

Proyecto para el Desarrollo de la Fase 1 de la Plataforma Digital Estatal

Interconexión con la Plataforma Digital Nacional

*Sistema de servidores públicos que intervengan
en procedimientos de contrataciones (S2)*

*Sistema de Servidores Públicos y particulares
sancionados (S3)*

Índice

1. Introducción	2
2. Justificación	2
3. Alcances	4
4. Objetivos	5
4.1 Objetivo general	5
4.2 Objetivos específicos	5
5. Líneas de acción del proyecto	6
5.1 Obtención de información del Ejecutivo Estatal.	7
5.1.1 Identificación de proveedores de información del Sistema 2 y Sistema 3.	8
5.1.2 Identificación y agrupación de proveedores según el nivel de adopción tecnológica.	10
5.1.3 Comparativa de formatos de datos existentes contra el estándar de datos emitido por la Plataforma Digital Nacional.	11
5.1.4 Planteamiento de soluciones para interconexión con proveedores.	12
5.1.5 Ejecución individualizada de soluciones por proveedor.	13
5.1.6 Integración y conexión con los proveedores.	15
5.2 Implementación de la Plataforma Digital Estatal en ambiente de desarrollo.	17
5.2.1 Definición del perímetro de seguridad.	18
5.2.2 Preparación de ambiente de desarrollo.	19
5.2.3 Desarrollo de la Plataforma Digital Estatal.	22
5.2.4 Ejecución del “Plan de Pruebas” en ambiente de desarrollo.	27
5.3 Instalación de la Plataforma Digital Estatal en ambiente de producción.	29
5.3.1 Adquisición en renta de Servidor Virtual Privado.	30
5.3.2 Migración de la Plataforma Digital Estatal al ambiente de producción.	31
5.3.3 Ejecución del “Plan de Pruebas” en ambiente de producción.	34
5.3.4 Resolución satisfactoria del plan de pruebas en ambiente de producción emitida por la Plataforma Digital Nacional.	35

5.3.5 Definición del plan de monitoreo de la Plataforma Digital Estatal.....37

Anexo I Cronograma de actividades ¡Error! Marcador no definido.

1. Introducción

El presente documento describe las actividades que realizará la Secretaría Ejecutiva del Sistema Estatal Anticorrupción (SESEA) para el desarrollo de la Plataforma Digital Estatal (PDE), la migración de la PDE hacia un ambiente de producción, así como la obtención de información del Ejecutivo Estatal sobre el Sistema de los servidores públicos que intervengan en procedimientos de contrataciones (Sistema 2) y del Sistema de servidores públicos y particulares sancionados (Sistema 3), a fin de interconectar a la Plataforma Digital Estatal con la Plataforma Digital Nacional.

Con la finalidad de dar claridad de las actividades se establece una serie de apartados en la descripción contenida en el presente documento.

2. Justificación

La Plataforma Digital Nacional (PDN) está conceptualizada como una fuente de inteligencia para construir integridad y combatir la corrupción que creará valor para el gobierno y la sociedad a partir de grandes cantidades de datos.

El desarrollo de la PDN considera seis sistemas que contienen datos estratégicos para la lucha contra la corrupción, contemplados en la Ley General del Sistema Nacional Anticorrupción:

1. Declaraciones patrimoniales, de intereses y constancia de declaración fiscal.
2. Servidores públicos que intervienen en procedimientos de contratación.

3. Servidores públicos y particulares sancionados.
4. Información y comunicación del Sistema Nacional Anticorrupción y el Sistema Nacional de Fiscalización
5. Denuncias por faltas administrativas y hechos de corrupción.
6. Contrataciones Públicas

Es importante señalar que la PDN no será generadora de los datos de cada sistema, sino que es una plataforma de interoperabilidad.

Por su parte, los Sistemas Locales Anticorrupción serán los encargados de resguardar la información para su integración a los sistemas de la PDN, según se establecen las Bases para el Funcionamiento de la Plataforma Digital Nacional

Dentro del marco normativo que seguirá la Plataforma Digital Estatal se contemplan las siguientes Leyes:

- Ley General del Sistema Nacional Anticorrupción:
 - Artículo 48 *“El comité Coordinador emitirá las bases para el funcionamiento de la Plataforma Digital Nacional y será administrada por la Secretaría Ejecutiva, a través del Secretario Técnico.”*
 - Artículo 49 *“Estará conformada por la información que a ella incorporen las autoridades integrantes del Sistema Nacional y contará, al menos, con 6 sistemas electrónicos.”*
- Ley General de Responsabilidades Administrativas:
 - Artículo 27 *“El Sistema 1 contendrá información que generen los entes públicos facultados para la fiscalización y control de recursos públicos. Se inscribirán los datos públicos de los servidores públicos obligados a presentar declaraciones de situación patrimonial y de intereses, así como la constancia que emita la autoridad fiscal sobre la presentación de declaración anual de impuestos. En el sistema 3, se inscribirán y se harán públicas las constancias de sanciones o de inhabilitación que se encuentren firmes en contra de los servidores públicos*

o particulares que hayan sido sancionados por actos vinculados con faltas grandes. Los entes públicos deberán consultar este sistema, previo al nombramiento, designación o contratación de quienes pretendan ingresar al servicio público."

- *Artículo 43 "En el sistema 2 se incluirán los nombres y adscripción de los Servidores Públicos que intervengan en procedimientos para contrataciones públicas para la adjudicación de un contrato, otorgamiento de una concesión, licencia, permiso o autorización y sus prórrogas, así como la enajenación de bienes muebles y aquellos que dictaminan en materia de avalúos. La información deberá ser puesta a disposición de todo público y deberá ser actualizada quincenalmente.*
- *Ley del Sistema Anticorrupción del Estado de Chihuahua:*
 - *Artículo 48 "El Sistema Estatal de Información, así como las autoridades integrantes de Sistema, serán el receptor e integrador de la información que se incorpore para su transmisión e integración a la Plataforma.*

De igual manera, es importante mencionar que los Sistemas Locales Anticorrupción promoverán la información contenida en la Plataforma en formato de datos abiertos, conforme la Ley General de Transparencia y Acceso a la Información Pública.

3. Alcances

- a) Desarrollo de los Sistemas 2 y 3 de la Plataforma Digital Estatal interconectada con el Poder Ejecutivo Estatal.
- b) Creación de un almacén de datos de la información del Sistema 2 y 3.
- c) Desarrollo de un portal público para la consulta de datos que tienen carácter público, de acuerdo con la Ley General de Transparencia y Acceso a la Información.
- d) Desarrollo de interfaz a la Plataforma Digital Estatal para los distintos usuarios autorizados.

4. Objetivos

4.1 Objetivo general

El objetivo general es la creación de la Plataforma Digital Estatal; la adquisición de información del Ejecutivo Estatal de los Sistemas 2 y 3, así como la respectiva interconexión con la Plataforma Digital Nacional.

4.2 Objetivos específicos

- Adquisición de información del Ejecutivo Estatal para el Sistema 2 y Sistema 3.
 - Diseño de instrumento de diagnóstico.
 - Identificación de proveedores de información.
 - Agrupación de proveedores según el nivel de adopción tecnológica.
 - Comparativa de formatos de datos existentes contra el estándar de datos.
 - Planteamiento de soluciones para interconexión con proveedores.
 - Ejecución individualizada de soluciones por proveedor.
 - Integración y conexión con los proveedores.

- Desarrollo de la Plataforma Digital Estatal.
 - Definición de perímetro de seguridad.
 - Preparación de ambiente de desarrollo.
 - Desarrollo de Plataforma Digital.
 - Elaboración de Portal Web.
 - Desarrollo de API's para la interconexión del Sistema 2 con la Plataforma Digital Nacional.
 - Desarrollo de API's para la interconexión del Sistema 3 con la Plataforma Digital Nacional.
 - Creación de estructura de bases de datos.
 - Carga de datos sintéticos.
 - Ejecución del "Plan de Pruebas" en ambiente de desarrollo.

- Migración de la Plataforma Digital Estatal a un ambiente de producción.
 - Adquisición y configuración del Servidor Virtual Privado.
 - Migración de PDE a un ambiente de producción.
 - Ejecución del “Plan de Pruebas” en ambiente de producción.
 - Resolución satisfactoria del plan de pruebas en ambiente de producción emitido por la Plataforma Digital Nacional.
 - Definición de plan de monitoreo de la PDE.

5. Líneas de acción del proyecto

La Plataforma Digital Estatal (PDE) estará alojada en un Servidor Virtual Privado (VPS, por sus siglas en inglés), garantizando de esta manera la conexión continua con la Plataforma Digital Nacional, los usuarios podrán consultar información en la PDE o de igual manera en la Plataforma Digital Nacional (PDN), se recibirán las peticiones de búsqueda mediante API's, lo cual ordenará los datos en un mismo estándar; es decir, los datos estarán organizados en un mismo lenguaje y podrán ser comparados entre sí. La PDE se conectará a la base de datos correspondiente, obteniendo el resultado de la búsqueda, para finalmente resolver la petición.

