TERMINOS DE REFERENCIA

Servicio de Hosting gestionado para las aplicaciones de SEDAPAR S.A.

1. DENOMINACIÓN DE LA CONTRATACIÓN

Servicio de Hosting gestionado para las aplicaciones de SEDAPAR S.A.

2. FINALIDAD PUBLICA

SEDAPAR cuenta con diversas aplicaciones informáticas que, por criterios de seguridad, rendimiento y disponibilidad, se encuentran operando en servidores externos e internos. Estas aplicaciones son de vital importancia, al constituir los principales medios de comunicación y soporte tanto a nivel interno como externo. Su correcta operación y disponibilidad permanente resultan esenciales para asegurar la continuidad operativa de la organización, la atención oportuna de los procesos institucionales y la prestación adecuada de los servicios a los usuarios.

3. OBJETIVOS DE LA CONTRATACION

ítem	Servicio	Prestación
ítem único	Servicio de Hosting gestionado para las aplicaciones de SEDAPAR S.A.	Principal

4. ACTIVIDAD DEL POI

AOI50012900004 GESTION DE ACTIVIDADES DEL PLAN DE GOBIERNO DIGITAL IMPLEMENTADO.

5. CÓDIGO CATÁLOGO ÚNICO DE BIENES, SERVICIOS Y OBRAS (CUBSO)

Nro: 3406
Código: 8111210200255399
Título: SERVICIO DE ALOJAMIENTO EXTERNO DE CORREO ELECTRONICO

6. TÉRMINOS DE REFERENCIA

6.1. DESCRIPCION Y CANTIDAD DEL SERVICIO A CONTRATAR

- Hosting de servidores en Internet
- Contratación del servicio de gestión y soporte e implementación de los requerimientos de la entidad en la red

6.2. Características técnicas

6.2.1. Servidores en la Nube

La entidad requiere tener disponible una cierta cantidad de servidores en la nube, los cuales de manera combinada puedan llegar hasta las siguientes características:

24 CPU

32 GB RAM

4TB de almacenamiento SSD

Estas características son la sumatoria total máxima que pueden lograr los recursos asignados a diferentes servidores y/o servicios que requiera la entidad.

Los recursos se podrán migrar de un servicio a otro, para poder asegurar el correcto funcionamiento de los servicios, pudiendo por ejemplo quitar memoria RAM al servicio de Pagina Web y asignarlo al Servicio de Antispam ante un posible ataque de correo no deseado.

Adicionalmente todos los servicios se deberán de mantener dentro de un Data Center ubicado dentro de Perú el cual deberá de tener direcciones IP Peruanas para la atención de los servicios web públicos estas direcciones IP, deberán de correr sobre un enlace a Internet redundado por lo menos con dos salidas locales completamente independientes.

En caso de que de alguna caída de un operador el servicio deberá de mantener las direcciones Ips Asignadas sin necesidad de mediar modificación alguna para que el segundo operador pueda ingresar, para asegurar la disponibilidad de la conexión al 100%

El Centro de Datos deberá tener la contingencia necesaria para el caso eléctrico por lo que la plataforma de alimentación primaria falle deberá de tener un generador eléctrico de ingreso automático, que permita mantener la continuidad operativa de la plataforma.

La entidad tiene un repositorio CDN de contenidos, el cual corre en PHP, esta cuenta con un peso aproximado de 20Gb, el cual constantemente es indexado por los motores de búsqueda (Google, Bing etc) por lo cual es necesario que el ancho de banda de este servicio permita entregar el contenido incluso cuando se encuentre indexado por los motores de búsqueda, esta deberá de ser almacenada como archivo de consulta en el futuro.

Adicionalmente el nuevo portal de SEDAPAR, esta desarrollado en PERL, HTML5 y postgres por lo cual el servicio de hosting deberá de optimizar los recursos necesarios tanto en volúmenes de disco duro. Para poder soportar esta plataforma.

Esta página tiene un movimiento aproximado de 21 millones visitas los últimos 12 meses, por lo cual es necesario que este servicio se encuentre siempre en línea, y pueda ser accedido tanto por IPv4 como por IPv6.

Asimismo, el proveedor se comprometerá a mantener en línea este servicio con un SLA 99.95 % de disponibilidad.

La gestión de contenidos se realizará por la entidad.

