcción, metros cuadrados del terreno y precio de venta. Además, el documento de solicitud registra su identificador, su fecha de creación, y el monto solicitado de subsidio. El postulante pude solicitar hasta un 70% del precio de la vivienda.

Cada postulante puede hacer tres solicitudes, con una vivienda distinta por solicitud.

Los Evaluadores del Serviu, se encargan de revisar el estado de cada vivienda inscrita, realizando un registro de las condiciones generales de la misma considerando, además, las características de su entorno. Esta actividad pondera un puntaje de 1 a 100 puntos dependiendo del resultado de la valoración. Cada solicitud de subsidio debe asociarse a una Evaluación.

Los postulantes pueden hacer seguimiento telefónico del estado de su evaluación, quedando registrada su intervención en el proceso con la hora y el día en que fue realizada.

Desarrollo

Identificación de procesos que la empresa desarrolla, Establecimiento de necesidades que presentan.

Entendiendo por proceso *una unidad de actividad que se caracteriza por la ejecución de una secuencia de instrucciones, posee un estado actual y utiliza un conjunto de recursos de sistemas asociados*[1] en el caso propuesto se han encontrado los siguientes, con las señaladas necesidades:

Proceso	**Necesidades**
Inscripción de postulante	• Clase de usuario: postulante. • Registro de postulante en plataforma de oficina serviu de su región. Opera entre marzo y mayo. • Formulario de inscripción de postulante, para que ingrese datos personales. ○ Requisitos adicionales dependiendo, si es casado o soltero; nombre de cónyuge o años trabajando y fecha de nacimiento, respectivamente. • Cada postulante puede inscribirse solo una vez. • Otros datos señalados en la inscripción: número correlativo único, fecha de inscripción y fotos del postulante al momento de inscribirse.
Entrega de libreta de ahorro a postulante.	• Entrega de liberta de ahorro, que en su carátula señala: número, fecha de creación y vigencia, además de foto y firma del postulante. • Libreta es intransferible
Reposición de libreta de ahorro a postulante (en caso de pérdida)	• Entrega de nueva libreta, que deja no vigente la anterior.
Confirmación de requisitos para solicitar subsidio	• En oficina serviu se recibirá a postulante que ○ debe tener registro de depósitos mensuales de al

1 Stalling, 2005.

	menos un 2% de su sueldo menual. ◦ Debe haber reunido un ahorro mayor o igual a $500.000.
Solicitud de subsidio.	• La solicitud debe señalar: identificador o número fiscal de la vivienda, dirección, fecha de construcción, m² del terreno y precio de venta. • También señalará: identificador de solicitud, fecha de creación, monto solicitado de subsidio (que podrá ser hasta el 70% del precio de la vivienda). • Cada postulante puede realizar hasta tres solicitudes.
Registro de Evaluación de vivienda, realizada por evaluadores de Serviu	• Clase de usuario: evaluador • Evaluadores de Serviu revisan el estado de cada vivienda inscrita . Realizan registro de condiciones generales y entorno. Este registro tiene una puntuación entre 1 y 100. • Cada solicitud de subsidio estará asociada a una evaluación.
Registro de seguimiento telefónico del estado de la evaluación realizada por los postulantes.	• Clase de usuario: operador de callcenter • Plataforma para callcenter que entregue información respecto al estado de las solicitudes.

Identificación del beneficio que el sistema de información traerá a la empresa, justificar

La elevada cantidad de información que requiere gestionar Serviu para la entrega de subsidios hace imposible considerar la posibilidad de no utilizar un sistema integrado que comunique dentro de la organización la información necesaria para cumplir con su cometido. El sistema de información permitirá a Serviu entregar un servicio expedito y eficiente, pues al tener centralizada la información, será posible hacer un seguimiento efectivo tanto de las solicitudes, como de los postulantes, y su estado dentro del sistema.

La automatización de la revisión de requisitos de los distintos pasos mitigará de forma sustantiva la posibilidad de incurrir en errores dentro del proceso de postulación.

Metodología de desarrollo

Para el desarrollo de este sistema, la metodología que mejor se adapta es la de tipo tradicional ya que los requerimientos responden a las necesidades de un organismo estatal, cuyo funcionamiento se determina por medio de la ley, por lo tanto, existe un menor riesgo de aparición de nuevos requerimientos en el transcurso del desarrollo.

Otra ventaja de utilizar la metodología tradicional es que el sistema se entregará funcionado completamente a la organización que se limitará a su uso, sin necesidad de señalar nuevos requerimientos o cambios en su funcionamiento.

