



ESPECIFICACIONES TÉCNICAS

RENOVACIÓN DE LICENCIAS PARA LAS SOLUCIONES DE SEGURIDAD Y
RESPALDO DE LAS PÁGINAS WEB INSTITUCIONALES DEL PODER JUDICIAL

SANTO DOMINGO, R.D.
15 DE ENERO DEL 2025



CONTENIDOS

CONTENIDOS.....	2
NOMBRE DEL PROCESO	3
OBJETIVO GENERAL	3
INTRODUCCION	3
DE LOS BIENES Y SERVICIOS A ADQUIRIRSE.....	4
HITOS	4
FORMA DE PAGO	4
ESPECIFICACIONES TÉCNICAS	4
OTROS REQUERIMIENTOS	5
TIEMPO DE ENTREGA.....	5
LUGAR DE ENTREGA	5
CRITERIOS DE EVALUACIÓN	5
CRITERIOS DE ADJUDICACIÓN	6



NOMBRE DEL PROCESO

Renovación de licencias para las soluciones de Seguridad y Respaldo para las Páginas Institucionales del Poder Judicial.

OBJETIVO GENERAL

Renovar las licencias de las soluciones de Seguridad y Respaldo para las Páginas Institucionales del Poder Judicial de cara al alto riesgo y probabilidad de ocurrencia de ciberataques dirigidos a las instituciones públicas y al alto índice de propagación de software malicioso en portales web.

INTRODUCCION

Los proyectos de implementación del Plan Visión Justicia 20/24 y la Ley 339-22 están apoyados en tecnologías y soluciones clave como Microsoft Azure y Office 365. En este momento la infraestructura que aloja la página web <https://poderjudicial.gob.do/>, <https://transparencia.poderjudicial.gob.do/>, entre otras está alojada en la nube de Microsoft y estas páginas utilizan el gestor de contenidos WordPress.

Durante el proceso de implementación y gestión de estos servicios hemos identificado los siguientes riesgos asociados con la seguridad de los sistemas de información:

- Interrupción indefinida de las operaciones institucionales como resultado de ciberataques.
- Filtración de información confidencial.
- Pérdida de información.
- Propagación de software malicioso.

Todo esto podría derivar en daños a la reputación institucional y el incumplimiento de leyes, normas y estándares.

De cara al alto riesgo y probabilidad de ocurrencia de ciberataques dirigidos a las instituciones públicas y al alto índice de propagación de software malicioso en portales web, es necesario dar continuidad a la aplicación de controles de seguridad enfocados en estos portales web y las tecnologías que los soportan. En este caso, uno de sus componentes principales, el gestor de contenido WordPress; por lo que es mandatorio proceder con la habilitación de los siguientes servicios de suscripción.



DE LOS BIENES Y SERVICIOS A ADQUIRIRSE

Renovación de licencias de las soluciones de Seguridad y Respaldo para las Páginas Institucionales:

- a) WordPress WordFence Premium (Soluciones de seguridad).
- b) WPvivid Backup and Migration Plugin Freelancer (Complemento para el respaldo y migración de sitio web).

HITOS

El siguiente hito serán factor clave para medir el avance del proceso y liberar el pago:

- a) Hito – Entrega de licencias.

FORMA DE PAGO

La forma de pago propuesta es:

- a. **100%** pago final, contra entrega de una certificación de recepción conforme por parte de la Dirección de Tecnologías de la Información y la Comunicación.

ESPECIFICACIONES TÉCNICAS

Soluciones de Seguridad y Respaldo para las Páginas Institucionales			
No.	Especificación técnica	UDM	Cantidad
1	WordPress WordFence Premium (Soluciones de seguridad): 1.1 Lista negra de IP en tiempo real. 1.2 Actualizaciones de reglas de firewall en tiempo real. 1.3 Escaneo de Malware. 1.4 Actualizaciones de firmas de Malware en tiempo real. 1.5 Chequeo de reputación de sitios e IP. 1.6 Alertas de seguridad y reportes. 1.7 Bloqueo de Países. 1.8 Reparación de archivos. 1.9 Monitoreo en tiempo real. 1.10 Soporte en línea. Tres (03) años de suscripción	Licencias	11
2	WPvivid Backup and Migration Plugin Freelancer (Complemento de respaldo y migración de sitio web): 2.1 Migración (Auto migración).	Licencias	1



	2.2 Respaldo (carpetas y archivos, base de datos, incremental, puntos de restauración, multisitios, temas plugins). 2.3 Almacenamiento remoto (FTP, Google Drive, Dropbox, OneDrive, Amazon S3). 2.4 Calendario (incremental, contenido personalizado, tiempo de inicio personalizado). 2.5 Restauración (página web desde el almacenamiento remoto). 2.6 Roles y Capacidades (Muestra las secciones individuales de acuerdo con los roles de usuario). 2.7 Reportes (Correos). 2.8 Lista blanca. 2.9 Soporte 24*7. Un (01) año de suscripción		
--	---	--	--

OTROS REQUERIMIENTOS

Adicionalmente, de manera obligatoria, el oferente debe presentar en su Oferta Técnica lo siguiente:

No.	Descripción de Otros Requerimientos
1	Servicio de instalación y configuración de las licencias.
2	Documentación emitida por el fabricante o el representante autorizado donde se especifique que el tiempo de respuesta para soporte de la solución adquirida debe ser 8 x5 por un año.

TIEMPO DE ENTREGA

La entrega de los servicios deberá ser en quince (15) días calendario contados a partir de la recepción de la orden de compra.

LUGAR DE ENTREGA

La entrega debe ser realizada en los portales de administración del Poder Judicial.

CRITERIOS DE EVALUACIÓN

Los bienes requeridos y los otros requerimientos serán evaluados bajo el método de **cumple / no cumple**, utilizando el siguiente cuadro:

Lote	Bienes Requeridos	No.	Detalles	Cumplimiento
x	Bien Requerido	1	Especificación técnica	Cumple/No Cumple
		2	...	
		3	...	



CRITERIOS DE ADJUDICACIÓN

La adjudicación será decidida por ítem a cuya propuesta: 1) haya sido calificada como CUMPLE en las propuestas técnicas y económicas por reunir las condiciones legales, técnicas y económicas requeridas en el presente Pliego de Condiciones, y 2) presente el menor precio.

El oferente que resulte adjudicatario deberá firmar un Acuerdo de Confidencialidad antes de iniciar con la implementación.

Aseguramos que los criterios utilizados para la elaboración de este documento están basados en los principios éticos, de transparencia, de imparcialidad y de procurar proteger los intereses del Poder Judicial.

Este documento sustituye, deroga y deja sin efecto cualquier otro relativo a las especificaciones técnicas para la Renovación de licencias para las soluciones de Seguridad y Respaldo para las Páginas Institucionales del Poder Judicial.

Elaborado por:

Bernardo Barreiro

Coordinador de Seguridad y
Monitoreo TIC

Luis A. Vargas De La Cruz

Analista Sr. de Seguridad y
Monitoreo TIC

Adderli de la Rosa

Coordinador de Seguridad
de Infraestructura

Revisado por:

Emmanuel E. Tejada

Subdirector de Seguridad de la Información y servicios TIC