Este servidor tiene una plataforma de interconexión con el portal de transparencia del estado, el cual no se encuentra protegido por SSL, por lo que

de manera interna el servicio deberá de proxear dicha información en un formato https hasta que transparencia realice los cambios a su infraestructura.

El Servicio deberá estar detrás de un WAF el cual en caso de direcciones IP que no sean de Perú, tengo un nivel adicional de seguridad, debiendo el DNS de manera inteligente censar el origen de la conexión y en caso de que sea una IP extranjera proceda a filtrar la conexión por medio del WAF, que deberá esta fuera de la infraestructura del centro de datos, con capacidad de CDN distribuidos para control de ataques externos.

6.2.2. Servicio de Correo Electrónico

Actualmente la entidad cuenta con aproximadamente 700 cuentas de correo electrónico corporativo, las cuales son utilizadas por sus trabajadores, estas cuentas de correo electrónico generalmente son accedidas por medio de un portal web, y son protegidas por un Certificado SSL, para la confidencialidad de la comunicación.

Este servicio puede ser accedido tanto de manera interna como de manera externa.

Se determinará varios perfiles de usuarios en los cuales se tendrá la capacidad de poder restringir el espacio de su buzón, así como determinar si el correo es de manera solo interna o interna o externa.

Este Servidor de correo electrónico deberá de tener incorporado una plataforma de gestión de correos compatible con Karpersky Antivirus (Antivirus de la Entidad) para el marcado de correo electrónico. Que estará instalado en otro servidor.

La dirección IP del servidor de correo electrónico deberá ser privada, y no estar publicada dentro de los registros MX, para evitar ataques de fuerza bruta, y proveer las políticas de seguridad necesarias que bloquee la cuenta en caso de que existan una cantidad de intentos fallidos de ingreso, que podrá ser desbloqueada por el personal de informática por medio de una interface web.

Solamente el servidor AntiSPAM, deberá poder ser observado desde la internet, el servidor de correo electronico no debe permitir ninguna conexión que no esté con direcciones IP desde Perú, permitiendo para esto solo el acceso por medio de un WAF, para evitar cualquier tipo de ataque externo.

Este servicio deberá ser compatible con los protocolos IMAPs, POP3s y SMTP TLS, los protocolos que no estén cifrados por SSL deberán de ser bloqueados a excepción del SMTP ya que aún existen muchos servidores en internet que transmiten correo electrónico por canales no seguros.

El proveedor deberá de implementar las políticas de seguridad DKIM, DMARC SPF, en todos los servicios, para mantener la reputación del dominio y de las direcciones IP.

6.2.3. Servicio de AntiSpam

Actualmente SEDAPAR cuenta con un licenciamiento sobre la plataforma Antivirus Kaspersky, por lo cual se deberá de generar un servidor dedicado, para que pueda implementarse en este el servicio de AntiSPAM, este servidor deberá de recibir todo el correo electrónico enviado desde internet analizarlo y marcarlo para después enviarlo después del análisis al servidor de correo electrónico, el cual dependiendo de las etiquetas agregadas, lo colocara en la bandeja especifica (SPAM Folder).

Este servidor será el único MX que se deberá de publicar a Internet, guardando la dirección IP del servidor de correo electrónico en el anonimato para evitar posibles ataques.

Así mismo el servicio de Antispam deberá de analizar también todos los correos electrónicos de salida, con la diferencia que en vez de marcarlo lo bloqueará, esto con el objetivo de mantener la reputación de las direcciones IP en Internet.

Adicionalmente el proveedor se encargará de mantener limpia la reputación de los servicios de correo electrónico en Internet, en caso de que sea agregado a una base de datos de spammers, deberá iniciar el proceso de limpieza e informe del incidente que dio a lugar ese reporte.

6.2.4. Servicio de Listas de Correo Electrónico

Existen varias listas de correo electrónicos utilizados para la comunicación interna, estas listas de correo electrónico en especial deberán de repartir el correo electrónico a todas las cuentas de email de la empresa, previa aprobación del contenido a retransmitir por medio de una moderación.

Adicionalmente deberá de mantener un registro de toda la información enviada.