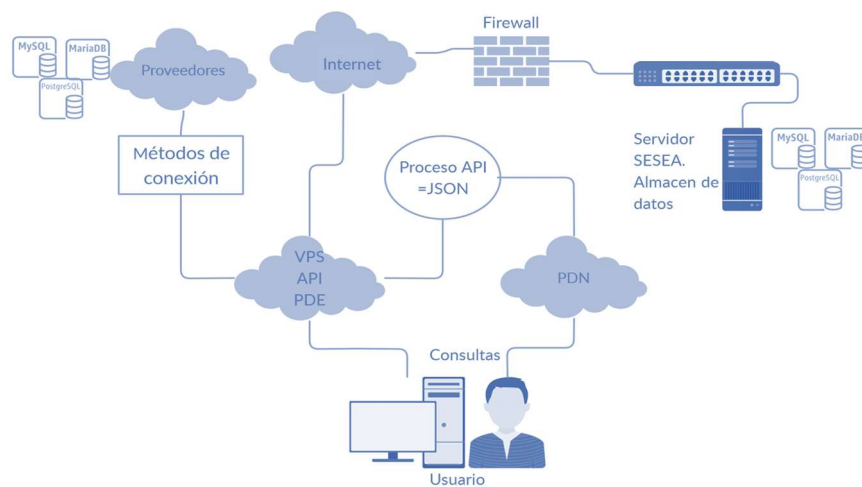


Ilustración 1, Flujo de información.

A continuación, se presenta la definición de una serie de actividades, divididas en tres macroprocesos, que se realizarán para lograr el acceso a la información del Ejecutivo Estatal para el Sistema 2 y Sistema 3, el desarrollo de la Plataforma Digital Estatal y migración a un ambiente de producción que estará interconectada con la Plataforma Digital Nacional.

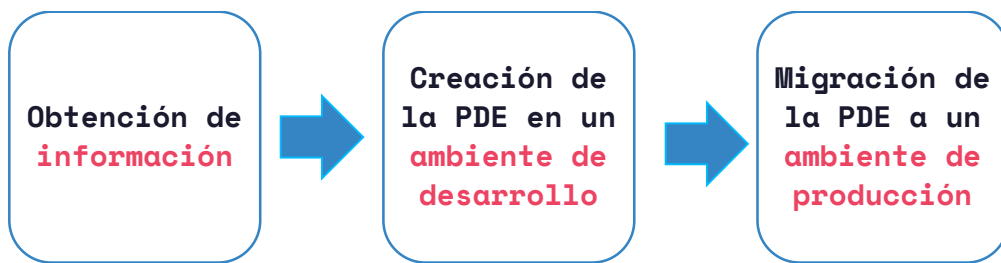


Ilustración 2, Diagrama de actividades principales.

5.1 Obtención de información del Ejecutivo Estatal.

A continuación, se presentan las principales actividades para lograr la obtención de información del Ejecutivo Estatal de los Sistemas 2 y 3.



Ilustración 3, Actividades principales para la obtención de información del Ejecutivo Estatal.

5.1.1 Identificación de proveedores de información del Sistema 2 y Sistema 3.

El instrumento de diagnóstico está diseñado para conocer los entes que generan información, el método de almacenamiento, el nivel de adopción tecnológico, así como la identificación de los responsables del resguardo de la información.

Dicho instrumento se enviará a los titulares de los entes para que realicen un nombramiento de enlaces con quienes la Secretaría Ejecutiva del Sistema Estatal Anticorrupción establecerá comunicación, a través de reuniones virtuales, para resolver dudas y comentarios; así como proporcionar información sobre el objetivo del instrumento. Una vez recopilados los resultados del instrumento se estará analizando la información, con la cual, se generará un directorio de entes proveedores de información.

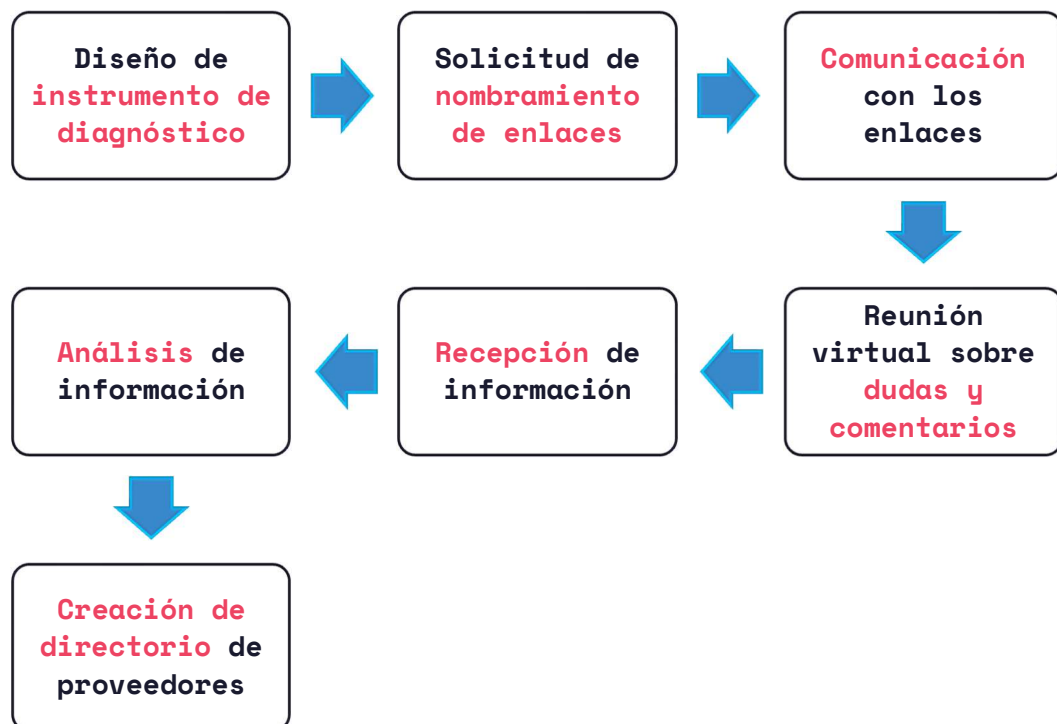


Ilustración 4, Actividades para la identificación de proveedores de los Sistemas 2 y 3

Posibles Riesgos

A continuación, se muestra una lista de los posibles riesgos identificados para la ejecución de esta actividad.

MATRIZ DE RIESGOS			
1	Riesgo	Probabilidad	Impacto
	<i>Problema con recepción de solicitud por parte de los proveedores</i>	<i>Media</i>	<i>Alto</i>
	<i>Acción de prevención</i>	<i>Tener acercamiento previo por teléfono</i>	
	<i>Acción de contención</i>	<i>Envío de solicitud por vías electrónicas</i>	
	<i>Acción de corrección</i>	<i>Envío de solicitud de manera física</i>	
2	Riesgo	Probabilidad	Impacto
	<i>Problemas para establecer comunicación con los enlaces</i>	<i>Media</i>	<i>Alto</i>
	<i>Acción de prevención</i>	<i>Realizar acercamientos previos explicando el objetivo del proyecto</i>	
	<i>Acción de contención</i>	<i>Continuar con el siguiente enlace en lista</i>	
	<i>Acción de corrección</i>	<i>Utilizar distintas vías electrónicas</i>	
3	Riesgo	Probabilidad	Impacto
	<i>Problemas para realizar reunión virtual con los entes proveedores</i>	<i>Media</i>	<i>Alto</i>
	<i>Acción de prevención</i>	<i>Realizar acercamientos previos para agenda de reunión</i>	
	<i>Acción de contención</i>	<i>Envío de videograbación explicando el funcionamiento y objetivo del instrumento</i>	
	<i>Acción de corrección</i>	<i>Comunicación con enlace técnico para la atención</i>	

Tabla 1, Riesgos para la identificación de proveedores de los Sistemas 2 y 3

5.1.2 Identificación y agrupación de proveedores según el nivel de adopción tecnológica.

Una vez recopilada la información, la Secretaría Ejecutiva, agrupará la información por tipo de nivel de adopción tecnológica (alto¹, medio²,bajo³) y por tipo de Sistema.

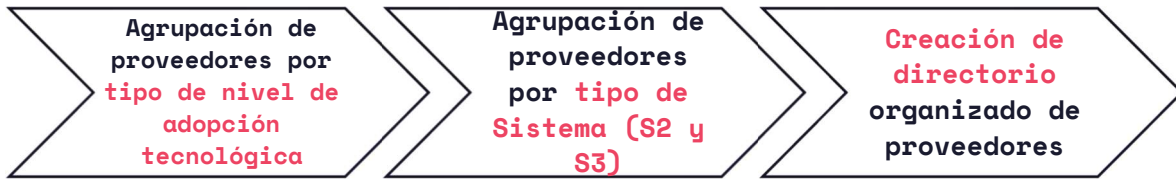


Ilustración 5, Actividades para la identificación y agrupación de proveedores según el nivel de adopción tecnológica

Posibles Riesgos

A continuación, se muestra una lista de los posibles riesgos identificados para la ejecución de esta actividad.