Diagrama de casos de uso

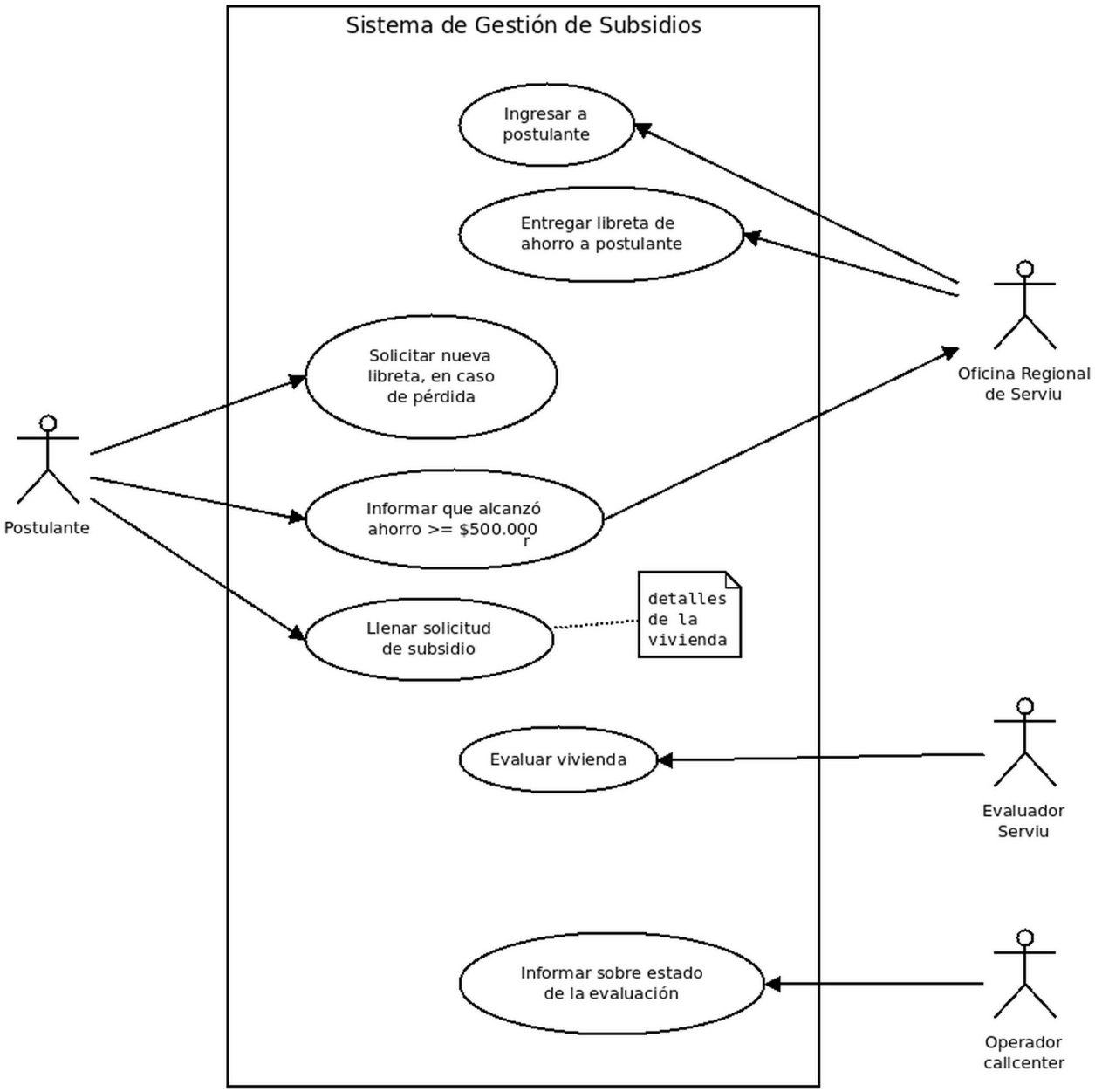
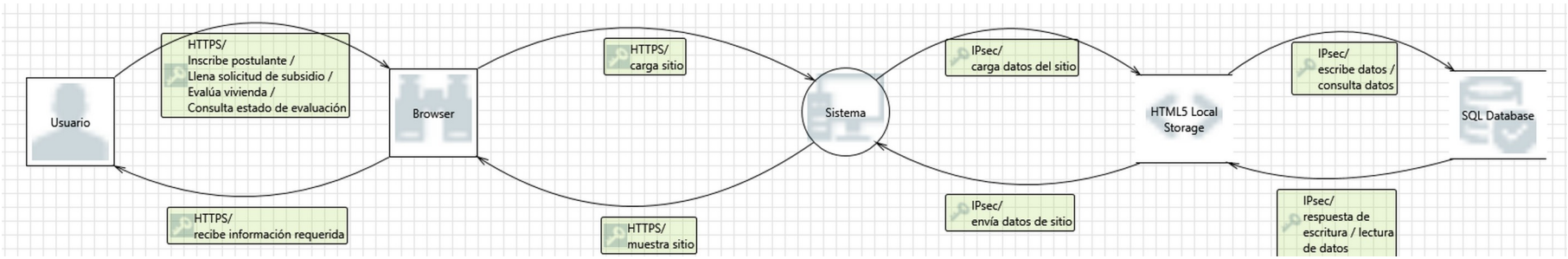