6.2.5. Backups de Información

Adicionalmente se requiere un espacio Backups de 1Tb, el cual servirá para poder tener copias de seguridad diarias de la información que la entidad requiera, siendo lo primordial el gestor de contenido y el correo electrónico

Este espacio se deberá de encontrar en una posición física diferente de donde se encuentran hospedados los servicios principales, y esta no deberá de compartir ninguna infraestructura con los recursos asignados a estos servicios para en el caso de una contingencia critica toda la información se encuentre resguardada en una posición diferente.

Esta copia de seguridad deberá estar montado dentro todos los servicios con un formato NFS, y no deberá estar disponible desde Internet.

Así mismo en caso de que se requiera esta Partición deberá ser accesible en un modo de solo lectura desde la sede administrativa, para lo cual la transmisión también utilizara el canal cifrado IPSEC, La entidad determinara desde que direcciones IP de su red interna realizara el acceso a estos recursos.

6.2.6. Servicio de DNS

Actualmente la entidad cuenta con varios dominios los cuales deberán de ser gestionados, por servidores DNS que de manera nativa tengan soporte IPv4 y IPv6, los dominios son:

sedapar.com.pe, ov.sedapar.com.pe

Todos estos dominios serán manejados por los servidores DNS que maneje el proveedor, y deberán ser administrados por los mismos, ya que deberá de realizar cualquier modificación que la entidad requiera.

Estos servidores DNS deberán estar en por lo menos dos nodos diferentes en internet, (no pertenecer al mismo segmento de red) y deberá de tener por lo menos dos, uno primario y uno secundario.

Este servidor DNS deberá de tener GeoIP activado para poder responder dependiendo el origen de la dirección IP por origen.

6.2.7. Servicio de MPLS entre SEDAPAR y el DataCenter

Existen servicios sensibles los cuales deberán de tener una capa adicional de protección por lo que se implementara un canal de comunicación encriptado entre la red donde se encontrarán los servicios y/o servidores y la red interna de SEDAPAR, esto para resguardar la privacidad de la comunicación.

El enlace deberá de ser por medio de Fibra óptica con una conexión 1:1 20Mb

Sobre este enlace se redireccionarán los siguientes servicios:

- Administración del Servidor de Correo Electrónico.
- Canalización de los Web Services para el funcionamiento de la plataforma de Pago VISA, así como para el funcionamiento de la oficina virtual.
- Administración de contenidos de la Pagina Web.
- Cualquier otro que lo requiera la entidad.
- Acceso de las máquinas de la entidad a la plataforma de correo electrónico, página web u otros que tenga hospedado dentro de su plataforma.

6.2.8. Servicio de Protección Perimétrica e Interconexión

Asimismo, todos los servicios deberán de estar interconectados a Internet con un ancho de banda simétrico de por lo menos 1Gbps, debiendo asignar a los servicios que se mantengan activos direcciones IP Publicas tanto de Versión 4 como Versión 6 como lo dispuesto en el decreto supremo 081- 2017-PCM.

Todos los servicios deberán estar detrás de una plataforma de protección Anti DoS, ya que en muchas oportunidades la Pagina web y el servidor de correo electrónico de la institución a sido producto de ataques de este tipo lo cual imposibilita el acceso a la misma, debiendo estar todos los servicios protegidos contra este tipo de ataques.

De igual manera se deberá de mantener una plataforma de Firewall para que solo los servicios necesarios estén expuestos a Internet y todos los demás

puertos estén bloqueados.

Las plataformas de gestión y administración referentes a los servicios de correo electrónico deberán estar limitadas a ser accedidas por determinadas maquinas dentro de la red de la entidad, la comunicación se realizará por medio de la MPLS y no deberá estar disponible desde internet.

Adicionalmente se deberá de proveer un servicio WAF para que todas las conexiones no procedentes de Perú tengan una capa adicional de protección.

6.2.9. Plataforma de Monitoreo

El proveedor deberá de poner a disposición de la entidad una plataforma de monitoreo donde se observe todos los recursos asignados, pudiendo observar los parámetros de uso de disco, uso de red.

En caso de falla en alguno de los elementos asignados deberá de generar una notificación por medio de mensaje de correo electrónico, SMS y/o Chat.

Esta plataforma deberá de mantener un histórico del comportamiento de los recursos durante la duración del servicio.

6.2.10. Servicio de Gestión, Implementación y Soporte

Todos los servicios serán mantenidos operativos por el proveedor debiendo este de solucionar cualquier problema de cualquier índole que se pueda presentar asegurando la permanencia de los servicios en línea.