MATRIZ DE RIESGOS			
1	Riesgo	Probabilidad	Impacto
	Información incompleta de directorio	Media	Alto
	Acción de prevención	Informar la importancia del proyecto	
	Acción de contención	NA	
	Acción de corrección	Tener comunicación con enlaces para solicitar	

Tabla 2, Riesgos identificados para la agrupación de proveedores por nivel de adopción tecnológica de los Sistemas 2 y 3

¹ Proveedores que cuentan con Información almacenada en bases de datos y servicio de Internet.

² Proveedores que cuentan con Información almacenada en hojas de cálculo y servicio de Internet.

³ Proveedores que cuentan con registros en papel y no tienen servicio de Internet

5.1.3 Comparativa de formatos de datos existentes contra el estándar de datos emitido por la Plataforma Digital Nacional.

Al establecer comunicación con los responsables del resguardo de la información, se procederá a comunicarles sobre la existencia del estándar de datos requerido para la interconexión con la Plataforma Digital Nacional, por lo que se les solicitará la estructura actual, con la finalidad de hacer una comparación con el estándar de datos para posteriormente, dar a conocer las diferencias a los entes.

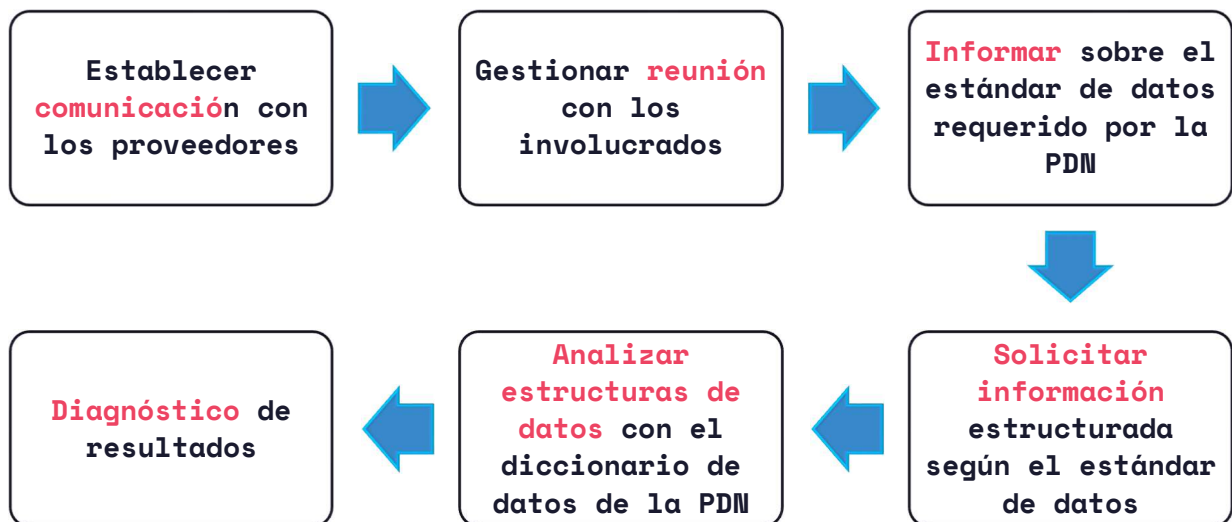


Ilustración 6, Actividades para realizar la comparativa de formatos de datos existentes contra el estándar de datos emitido por la PDM

Posibles Riesgos

A continuación, se muestra una lista de los posibles riesgos identificados para la ejecución de esta actividad.

MATRIZ DE RIESGOS			
1	Riesgo	Probabilidad	Impacto
	<i>Proveedores de información no facilitan información</i>	<i>Media</i>	<i>Alto</i>
	<i>Acción de prevención</i>	<i>Dar a conocer el proyecto y la normativa aplicable a los proveedores de información</i>	
	<i>Acción de contención</i>		
	<i>Acción de corrección</i>	<i>Apercibimiento por parte de la autoridad competente</i>	
2	Riesgo	Probabilidad	Impacto
	<i>Información incompleta</i>	<i>Media</i>	<i>Alto</i>
	<i>Acción de prevención</i>	<i>Realizar acercamientos previos explicando el objetivo del proyecto</i>	
	<i>Acción de contención</i>		
	<i>Acción de corrección</i>	<i>Proporcionar el estándar de datos emitido por la PDN</i>	

Tabla 3, Riesgos identificados para realizar la comparativa de formatos de datos existentes contra el estándar de datos emitido por la PDN

5.1.4 Planteamiento de soluciones para interconexión con proveedores.

Se desarrollará un plan de solución por cada nivel de adopción tecnológico con la finalidad de lograr la interconexión de información con los diversos proveedores dependiendo de las capacidades tecnológicas de los mismos.



Ilustración 7, Diseño de plan de solución para obtención de información dependiendo del nivel de adopción tecnológico.

Posibles Riesgos

A continuación, se muestra una lista de los posibles riesgos identificados para la ejecución de esta actividad.

MATRIZ DE RIESGOS			
1	Riesgo	Probabilidad	Impacto
	Falta de comunicación con entes	Medio	Alto
	Acción de prevención	Dar a conocer el proyecto y la normativa aplicable a los proveedores de información	
	Acción de contención	Informar a los entes la importancia del proyecto	
	Acción de corrección	Apercibimiento por parte de la autoridad competente	

Tabla 4, Riesgos identificados para el planteamiento de soluciones para interconexión con proveedores

5.1.5 Ejecución individualizada de soluciones por proveedor.

Se realizará la ejecución individualizada de soluciones por proveedor respetando las actividades y las fechas compromisos acordadas.



Ilustración 8, Ejecución de soluciones por proveedor

- Nivel de adopción tecnológico alto.
 - Se plantea el acceso a la información a través de vistas o accediendo a copias de las tablas necesarias, con usuarios de lectura, realizando pruebas de acceso.
 - Se solicita información estructurada según el estándar de datos de la PDN.
 - Se analiza la estructura de datos contra el estándar emitido por la PDN.
- Nivel de adopción tecnológico medio y bajo.

Los sistemas de captura⁴ desarrollados por la Secretaría Ejecutiva almacenarán la información cumpliendo con el estándar de datos requerido por la Unidad de Servicios Tecnológicos y Plataforma Digital de la Secretaría Ejecutiva del Sistema Nacional Anticorrupción.

Posibles Riesgos

A continuación, se muestra una lista de los posibles riesgos identificados para la ejecución de esta actividad.

MATRIZ DE RIESGOS			
1	Riesgo	Probabilidad	Impacto

⁴ Tendrán la capacidad de capturar y actualizar la información ya cargada.

Problema de acceso a la información del proveedor	Media	Alto	
Acción de prevención	Obtención de credenciales previamente		
Acción de contención	Definir plan de contención en coordinación con el proveedor		
Acción de corrección	Solicitar credenciales de acceso validadas por parte del proveedor		
2	Riesgo	Probabilidad	Impacto
Problemas para el desarrollo de la aplicación de captura	Baja	Alto	
Acción de prevención	Realizar plan de desarrollo de software		
Acción de contención	Carga de información en lotes		
Acción de corrección	Consultar documentación de desarrollo		
3	Riesgo	Probabilidad	Impacto
Problemas con servidor de almacenamiento	Media	Alto	
Acción de prevención	Realizar copias de seguridad del estado de los servidores virtuales		
Acción de contención	Utilizar servidor de respaldo		
Acción de corrección	Reemplazo de dispositivo que presente falla		

Tabla 5, Riesgos identificados para la ejecución de soluciones por proveedor

5.1.6 Integración y conexión con los proveedores.

En cuanto a los entes de nivel de adopción tecnológico alto se refiere, una vez teniendo acceso a la información se volverá a comparar la estructura y se validará o se harán observaciones, debido a que la comunicación será constante, la actualización de información se reflejará al instante.

Por lo que respecta a los entes de nivel de adopción tecnológico medio y bajo se definirá la periodicidad y método de actualización de la información.

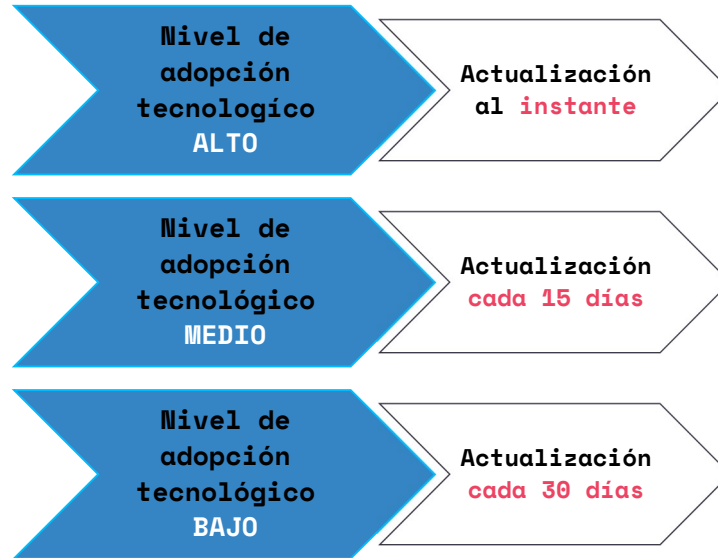


Ilustración 9, Integración y conexión con los proveedores

Posibles Riesgos

A continuación, se muestra una lista de los posibles riesgos identificados para la ejecución de esta actividad.

