

Términos de referencia

RENOVACION DE HERRAMIENTAS DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE PORTAL WEB Y APLICACIONES DE LA DIRECCIÓN GENERAL DE MIGRACIÓN

Marzo de 2025 Santo
Domingo, D. N.



INDICE

<i>1</i>	<i>Nombre del proceso y disposiciones generales</i>	<i>2</i>
<i>2</i>	<i>Descripción general del proceso</i>	<i>2</i>
<i>3.</i>	<i>Objetivos del proceso</i>	<i>2</i>
<i>4.</i>	<i>Sobre las herramientas de Ciberseguridad.....</i>	<i>3</i>
<i>5.</i>	<i>Sobre la experiencia de los oferentes.....</i>	<i>4</i>
<i>6.</i>	<i>Entregables del proceso.....</i>	<i>5</i>
<i>7.</i>	<i>Condiciones mínimas requeridas para la ejecución del proceso.....</i>	<i>5</i>
<i>8.</i>	<i>Requerimiento de Acuerdo de Nivel de Servicios.....</i>	<i>5</i>
8.1.	Objetivo	5
8.2.	Alcance	5
8.3.	Definiciones de Severidad de las averías	6
8.4.	Urgente	6
8.5.	Definiciones de Tiempo ante reportes de avería.....	7
8.6.	Excepciones de cumplimiento a los tiempos de respuesta y resolución	8
8.7.	Violaciones al acuerdo de nivel de servicios.....	8
8.8.	Medición de Cumplimiento de Indicadores de Calidad y desempeño.....	8
8.9.	Revisión y Mejora Continua.....	9



1 Nombre del proceso y disposiciones generales

Adquisición e implementación de herramientas de ciberseguridad para la protección de portal web y aplicaciones de la Dirección General De Migración.

Las informaciones y especificaciones técnicas descritas en el presente documento son de uso confidencial, con la finalidad de que los oferentes/proponentes puedan preparar propuestas para el presente proceso. Las mismas no podrán ser divulgadas o publicadas por los oferentes o el personal que este bajo la responsabilidad de este.

2 Descripción general del proceso

La Dirección General de Migración de la República Dominicana se propone incrementar la seguridad de su infraestructura tecnológica, mediante la adquisición e implementación de herramientas de ciberseguridad consolidadas en un Centro de Operaciones de Seguridad y Centro de Operaciones de Red, que permita proteger el portal web, aplicaciones e información sensible de la institución.

3 Objetivos del proceso

Los objetivos perseguidos por la Dirección General de Migración, al momento de desarrollar el proceso antes mencionado, radican en los siguientes aspectos fundamentales:

- a) Fortalecer las capacidades de ciberseguridad de la Dirección General de Migración.
- b) Lograr que Dirección General de Migración cuente con una infraestructura tecnológica que garantice la seguridad, confidencialidad, integridad y disponibilidad de sus sistemas.
- c) Por lo que, la Dirección General de Migración se propone invitar a diferentes oferentes con experiencia en el desarrollo de procesos para el diseño e implementación de una solución de seguridad cibernética orientadas a la integridad de sistemas.



4 Sobre las herramientas de Ciberseguridad

Esta plataforma deberá incluir licencia para 12 meses a partir de su implementación y debe poseer las siguientes características sin limitarse a:

- La Web Application Firewall (WAF) debe poseer capacidad de optimización web, DNS y CDN; aplicando seguridad WAF, limitación de velocidad, certificados digitales (SSL) y que permita una visibilidad completa del tráfico y las vulnerabilidades para la toma de decisiones.
- WAF debe proteger contra ataques basados en aplicaciones (capa 7) y que sea escalable para proteger las aplicaciones web críticas de ataques maliciosos.
- Debe proteger las páginas de internet contra ataques de inyección de código SQL, secuencias de comandos en sitios cruzados y solicitudes de falsificación entre sitios.
- Debe ser flexible y de fácil administración e integración con otras aplicaciones.
- Protección DDoS avanzada contra ataques volumétricos de capa 3/4/7 para proteger los sitios web, aplicaciones y redes completas garantizando que el rendimiento del tráfico legítimo no se vea comprometido.