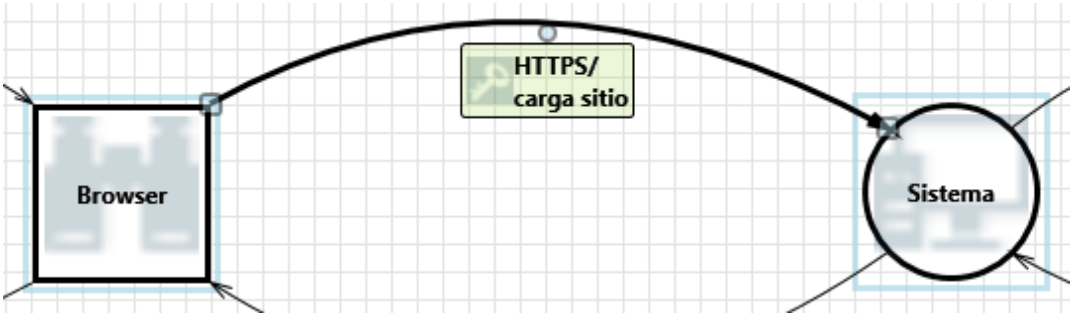
Diagrama de Amenazas



Análisis de informe de amenazas basado en stride

El siguiente análisis ha sido realizado a partir del reporte de amenazas generado por Microsoft Threat Modeling Tool 2016. Las mitigaciones propuestas están destacadas:

Interaction: HTTPS/ carga sitio



1. Spoofing the Browser External Entity

[State: Not Started] [Priority: High]

Category: Spoofing

Description: Browser may be spoofed by an attacker and this may lead to unauthorized access to Sistema. Consider using a standard authentication mechanism to identify the external entity.

Justification: Se omitirá toda información existente en caché o cookies que pueda intervenir en la lectura del sitio.

Short Description: Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.

2. Cross Site Scripting

[State: Not Started] [Priority: High]

Category: Tampering

Description: The web server 'Sistema' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.

Justification: Se omitirá cualquier dato que se esté recibiendo, ya sea por método POST o GET.

Short Description: Tampering is the act of altering the bits. Tampering with a process involves changing bits in the running process. Similarly, Tampering with a data flow involves changing bits on the wire or between two running processes.

3. Elevation Using Impersonation

[State: Not Started] [Priority: High]

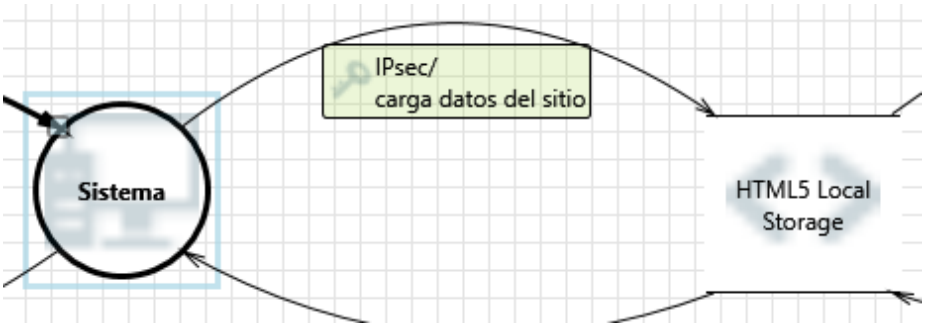
Category: Elevation Of Privilege

Description: Sistema may be able to impersonate the context of Browser in order to gain additional privilege.

Justification: Se verificará que el navegador utilizado esté actualizado.

Short Description: A user subject gains increased capability or privilege by taking advantage of an implementation bug.