MATRIZ DE RIESGOS			
1	Riesgo	Probabilidad	Impacto
	Problema de acceso a la información del proveedor	Media	Alto
	Acción de prevención	Obtención de credenciales previamente	
	Acción de contención	Definir plan de contención en coordinación con el proveedor	
	Acción de corrección	Envío de solicitud de manera física	
2	Riesgo	Probabilidad	Impacto

Falta de compromiso para actualización de información		Media	Alto
Acción de prevención		Dar a conocer el proyecto y la normativa aplicable a los proveedores de información	
Acción de contención		Proseguir con los datos existentes y marcarlos en “actualización”.	
Acción de corrección		Apercibimiento por parte de la autoridad competente	
3	Riesgo	Probabilidad	Impacto
Falta de conocimiento para el uso de aplicación de captura		Baja	Alto
Acción de prevención		Realizar y enviar manual de usuario a los proveedores	
Acción de contención		Realizar carga de datos por lotes	
Acción de corrección		Realizar y enviar manual de usuario a los proveedores	

Tabla 6, Riesgos identificados para la integración y conexión con los proveedores

5.2 Implementación de la Plataforma Digital Estatal en ambiente de desarrollo.

A continuación, se presentan las actividades a realizar para la implementación de la Plataforma Digital Estatal en un ambiente de desarrollo.



Ilustración 10, Implementación de la Plataforma Digital Estatal en ambiente de desarrollo

5.2.1 Definición del perímetro de seguridad.

Para garantizar la seguridad de los datos que maneje la Plataforma Digital Estatal se tomarán en cuenta los estándares internacionales, utilizando como guía la norma ISO⁵/IEC⁶ 22237 para la definición de la infraestructura dependiendo de las siguientes necesidades:

- Propósito de la empresa y la instalación del proveedor de Internet, es decir, que el proveedor proporcione un servicio de acuerdo con las necesidades.
- Analizar el nivel de seguridad según la sensibilidad de la información que se va a resguardar.

⁵ Organización Internacional de Normalización por sus siglas en inglés.

⁶ Comisión Electrotécnica Internacional por sus siglas en inglés.

- Definición del espacio físico facilitando la instalación de los diversos dispositivos de almacenamiento y comunicación.
- Definición de alojamiento temporal o permanente.

Los Sistemas de Gestión de Seguridad de la Información (SGSI) son el medio más eficaz de minimizar riesgos, al asegurar que se identifican y valoran los procesos de negocio y/o servicios de Tecnologías de la Información, activos y sus riesgos, considerando el impacto para la organización, y se adoptan los controles y procedimientos más eficaces y coherentes con la estrategia de negocio, por lo cual se utilizará la norma ISO/IEC 27001 para garantizar:

- **Confidencialidad**, asegurando que sólo quienes estén autorizados puedan acceder a la información.
- **Integridad**, asegurando que la información y sus métodos de proceso son exactos y completos.
- **Disponibilidad**, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

5.2.2 Preparación de ambiente de desarrollo.

La Secretaría Ejecutiva del Sistema Estatal Anticorrupción cuenta con un servidor físico, en él se encuentran virtualizados 2 servidores, uno de aplicaciones y otro de base de datos, los cuales están siendo utilizados para el desarrollo del portal web, desarrollo de las API's para los Sistemas 2 y 3, así como la creación de bases de datos y las respectivas cargas de información sintética. A continuación, se muestran las principales características.

Ambiente de desarrollo	Servidor físico (host)	Servidor de aplicaciones (virtualizado)	Servidor de base de datos (virtualizado)
Procesador	Intel Xeon 16 núcleos	Intel Xeon 2 núcleos	Intel Xeon 6 núcleos
Memoria RAM	32 GB	2 GB	10 GB

Almacenamiento	<i>1 TB (RAID 1)</i>	<i>120 GB</i>	<i>200 GB</i>
Sistema Operativo	<i>Proxmox</i>	<i>Debian 10.1</i>	<i>Debian 10.1</i>

Tabla 7, Descripción del servidor en ambiente de desarrollo.

Para la elaboración de la Plataforma Digital Estatal únicamente se utilizarán herramientas de código abierto, esto quiere decir que no generará costo extra de licenciamiento de software; en el servidor físico se encuentra instalado el sistema operativo Proxmox 11.0 utilizado para la creación de los servidores virtuales descritos previamente.

A continuación, se muestra las herramientas que serán utilizadas para el desarrollo de la Plataforma Digital Estatal.

Herramientas	Plataforma Digital Estatal		
	Servidor de aplicaciones		Servidor de bases de datos
	Front-End	Back-End	Bases de datos
Lenguajes	<i>JavaScript, CSS3, HTML5</i>	<i>PHP</i>	<i>SQL</i>
Framework	<i>Bootstrap, JQuery</i>	<i>Laravel</i>	
Biblioteca	<i>DataTables</i>	<i>Composer</i>	<i>Eloquent</i>
Servidor	<i>Apache</i>		<i>MariaDB, PostgreSQL</i>
Editor de texto	<i>Visual Studio Code</i>		
IDE's⁷			<i>Workbench, HeidiSQL, PgAdmin</i>

Tabla 8, Herramientas para el desarrollo de la Plataforma Digital Estatal

En el servidor virtual de base de datos se tiene instalado el sistema operativo Debian 10.1 donde se encuentran instalados PostgreSQL 12.0 y MariaDB 10.3.22, como motor de base de datos, los programas HeidiSQL, Workbench y PgAdmin como IDE's.

⁷ Entorno de Desarrollo Integrado por sus siglas en inglés.

En el servidor de aplicaciones se encuentra instalado el sistema operativo Debian 10.1 con un servidor Apache 2.4.38 será el encargado de interpretar las peticiones web, el lenguaje de programación para el desarrollo del Portal será PHP con el Framework Laravel 5.*, para el desarrollo del Back-End; para el desarrollo de Front-End se utilizará Bootstrap, JQuery, CSS3, JavaScript.

El acceso a las API's de la PDE se gestionará a través del protocolo de autorización OAuth 2.0, el cual es un estándar ampliamente usado por la industria de Internet. El estándar OAuth 2.0 permitirá a la PDN obtener acceso necesario a las API's de la PDE a través del uso de tokens de autorización.

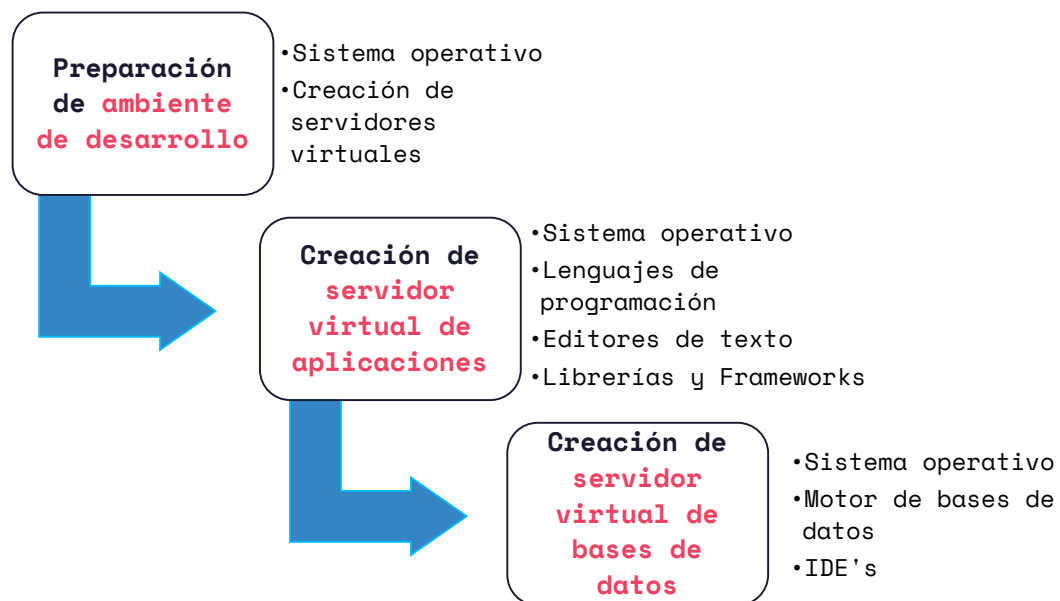


Ilustración 11, Actividades para la preparación del ambiente de desarrollo

Posibles Riesgos

A continuación, se muestra una lista de los posibles riesgos identificados para la ejecución de esta actividad.