4.1 Sobre el dimensionamiento de la solución.

Con la finalidad de que los oferentes puedan estimar el alcance de sus propuestas para la adquisición de la herramienta de seguridad a continuación se describe el alcance mínimo que debe poseer:

Solución Application Security Advanced

- Plan Enterprise - SaaS - 12 Meses (1 Yr)
- Application Security Advanced
- DNS queries 150 (MM) / CDN 250(MM) Request
- WAF / Advanced DDoS
- Advanced Rate Limiting
- 5 Primary Domains
- 5 Advanced Certificate Manager
- 10 TB Mensual
- Bot Management 250(MM)
- API Shield 250(MM)
- Argo Smart
- Load Balancing con 2 orígenes y capacidad para 50 millones de solicitudes.
- Spectrum, con soporte para 50 conexiones concurrentes y 0.5 TB de transferencia.
- Plan de soporte Premium (CSM) 24x7x365, que incluye horas de servicio profesional.
- Servicios profesionales, con 60 horas dedicadas a la configuración de dominios y reglas WAF.



- Capacitación técnica, que consta de 5 sesiones de 3 horas cada una, sumando un total de 15 horas.

Nota:

1. *Todas las soluciones tecnológicas que formen parte del sistema propuesto, y su arquitectura deberán estar diseñadas para que sea escalable, para garantizar el crecimiento futuro de acuerdo con la evolución de las amenazas y necesidades futuras.*
2. *Todas las soluciones tecnológicas deberán estar sustentadas con entrenamientos para procurar un óptimo aprovechamiento de la tecnología disponible.*
3. *Todas las soluciones tecnológicas que formen parte del sistema propuesto deberán cumplir con las mejores prácticas de seguridad de la información para garantizar la integridad de estas.*
4. *No deberán incluir tecnologías que se encuentren en etapa de prueba, esto quiere decir que los sistemas, programas y equipamientos propuestos deberán estar instalados y en funcionamiento satisfactoriamente en proyectos similares.*
5. *Deberá presentarse un listado de todos las herramientas y aplicaciones propuestos, en donde se indique especificaciones técnicas y capacidades de estos.*

5 Sobre la experiencia de los oferentes y certificaciones

- Experiencia

Los oferentes deberán contar con experiencia en el desarrollo de 3 o más proyectos de implementación de soluciones de ciberseguridad a instituciones de seguridad nacional.

El oferente debe ser partner de la marca y estar autorizado para prestar este servicio en el País

- Certificaciones

Para asegurar la correcta configuración de la solución y optimizar su uso, así como proporcionar soporte post-venta, los oferentes deberán presentar constancia de las siguientes certificaciones:

***ASP I / ASP II / ASA / ACE / ASE ***



6 Entregables del proceso.

- a. Credenciales de administración de todas las herramientas implementadas.
- b. Entrenamiento y transferencia de conocimiento al personal de DGM.
- c. Documentación para entrega del proceso.
- d. Soporte local por 1 año 24/7/365 de la empresa que hace la implementación.
- e. Soporte por 1 año de la empresa fabricante.

7 Condiciones mínimas requeridas para la ejecución del proceso.

Las condiciones mínimas que se indican han sido desarrolladas de forma enunciativa, no limitativa, lo que quiere decir, que los oferentes deberán incluir todas las opciones que según su experiencia en proyectos iguales o similares sean necesarios para lograr los objetivos perseguidos por la Dirección General de Migración en el desarrollo del proceso en cuestión.

8 Requerimiento de Acuerdo de Nivel de Servicios.

8.1. Objetivo

El objetivo de este Documento es proporcionar a las partes interesadas los mecanismos adecuados para lograr un nivel de soporte y servicio, conocido como Acuerdo de Nivel de Servicio (SLA, por sus siglas en inglés) que cumpla con los requisitos de la Dirección General de Migración.

8.2. Alcance

El alcance de este documento se limita a los bienes y servicios ofrecidos bajo el proceso de Implementación de una solución integral para fortalecer las capacidades de ciberseguridad de la Dirección General de Migración de República Dominicana.



8.3. Definiciones de Severidad de las averías

Todos los casos y solicitudes deberán ser clasificados según su nivel de criticidad, lo cual se define a continuación:

a. Baja

Consulta técnica y/o de uso. Las tareas se desarrollan y los equipos funcionan normalmente, no se ve comprometida la calidad de los servicios a los usuarios, clientes internos, externos y partes interesadas.

b. Media

Los equipos y sistemas continúan funcionando, pero de manera degradada, pueden estar informando sobre posibles daños o mal funcionamiento. Se puede percibir pérdida de calidad para la entrega de productos y servicios a la Dirección General de Migración.

c. Alta

Los equipos y sistemas enfrentan problemas que pudieran imposibilitar que estos cumplan sus objetivos, o que el centro fuera incapaz de recibir las imágenes y alertas de los sistemas desplegados en la frontera. Problemas estos que pueden suceder de forma intermitente o en escenarios/condiciones específicas.