Interaction: IPsec/ carga datos del sitio



4. Spoofing of Destination Data Store HTML5 Local Storage

[State: Not Started] [Priority: High]

Category: Spoofing

Description: HTML5 Local Storage may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of HTML5 Local Storage. Consider using a standard authentication mechanism to identify the destination data store.

Justification: Se realizará autenticación del usuario por medio de contraseña y un captcha, para evitar accesos automatizados.

Short Description: Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.

5. Potential Excessive Resource Consumption for Web Server or HTML5 Local Storage

[State: Not Started] [Priority: High]

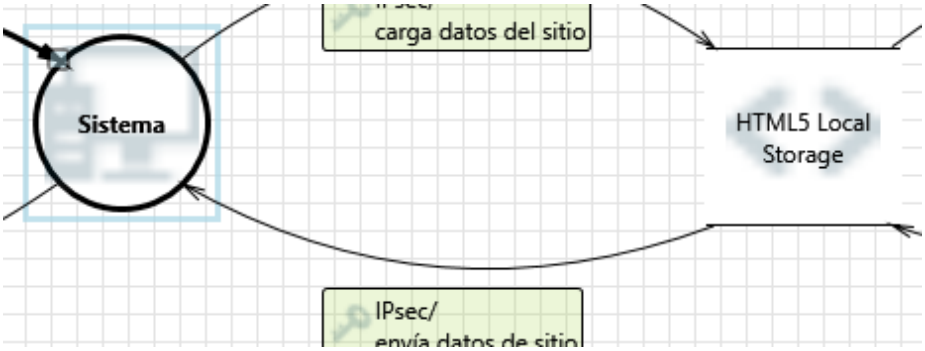
Category: Denial Of Service

Description: Does Sistema or HTML5 Local Storage take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.

Justification: En la programación se asegurará de requerir la menor cantidad de datos posibles, para evitar posibilidades de caída del sistema.

Short Description: Denial of Service happens when the process or a datastore is not able to service incoming requests or perform up to spec.

Interaction: IPsec/ envía datos de sitio



6. Weak Access Control for a Resource

[State: Not Started] [Priority: High]

Category: Information Disclosure

Description: Improper data protection of HTML5 Local Storage can allow an attacker to read information not intended for disclosure. Review authorization settings.

Justification: La información retornada solo podrá ser accesible tras la autenticación que permite su generación.

Short Description: Information disclosure happens when the information can be read by an unauthorized party.

7. Persistent Cross Site Scripting

[State: Not Started] [Priority: High]

Category: Tampering

Description: The web server 'Sistema' could be a subject to a persistent cross-site scripting attack because it does not sanitize data store 'HTML5 Local Storage' inputs and output.

Justification: Solo se mostrará el contenido de la página, evitando que el usuario pueda modificarla.

Short Description: Tampering is the act of altering the bits. Tampering with a process involves changing bits in the running process. Similarly, Tampering with a data flow involves changing bits on the wire or between two running processes.

8. Cross Site Scripting

[State: Not Started] [Priority: High]

Category: Tampering

Description: The web server 'Sistema' could be a subject to a cross-site scripting attack because it does not sanitize untrusted input.

Justification: En la programación se incluirá código que sanitice los datos que estén siendo procesados, a fin de que no afecten al sistema.

Short Description: Tampering is the act of altering the bits. Tampering with a process involves changing bits in the running process. Similarly, Tampering with a data flow involves changing bits on the wire or between two running processes.

9. Spoofing of Source Data Store HTML5 Local Storage

[State: Not Started] [Priority: High]

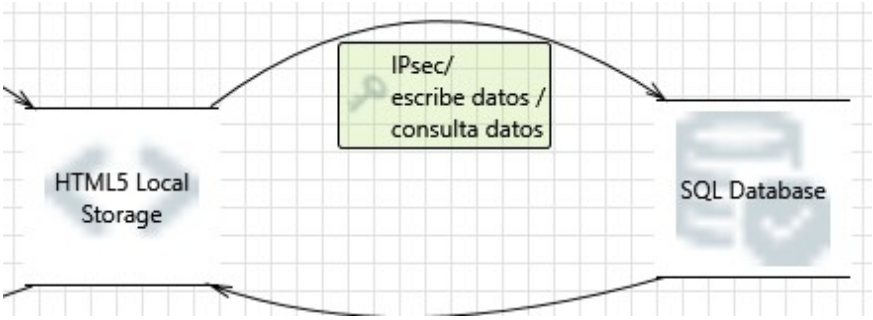
Category: Spoofing

Description: HTML5 Local Storage may be spoofed by an attacker and this may lead to incorrect data delivered to Sistema. Consider using a standard authentication mechanism to identify the source data store.