MATRIZ DE RIESGOS			
1	Riesgo	Probabilidad	Impacto
	Falla física del servidor	Baja	Medio
	Acción de prevención	Utilizar dispositivos de protección de energía	
	Acción de contención	Utilizar otro dispositivo como servidor de respaldo	
	Acción de corrección	Cambio de equipo físico	
2	Riesgo	Probabilidad	Impacto
	Falla de algún sistema operativo	Baja	Medio
	Acción de prevención	Realizar copias de seguridad	
	Acción de contención	Utilizar otro dispositivo como servidor de respaldo	
	Acción de corrección	Reinstalación de sistema operativo mediante copias de seguridad	

Tabla 9, Riesgos identificados para la preparación del ambiente de desarrollo

5.2.3 Desarrollo de la Plataforma Digital Estatal.

La Plataforma Digital Estatal será desarrollada con la metodología “SCRUM”⁸ utilizada para trabajar colaborativamente en equipo, especialmente en entornos complejos donde se necesita obtener resultados pronto, donde los requisitos son cambiantes o poco definidos; en “SCRUM” un proyecto se ejecuta en ciclos temporales cortos y de duración fija (2, 3 ó 4 semanas) y cada iteración tiene que proporcionar un resultado completo, un incremento de producto final que sea susceptible de ser entregado al cliente cuando lo solicite.

⁸ SCRUM el arte de hacer el doble de trabajo en la mitad de tiempo (Jeff Sutherland, 2014)



Ilustración 12, Proceso “SCRUM”

En combinación con el modelo “Cascada Enriquecida”⁹, es un proceso de desarrollo secuencial, en que el desarrollo de software se concibe como un conjunto de etapas que se ejecutan una tras otra siguiendo un flujo de arriba hacia abajo como una cascada, considerando:

- **Análisis**, se determinan las características del software a desarrollar sin entrar en detalles técnicos.
- **Diseño**, se describe la estructura interna del software y las relaciones entre las entidades que lo componen.
- **Implementación**, se programan los requisitos especificados haciendo uso de las estructuras de datos diseñadas en la fase anterior.

⁹<http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/175/A5%20Cap%C3%ADtulo%202.pdf>

- **Verificación**, una vez que termina la fase de implementación se verifica que todos los componentes del sistema funcionen correctamente y cumplan con los requisitos.
- **Mantenimiento**, se instala la aplicación en el sistema y se comprueba que funcione correctamente en el entorno que se va a utilizar. Consiste en la modificación del producto ya sea para corregir errores o para mejorar el rendimiento o las características.

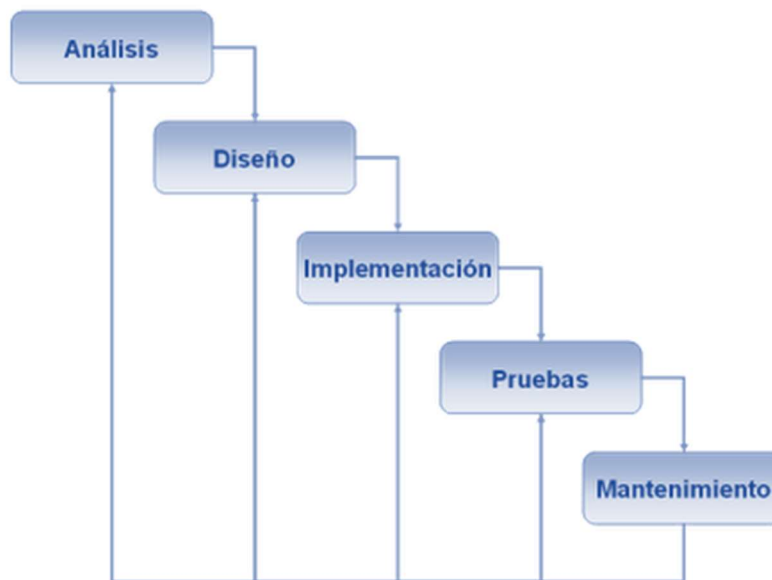


Ilustración 13, Proceso Cascada enriquecida

La PDE se desarrollará implementando la arquitectura MVC (Model View Controller, por sus siglas en inglés), asegurando que cada uno de los componentes se encuentren separados permitiendo así una mayor facilidad en la incorporación de módulos.

- **Modelo**. Contiene la representación de los datos que maneja el sistema.
- **Vista**. Interfaz de usuario que compone la información que será enviada al cliente y los mecanismos de interacción.
- **Controlador**. Actúa como intermediario entre el modelo y la vista gestionando el flujo de la información entre

ambos, así como, las transformaciones para adaptar los datos a las necesidades de cada uno.

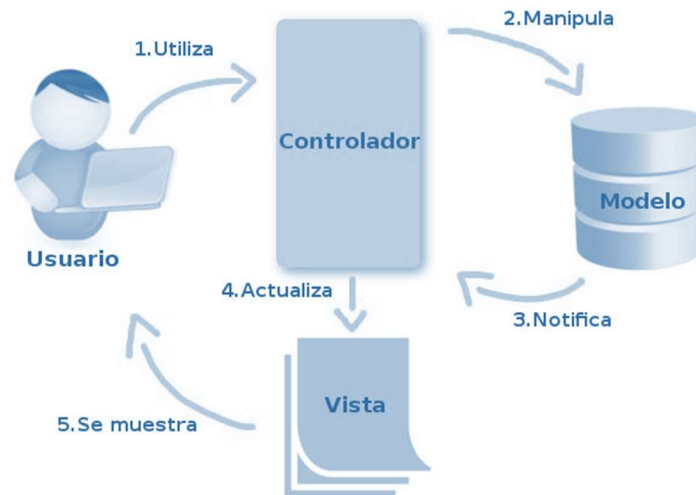


Ilustración 14, Arquitectura “Modelo Vista Controlador”

El desarrollo del Front-End será realizado haciendo uso de herramientas y tecnologías actuales como CSS, HTML5 y Bootstrap.

El desarrollo del Back-End estará realizado en el lenguaje PHP con Framework Laravel, se utilizará el ORM Eloquent para la integración de las bases de datos, es decir, nos permite llevar la capa de persistencia en bases de datos por medio de objetos ahorrando trabajo, en comparación con la comunicación directa hacia la misma.

Las bases de datos serán estructuras de datos normalizados que serán accedidas mediante los controladores de la Plataforma Digital Estatal.

Se definirán los accesos a la PDE, la navegación del portal y las páginas de interés a mostrar.



Ilustración 15, Desarrollo de la Plataforma Digital Estatal

Posibles Riesgos

A continuación, se muestra una lista de los posibles riesgos identificados para la ejecución de esta actividad. (Tabla 10).

MATRIZ DE RIESGOS			
1	Riesgo	Probabilidad	Impacto
	Falla física del servidor	Baja	Medio
	Acción de prevención	Utilizar dispositivos de protección de energía	
	Acción de contención	Utilizar otro dispositivo como servidor de respaldo	
	Acción de corrección	Cambio de equipo físico	
2	Riesgo	Probabilidad	Impacto
	Falla de algún sistema operativo	Baja	Medio
	Acción de prevención	Realizar copias de seguridad	

Acción de contención		Utilizar otro dispositivo como servidor de respaldo	
Acción de corrección		Reinstalación de sistema operativo mediante copias de seguridad	
3	Riesgo	Probabilidad	Impacto
Falla de alguna versión de desarrollo de la PDE		Baja	Medio
Acción de prevención		Utilizar programas de control de versiones	
Acción de contención		Utilizar otro dispositivo como servidor de respaldo	
Acción de corrección		Regresar a versión anterior del desarrollo	
4	Riesgo	Probabilidad	Impacto
Falta de capacidad técnica		Baja	Medio
Acción de prevención		Realizar plan de desarrollo según especificaciones técnicas	
Acción de contención		Apoyarse con asesoría y servicios técnicos	
Acción de corrección		Disponer de documentación técnica para solucionar posibles fallas	

Tabla 10, Riesgos identificados para el desarrollo de la PDE

5.2.4 Ejecución del “Plan de Pruebas” en ambiente de desarrollo.

Será solicitado el “Plan de Pruebas” en ambiente de desarrollo a la Unidad de Servicios Tecnológicos y Plataforma Digital de la Secretaría Ejecutiva del Sistema Nacional Anticorrupción (SESNA) recibiendo, en dado caso, observaciones correspondientes para realizar las adecuaciones necesarias. Una vez realizados los cambios, se procede a ejecutar nuevamente el “Plan de Pruebas” con el fin de obtener la validación respectiva.