8.4. Urgente

Cualquiera, algunos o todos los equipos o sistemas presentan un problema el cual les impide iniciar u operar, afectando por completo la operación, la falla impide la entrega completa o parcial de productos o servicios.

También se definen como urgentes los reportes pertenecientes a sistemas o equipos de infraestructura crítica para la Dirección General de Migración sin importar causa, contenido del reporte.



8.5. Definiciones de Tiempo ante reportes de avería.

a) Tiempo de respuesta

Tiempo que transcurre desde que se informa el caso al Oferente por cualquiera de las vías, telefónica, correo, o Ticket de servicio en el portal de mesa de ayuda y se tiene el primer contacto con cualquier consultor y/o personal de soporte.

b) Tiempo de solución

Tiempo que transcurre desde que se tiene el primer contacto o respuesta con cualquier consultor y/o personal de soporte del Oferente hasta que el caso es resuelto, validada la resolución y es cerrado.

En cada resolución de caso se deberá suministrar la Dirección General de Migración un informe de resolución del problema, causas, piezas o equipos utilizados.

c) Horario de Servicios

El horario de servicios que se utilizará para el Acuerdo de Nivel de Servicio será de lunes a viernes de 8:00 AM a 6:00 PM para los casos clasificados como **baja y media**. Para los casos clasificados como **urgente y alta** el horario es de **24 horas** y siete días a la semana (24x7).

d) Condiciones de Respuesta y Solución

El Oferente deberá crear las condiciones de un canal de mesa de ayuda para el reporte de casos y tiques, el mismo deberá contar con los campos requeridos indicando la severidad según las condiciones del o de los activos involucrados en el reporte, guiándose siempre por las pautas establecidas en este documento. Y los compromisos de respuesta y solución serán los establecidos a continuación:

Severidad	Tiempo de Respuesta	Tiempo de Resolución
Baja	Hasta 24 horas	Hasta 36 horas
Media	Hasta 8 horas	Hasta 24 horas
Alta	Hasta 4 horas	Hasta 12 horas
Urgente	Hasta 1 hora	Hasta 8 horas



La prioridad del caso luego de que se cumpla con el tiempo de respuesta y previo acuerdo con la persona que abrió el mismo, puede cambiar su severidad.

8.6. Excepciones de cumplimiento a los tiempos de respuesta y resolución

En los casos donde se realice una solución temporal y se logre devolver las capacidades a los niveles anteriores al reporte del caso, se deberá parar el conteo del tiempo de resolución, pero no se puede dar el caso como resuelto ni cerrarlo. Todas las excepciones realizadas deben ser documentadas, justificadas y deben ser aprobadas por el director del departamento de Tecnología de la Información y Comunicaciones de DGM. Las soluciones temporales no pueden exceder las 8 semanas, luego de este tiempo se considerará una violación al nivel de acuerdo de servicio.

8.7. Violaciones al acuerdo de nivel de servicios

Todas las violaciones al acuerdo de nivel de servicio serán sancionadas con indemnizaciones que estarán asociadas a los resultados de las mediciones del (SLA).

Las violaciones del acuerdo de nivel de servicio (SLA), se evaluarán trimestralmente, y los indicadores claves de desempeño (PKI) arrojarán los resultados los cuales serán usados para la toma de decisiones.

8.8. Medición de Cumplimiento de Indicadores de Calidad y desempeño.

Para establecer los indicadores de desempeño se utilizará la siguiente tabla, la cual según su nivel de cumplimiento se le asignará un valor.

Valor	Descripción
1	10% o más de los casos violaron el acuerdo de nivel de servicio (SLA)
2	20% o más de los casos violaron el acuerdo de nivel de servicio (SLA)
3	30% o más de los casos violaron el acuerdo de nivel de servicio (SLA)
4	40% o más de los casos violaron el acuerdo de nivel de servicio (SLA)



8.9. Revisión y Mejora Continua

Se establece que se debe revisar este Acuerdo de Nivel de Servicios por lo menos 1 vez al año, o si se dan alguna de las siguientes condiciones:

1. Se realizan excepciones de cumplimiento a los tiempos de respuesta y resolución a un 30% de los casos en un periodo de 3 meses.
2. Cambios significativos en la Infraestructura o en los sistemas y equipos suministrados que cambien los requerimientos de la Dirección General de Migración.