Justification: La programación del sitio mostrará solo la información solicitada y sin ofrecer campos por completar, para reducir la posibilidad de ataques.

Short Description: Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.

Interaction: IPsec/ escribe datos / consulta datos



10. Spoofing of Source Data Store HTML5 Local Storage

[State: Not Started] [Priority: High]

Category: Spoofing

Description: HTML5 Local Storage may be spoofed by an attacker and this may lead to incorrect data delivered to SQL Database. Consider using a standard authentication mechanism to identify the source data store.

Justification: En la programación se incluirá código que sanitice los datos que estén siendo procesados, a fin de que no se ingresen consultas SQL no deseadas.

Short Description: Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.

11. Spoofing of Destination Data Store SQL Database

[State: Not Started] [Priority: High]

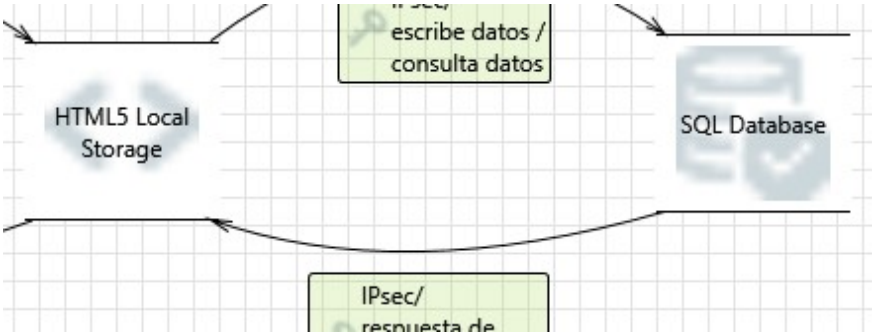
Category: Spoofing

Description: SQL Database may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of SQL Database. Consider using a standard authentication mechanism to identify the destination data store.

Justification: En la programación se limitará el campo de acción que tendrán los usuarios para generar consultas SQL, las que serán en todos los casos, tratadas mediante vistas para incrementar la seguridad de los datos.

Short Description: Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.

Interaction: IPsec/ respuesta de escritura / lectura de datos



12. Spoofing of Source Data Store SQL Database

[State: Not Started] [Priority: High]

Category: Spoofing

Description: SQL Database may be spoofed by an attacker and this may lead to incorrect data delivered to HTML5 Local Storage. Consider using a standard authentication mechanism to identify the source data store.

Justification: El resultado de las consultas SQL serán procesadas en la programación de tal modo que, si no corresponde su formato, no sean procesadas.

Short Description: Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.

13. Spoofing of Destination Data Store HTML5 Local Storage

[State: Not Started] [Priority: High]

Category: Spoofing

Description: HTML5 Local Storage may be spoofed by an attacker and this may lead to data being written to the attacker's target instead of HTML5 Local Storage. Consider using a standard authentication mechanism to identify the destination data store.

Justification: Las consultas SQL serán generadas para entregar siempre solo un resultado que esté vinculado a la identidad del usuario que las está solicitando.

Short Description: Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, website or a network address.

Conclusión

El desarrollo de este documento ha permitido analizar el proyecto de sistema para gestionar subsidios de SERVIU desde el punto de vista de las necesidades que éste debe satisfacer así como también las amenazas que enfrenta.

La realización de diagramas, así como las reflexiones respecto al sistema resultaron de especial utilidad para determinar los requerimientos que éste debe satisfacer; estos, a su vez, facilitaron la confección del diagrama de casos de uso que permitió acotar las necesidades a funciones concretas que el sistema debe contemplar.

Finalmente, la realización del diagrama de amenazas siguiendo la metodología STRIDE permitió visualizar qué puntos débiles podría tener el sistema, proveyendo información que será de gran utilidad al momento de programar el sistema.

Bibliografía

Stallings, William (2005). Sistemas operativos: aspectos internos y principios de diseño (5a edición). Pearson Prentice Hall.

Huang, Gary. Designing Security into Software Systems using Threat Modeling.. United States. Disponible en https://www.osti.gov/biblio/1639955 consultado el 21 de febrero de 2022.

Microsoft Trustworthy Computing. Microsoft Threat Modeling Tool 2016, User Guide. (2015). Disponible en https://download.microsoft.com/download/4/F/D/4FDDEA98-4ABD-47A7-AA0E-815CE8660A76/Threat%20Modeling%20Tool%202016%20User%20Guide.docx consultado el 22 de febrero de 2022.