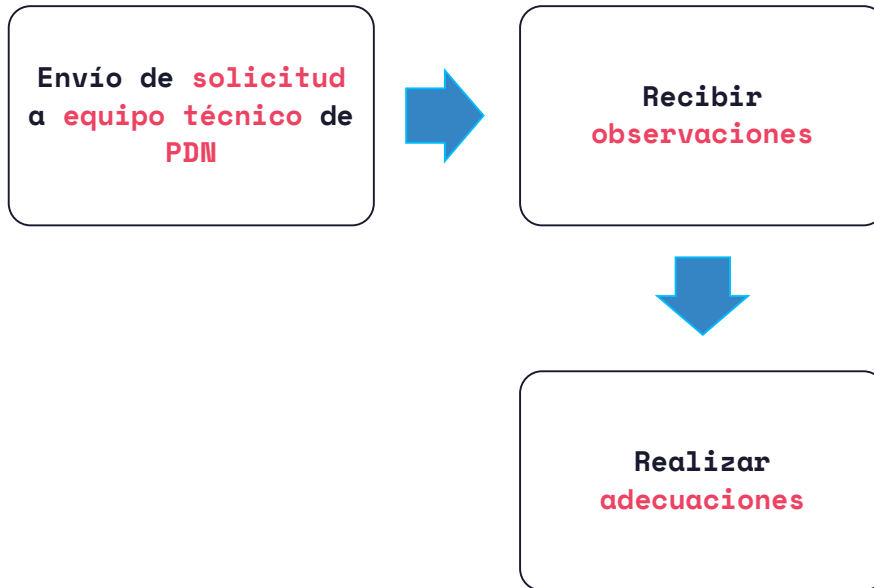


Ilustración 16, Actividades para la ejecución del “Plan de Pruebas” en ambiente de desarrollo Desarrollo

Posibles Riesgos

A continuación, se muestra una lista de los posibles riesgos identificados para la ejecución de esta actividad.

MATRIZ DE RIESGOS			
1	Riesgo	Probabilidad	Impacto
	Falla física del servidor	Baja	Medio
	Acción de prevención	Utilizar dispositivos de protección de energía	
	Acción de contención	Utilizar otro dispositivo como servidor de respaldo	
	Acción de corrección	Cambio de equipo físico	
2	Riesgo	Probabilidad	Impacto
	Falla de algún sistema operativo	Baja	Medio
	Acción de prevención	Realizar copias de seguridad	

Acción de contención		Utilizar otro dispositivo como servidor de respaldo	
Acción de corrección		Reinstalación de sistema operativo mediante copias de seguridad	
3	Riesgo	Probabilidad	Impacto
Falla de dispositivos de comunicación de la Secretaría		Baja	Alto
Acción de prevención		Utilizar equipos de protección de dispositivos	
Acción de contención		Utilizar servidor de respaldo en otra red	
Acción de corrección		Reparación o reposición de dispositivo	

Tabla 11, Riesgos identificados para el planteamiento de soluciones para interconexión con proveedores

5.3 Instalación de la Plataforma Digital Estatal en ambiente de producción.

A continuación, se presentan las actividades a realizar para la creación de la Plataforma Digital Estatal en un ambiente de desarrollo.

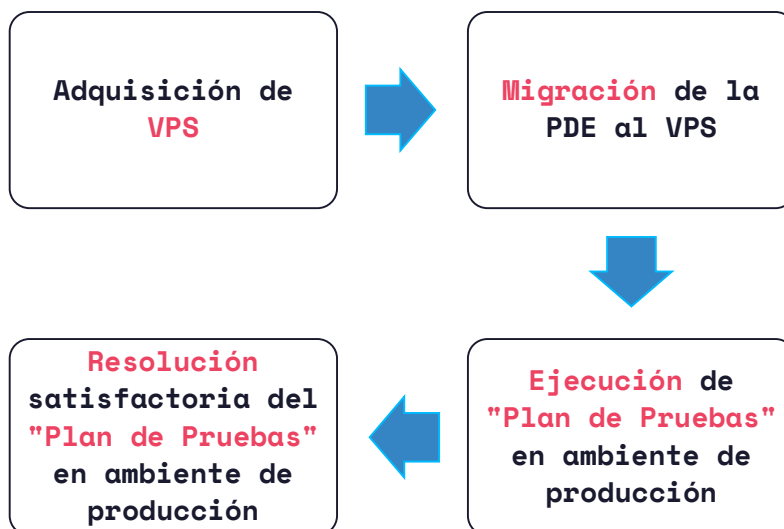


Ilustración 17, Instalación de la PDE en ambiente de producción

5.3.1 Adquisición en renta de Servidor Virtual Privado.

El Servidor Virtual Privado estará rentado con algún proveedor de hospedaje, que sea permisible para la instalación de sistema operativo y aplicaciones que se requieran, así como el realizar las configuraciones necesarias.

Por la naturaleza de los sistemas que serán desarrollados en la Secretaría Ejecutiva del Sistema Estatal Anticorrupción habrá un crecimiento constante, por lo cual es necesario contar con un VPS para la escalabilidad, tanto en almacenamiento, procesamiento y usuarios concurrentes.

Es una solución más segura y estable que el hosting esté compartido debido a que no se obtiene espacio de servidor dedicado, generalmente elegido por los propietarios de sitios web que tienen un tráfico de nivel medio que excede los límites de los planes de hosting compartido pero que aún no necesitan los recursos de un servidor dedicado.

Definición de especificaciones técnicas.

Para la definición de las especificaciones técnicas del VPS que se va a rentar, se determinarán realizando una estimación de:

- Capacidad de almacenamiento.
- Capacidad de procesamiento.
- Memoria RAM.
- Concurrencia.

La estimación de capacidad de almacenamiento se podrá realizar creando bases de datos según las especificaciones técnicas de la PDN y cargando una cantidad de registros sintéticos similar a los existentes.

Realizando pruebas de estrés (varias consultas simultáneas) se podrá monitorear el comportamiento del procesador para su estimación junto a la de memoria RAM.

Una vez la PDE se encuentre en producción realizando un monitoreo de tráfico de visitas se podrá estimar el consumo de los recursos.

Posibles Riesgos

A continuación, se muestra una lista de los posibles riesgos identificados para la ejecución de esta actividad.

MATRIZ DE RIESGOS			
1	Riesgo	Probabilidad	Impacto
	Problema en el trámite de renta	Baja	Alto
	Acción de prevención	Proporcionar documentación en tiempo y forma al área correspondiente	
	Acción de contención	Utilizar servidor de desarrollo	
	Acción de corrección	Persistir o intentar con otro proveedor	
2	Riesgo	Probabilidad	Impacto
	Falta de recurso	Baja	Alto
	Acción de prevención	Realizar la solicitud con tiempo para realizar la renta del VPS	
	Acción de contención	Utilizar servidor de desarrollo	
	Acción de corrección	Buscar proveedores más económicos	

Tabla 12, Riesgos identificados para la adquisición del VPS

5.3.2 Migración de la Plataforma Digital Estatal al ambiente de producción.

Teniendo acceso al servidor se procede a configurar el ambiente. Teniendo el ambiente preparado se realiza la migración de la Plataforma Digital Estatal con todos sus componentes y bases de

datos; y se realizan las configuraciones necesarias para obtener el acceso a la información de los proveedores.

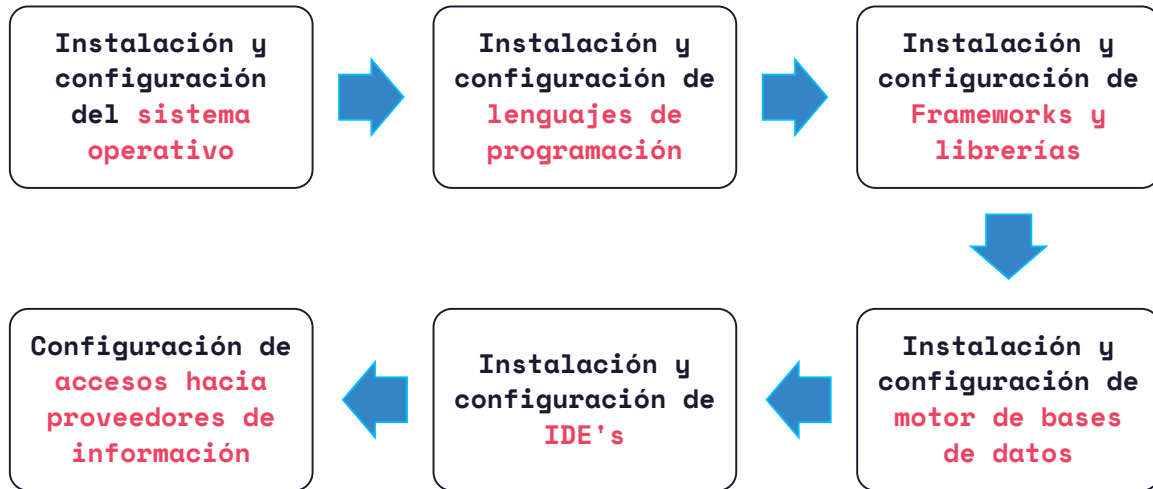


Ilustración 18, Migración de la PDE al ambiente de producción

Posibles Riesgos

A continuación, se muestra una lista de los posibles riesgos identificados para la ejecución de esta actividad.

MATRIZ DE RIESGOS			
1	Riesgo	Probabilidad	Impacto
	Falla física del servidor	Baja	Medio
	Acción de prevención	Utilizar dispositivos de protección de energía	
	Acción de contención	Utilizar otro dispositivo como servidor de respaldo	
	Acción de corrección	Cambio de equipo físico	
2	Riesgo	Probabilidad	Impacto

Falla de algún sistema operativo		Baja	Medio
Acción de prevención		Realizar copias de seguridad	
Acción de contención		Utilizar otro dispositivo como servidor de respaldo	
Acción de corrección		Reinstalación de sistema operativo mediante copias de seguridad	
3	Riesgo	Probabilidad	Impacto
Falla de dispositivos de comunicación de la Secretaría		Baja	Alto
Acción de prevención		Utilizar equipos de protección de dispositivos	
Acción de contención		Utilizar servidor de respaldo en otra red	
Acción de corrección		Reparación o reposición de dispositivo	
4	Riesgo	Probabilidad	Impacto
Falla de accesos en el VPS		Baja	Alto
Acción de prevención		Verificación de credenciales	
Acción de contención		Implementar temporalmente servidor de la SESEA ya existente	
Acción de corrección		Reportar falla al prestador del servicio	
5	Riesgo	Probabilidad	Impacto
Falla física del VPS		Baja	Alto
Acción de prevención		Preparar el servidor de la SESEA ya existente con las herramientas del VPS	
Acción de contención		Implementar temporalmente servidor de la SESEA ya existente	
Acción de corrección		Reportar falla al prestador del servicio	

Tabla 13, Riesgos identificados para la migración de la PDE al ambiente de producción

5.3.3 Ejecución del “Plan de Pruebas” en ambiente de producción.

Será solicitado el “Plan de Pruebas” en ambiente de producción a la Unidad de Servicios Tecnológicos y Plataforma Digital de la SESNA recibiendo, en dado caso, observaciones correspondientes para realizar las adecuaciones necesarias. Una vez realizados los cambios, se procede a realizar nuevamente el “Plan de Pruebas” con el fin de obtener la validación respectiva. (Ilustración 19).



Ilustración 19, Actividades para la ejecución del “Plan de Pruebas” en ambiente de producción

Posibles Riesgos

A continuación, se muestra una lista de los posibles riesgos identificados para la ejecución de esta actividad.

MATRIZ DE RIESGOS			
1	Riesgo	Probabilidad	Impacto
	Falla de dispositivos de comunicación de la Secretaría	Baja	Alto
	Acción de prevención	Utilizar equipos de protección de dispositivos	
	Acción de contención	Utilizar otro enlace de comunicación hacia el VPS	
	Acción de corrección	Reparación o reposición de dispositivo	

2	Riesgo	Probabilidad	Impacto
	Falla de accesos en el VPS	Baja	Alto
	Acción de prevención	Verificación de credenciales	
	Acción de contención	Implementar temporalmente servidor de la SESEA ya existente	
	Acción de corrección	Reportar falla al prestador del servicio	
3	Riesgo	Probabilidad	Impacto
	Falla física del VPS	Baja	Alto
	Acción de prevención	Preparar el servidor de la SESEA ya existente con las herramientas del VPS	
	Acción de contención	Implementar temporalmente servidor de la SESEA ya existente	
	Acción de corrección	Solicitar soporte técnico al prestador del servicio	

Tabla 14, Riesgos identificados en la ejecución del “Plan de Pruebas” en ambiente de producción

5.3.4 Resolución satisfactoria del plan de pruebas en ambiente de producción emitida por la Plataforma Digital Nacional.

Por cada uno de los Sistemas desarrollados, la SESEA enviará una solicitud de conexión a la Unidad de Servicios Tecnológicos y Plataforma Digital de la Secretaría Ejecutiva del Sistema Nacional Anticorrupción, realizando un conjunto de pruebas que se divide en:

- Pruebas de seguridad.
- Pruebas funcionales.
- Pruebas de estrés.

Cabe señalar que, para la aprobación de interconexión con la Plataforma Digital Nacional, es necesario contar con todos los casos de prueba evaluados exitosamente.

En caso contrario, será necesario realizar los ajustes para cumplir con todos los casos de prueba y solicitar nuevamente la validación por parte del equipo de la Plataforma Digital Nacional. (Ilustración 20).

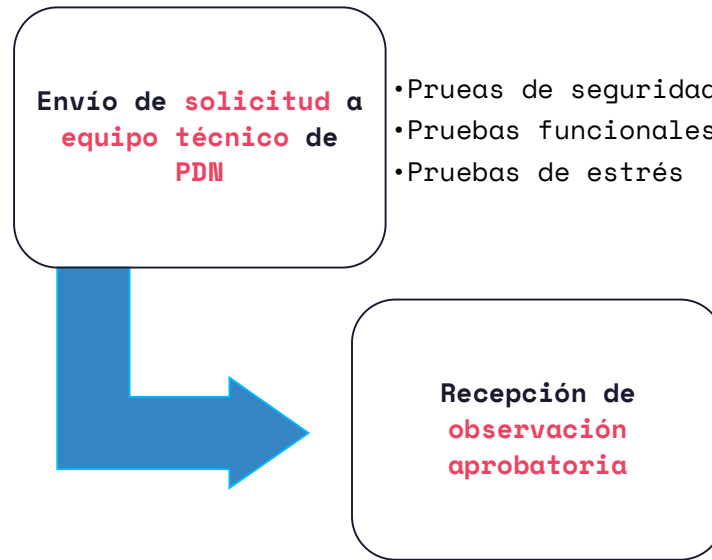


Ilustración 20, Resolución satisfactoria del “Plan de Pruebas” en ambiente de producción

Posibles Riesgos

A continuación, se muestra una lista de los posibles riesgos identificados para la ejecución de esta actividad. (Tabla 15).

MATRIZ DE RIESGOS			
1	Riesgo	Probabilidad	Impacto
	Falla de accesos en el VPS	Baja	Alto
	Acción de prevención	Verificación de credenciales	
	Acción de contención	Implementar temporalmente servidor de la SESEA ya existente	
	Acción de corrección	Reportar falla al prestador del servicio	
2	Riesgo	Probabilidad	Impacto
	Falla física del VPS	Baja	Alto

Acción de prevención	Preparar el servidor de la SESEA ya existente con las herramientas del VPS		
Acción de contención	Implementar temporalmente servidor de la SESEA ya existente		
Acción de corrección	Solicitar soporte técnico al prestador del servicio		
3	Riesgo	Probabilidad	Impacto
	Problemas de comunicación con PDM	Baja	Alto
Acción de prevención	Envío de solicitud por correo electrónico a diversos usuarios		
Acción de contención	Promover la PDE		
Acción de corrección	Notificar a la PDM		

Tabla 15, Riesgos identificados para la resolución satisfactoria del “Plan de Pruebas” en ambiente de producción

5.3.5 Definición del plan de monitoreo de la Plataforma Digital Estatal.

Se definirá un plan de monitoreo del comportamiento de la PDE en un ambiente de producción para solucionar y prevenir posibles fallas:

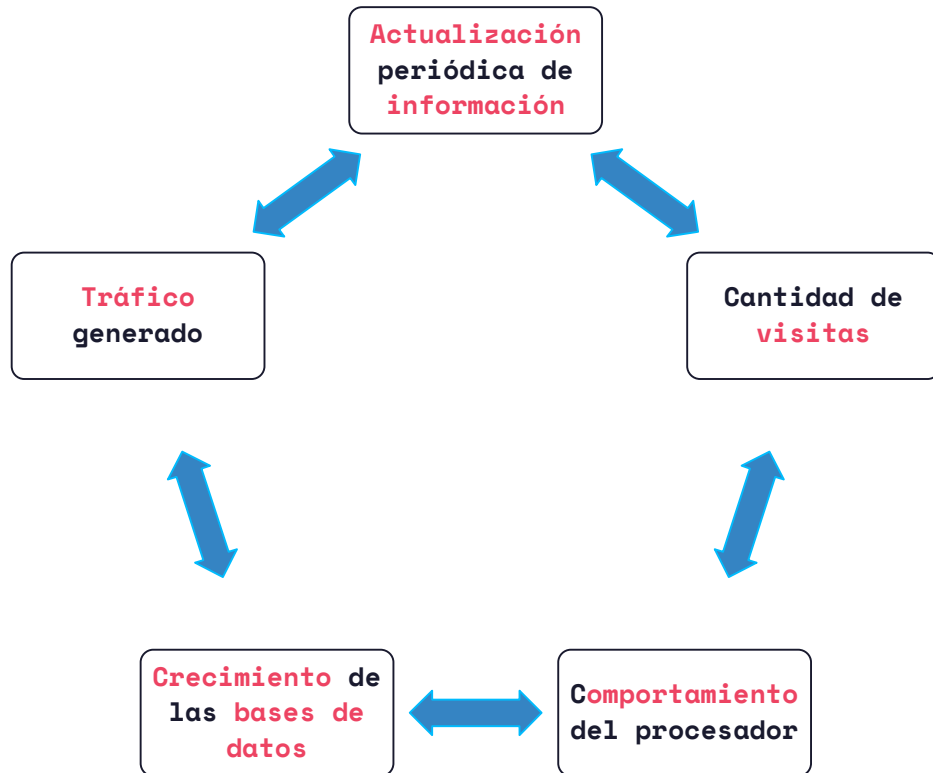


Ilustración 21, Definición de plan de monitoreo de la PDE

Posibles Riesgos

A continuación, se muestra una lista de los posibles riesgos identificados para la ejecución de esta actividad.

MATRIZ DE RIESGOS			
1	Riesgo	Probabilidad	Impacto
	Falla de accesos en el VPS	Baja	Alto
	Acción de prevención	Verificación de credenciales	
	Acción de contención	Implementar temporalmente servidor de la SESEA ya existente	

Acción de corrección		Reportar falla al prestador del servicio	
2	Riesgo	Probabilidad	Impacto
Falla física del VPS		Baja	Alto
Acción de prevención		Preparar el servidor de la SESEA ya existente con las herramientas del VPS	
Acción de contención		Implementar temporalmente servidor de la SESEA ya existente	
Acción de corrección		Solicitar soporte técnico al prestador del servicio	
3	Riesgo	Probabilidad	Impacto
Falta de información de los proveedores		Media	Alto
Acción de prevención		Realizar recordatorios periódicos a los proveedores	
Acción de contención		Implementar temporalmente servidor de la SESEA ya existente	
Acción de corrección		Solicitud de actualización de información	

Tabla 16, Riesgos identificados en el plan de monitoreo del comportamiento de la PDE en un ambiente de producción.

Contenido de Tablas

<i><u>Tabla 1. Riesgos para la identificación de proveedores de los Sistemas 2 y 3 ..</u></i>	<i><u>9</u></i>
<i><u>Tabla 2. Riesgos identificados para la agrupación de proveedores por nivel de adopción tecnológica de los Sistemas 2 y 3</u></i>	<i><u>10</u></i>
<i><u>Tabla 3. Riesgos identificados para realizar la comparativa de formatos de datos existentes contra el estándar de datos emitido por la PDN</u></i>	<i><u>12</u></i>
<i><u>Tabla 4. Riesgos identificados para el planteamiento de soluciones para interconexión con proveedores</u></i>	<i><u>13</u></i>
<i><u>Tabla 5. Riesgos identificados para la ejecución de soluciones por proveedor .</u></i>	<i><u>15</u></i>
<i><u>Tabla 6. Riesgos identificados para la integración y conexión con los proveedores</u></i>	<i><u>17</u></i>
<i><u>Tabla 7. Descripción del servidor en ambiente de desarrollo.</u></i>	<i><u>20</u></i>
<i><u>Tabla 8. Herramientas para el desarrollo de la Plataforma Digital Estatal</u></i>	<i><u>20</u></i>
<i><u>Tabla 9. Riesgos identificados para la preparación del ambiente de desarrollo</u></i>	<i><u>22</u></i>
<i><u>Tabla 10. Riesgos identificados para el desarrollo de la PDE</u></i>	<i><u>27</u></i>
<i><u>Tabla 11. Riesgos identificados para el planteamiento de soluciones para interconexión con proveedores</u></i>	<i><u>29</u></i>
<i><u>Tabla 12. Riesgos identificados para la adquisición del VPS</u></i>	<i><u>31</u></i>
<i><u>Tabla 13. Riesgos identificados para la migración de la PDE al ambiente de producción</u></i>	<i><u>33</u></i>
<i><u>Tabla 14. Riesgos identificados en la ejecución del “Plan de Pruebas” en ambiente de producción</u></i>	<i><u>35</u></i>
<i><u>Tabla 15. Riesgos identificados para la resolución satisfactoria del “Plan de Pruebas” en ambiente de producción</u></i>	<i><u>37</u></i>
<i><u>Tabla 16. Riesgos identificados en el plan de monitoreo del comportamiento de la PDE en un ambiente de producción.</u></i>	<i><u>39</u></i>

Contenido de Ilustraciones

<i><u>Ilustración 1, Flujo de información.</u></i>	<i><u>7</u></i>
<i><u>Ilustración 2, Diagrama de actividades principales.</u></i>	<i><u>7</u></i>
<i><u>Ilustración 3, Actividades principales para la obtención de información del Ejecutivo Estatal.</u></i>	<i><u>7</u></i>
<i><u>Ilustración 4, Actividades para la identificación de proveedores de los Sistemas 2 y 3.</u></i>	<i><u>8</u></i>
<i><u>Ilustración 5, Actividades para la identificación y agrupación de proveedores según el nivel de adopción tecnológica.</u></i>	<i><u>10</u></i>
<i><u>Ilustración 6, Actividades para realizar la comparativa de formatos de datos existentes contra el estándar de datos emitido por la PDN.</u></i>	<i><u>11</u></i>
<i><u>Ilustración 7, Diseño de plan de solución para obtención de información dependiendo del nivel de adopción tecnológico.</u></i>	<i><u>13</u></i>
<i><u>Ilustración 8, Ejecución de soluciones por proveedor.</u></i>	<i><u>14</u></i>
<i><u>Ilustración 9, Integración y conexión con los proveedores.</u></i>	<i><u>16</u></i>
<i><u>Ilustración 10, Implementación de la Plataforma Digital Estatal en ambiente de desarrollo.</u></i>	<i><u>18</u></i>
<i><u>Ilustración 11, Actividades para la preparación del ambiente de desarrollo.</u></i>	<i><u>21</u></i>
<i><u>Ilustración 12, Proceso “SCRUM”.</u></i>	<i><u>23</u></i>
<i><u>Ilustración 13, Proceso Cascada enriquecida.</u></i>	<i><u>24</u></i>
<i><u>Ilustración 14, Arquitectura “Modelo Vista Controlador”.</u></i>	<i><u>25</u></i>
<i><u>Ilustración 15, Desarrollo de la Plataforma Digital Estatal.</u></i>	<i><u>26</u></i>
<i><u>Ilustración 16, Actividades para la ejecución del “Plan de Pruebas” en ambiente de desarrollo.</u></i>	<i><u>28</u></i>
<i><u>Ilustración 17, Instalación de la PDE en ambiente de producción.</u></i>	<i><u>29</u></i>
<i><u>Ilustración 18, Migración de la PDE al ambiente de producción.</u></i>	<i><u>32</u></i>
<i><u>Ilustración 19, Actividades para la ejecución del “Plan de Pruebas” en ambiente de producción.</u></i>	<i><u>34</u></i>
<i><u>Ilustración 20, Resolución satisfactoria del “Plan de Pruebas” en ambiente de producción.</u></i>	<i><u>36</u></i>
<i><u>Ilustración 21, Definición de plan de monitoreo de la PDE.</u></i>	<i><u>38</u></i>

Glosario

Servidor Virtual Privado: Servidor hospedado con un prestador de servicio, la Secretaría Ejecutiva será responsable de la administración y configuración.

SCRUM: Metodología ágil y flexible para gestionar el desarrollo de software.

Sistema 2: Sistema de los servidores públicos que intervengan en procedimientos de contrataciones públicas.

Sistema 3: Sistema Nacional de servidores públicos y particulares sancionados.

API: Conjunto de reglas y especificaciones que las aplicaciones pueden seguir para comunicarse entre ellas.

Norma ISO/IEC 22237: Estándar para la seguridad física de instalaciones e infraestructuras de centros de datos.

Norma ISO/IEC 27001: Estándar para la seguridad de la información, especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información.

Información sintética: Información generada para realizar pruebas.

Sistema operativo 11.0: Plataforma de virtualización basada en sistemas de código abierto.

JavaScript: Lenguaje de programación orientado a objetos utilizado principalmente del lado del cliente.

CSS3: Lenguaje usado para definir la presentación de un documento estructurado escrito en HTML o XML.

Bootstrap: Framework CSS y JavaScript diseñado para la creación de interfaces limpias y con un diseño responsive.

JQuery: Librería de JavaScript de código abierto que permite agregar interactividad del sitio web.

PHP: Lenguaje de programación del lado del servidor de código abierto.

DataTables: Librería que permite agregar controles de interacción avanzada a tablas HTML.

Laravel: Framework de código abierto para el desarrollo de aplicaciones PHP.

Composer: Gestor de dependencias en proyectos de programación PHP.

Apache: Servidor web HTTP de código abierto multiplataforma.

Visual Studio Code: Editor de código fuente gratuito y de código abierto.

SQL: Lenguaje diseñado para administrar y recuperar información de sistemas de gestión de bases de datos relacionales.

Eloquent: ORM de Laravel para trabajar con las bases de datos.

MariaDB: Sistema de gestión de bases de datos relacional de código abierto.

PostgreSQL: Sistema de gestión de bases de datos relacional de código abierto.

HeidiSQL: Software de código abierto que permite conectarse a servidores MySQL y MariaDB.

PgAdmin: Herramienta para administrar bases de datos en PostgreSQL.

IDE: Aplicación informática que proporciona servicios integrales que facilitan el desarrollo de software.

Framework: Estructura que se establece para la organización y el desarrollo de software ayudando a unir los distintos componentes de un proyecto.

Cascada Enriquecida: Proceso lineal de desarrollo de software.

Modelo Vista Controlador: Arquitectura de software que separa los datos y la lógica de negocio de una aplicación.

Plan de Pruebas: Conjunto de pruebas realizadas por la PDN para la verificación del funcionamiento de las API's.

Código abierto: Programas por los que no se paga licencia.