Adicionalmente en caso se requiera deberá de implementar nuevos servicios, así como modificar la disposición de recursos en caso sea necesarios.

6.3. Entregables

Informe Técnico de las configuraciones realizadas

- Detalle de infraestructura
- Esquema de Alojamientos y redundancias
- Dominios y Direcciones IP

6.4. CRITERIOS DE CALIFICACIÓN DEL POSTOR

A. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

El postor debe acreditar un monto facturado acumulado equivalente a S/ 40 000,00 (cuarenta mil y 00/100 soles) por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los ocho (8) años anteriores a la fecha de la presentación de ofertas que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes:

- Servicios de hosting gestionado de aplicaciones institucionales.
- Servicios de alojamiento de sistemas de información.

- Servicios de data center, cloud computing o infraestructura como servicio (IaaS).
- Servicios de correo electrónico corporativo y plataformas web institucionales.
- Servicios de conectividad y servicios IP asociados a centros de datos.

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones.

B. PERFIL DEL PERSONAL

Requisitos del Personal

- **01 Personal Técnico**

  Ingeniero o bachiller titulado en ingeniería de sistemas, computación e informática, software o Ciencias de la Computación.

  Deberá acreditar mínimo tres (03) años de experiencia en soporte y mantenimiento de servicios de Web Hosting o Correo electrónico o servicios IP o servicios de alojamiento de sistemas de información.

  Copia Simple de Certificado de Capacitación técnica en RHCE (Red Hat Certified Engineer) o DCAP o LPIC o IPv6 o similar.

7. PRESTACIONES ACCESORIAS

No aplica.

8. OTROS RECURSOS QUE EL CONTRATISTA NECESITE PARA EJECUTAR LA CONTRATACIÓN

No aplica

9. MODALIDAD DE PAGO

Suma Alzada

10. PLAZO DE EJECUCIÓN

Los servicios materia de la presente convocatoria se prestarán en el plazo de **12 meses**

11. LUGAR DE PRESTACIÓN DEL SERVICIO

El servicio será brindado en forma remota desde el centro de servicio del proveedor, debiendo para ello contar con todas las facilidades de comunicación y de infraestructura

necesarios para brindar el servicio de manera idónea tanto el PROVEEDOR como SEDAPAR.

Para la implementación de todos los servicios se deberá de tener un plazo máximo de 5 días hábiles y no deberá de afectar la continuidad de los servicios.

Si el PROVEEDOR considera que es necesario la asistencia presencial, en este caso el PROVEEDOR asume los gastos de traslados, alojamiento y viáticos.

En caso de que sea requerido el proveedor deberá de realizar la migración de todos los contenidos, y este deberá de asegurar la continuidad de la funcionalidad.

12. SISTEMA DE ENTREGA

No Aplica

13. FORMA DE PAGO

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en una (1) armada, a los 10 Días de recibida la conformidad de implementación de todos los servicios y recepción de los entregables respectivos

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- Conformidad emitida por el Departamento de Tecnologías de Información y Comunicación, emitiendo su conformidad de la prestación efectuada, cumplimiento de Términos de Referencia y demás obligaciones del contratista.
- Comprobante de pago.

Dicha documentación se debe presentar en SGD (Sistema de Gestión Documental) ubicado en la página Web de SEDAPAR S.A. (https://sgd.sedapar.com.pe/pages/inicio) o en la Oficina de Tramite Documentario (Mesa de Partes) de SEDAPAR S.A. sito en Av. Virgen del Pilar N° 1701, distrito de Arequipa, provincia de Arequipa, departamento de Arequipa.

El pago se realiza en un plazo máximo de diez días hábiles luego de otorgada la conformidad por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles.

14. CONFORMIDAD

La conformidad será emitida por el Departamento de Tecnologías de la Información y Comunicación.

La conformidad se emite en un plazo máximo de siete días contabilizados desde el día siguiente de recibido el entregable, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación, o si se trata de consultorías, en cuyo caso la conformidad se emite en un plazo máximo de veinte días, bajo responsabilidad del servidor o funcionario que debe emitir la conformidad. La sola recepción de bienes en la entidad o en el destino final, según sea el caso, no constituye la conformidad del área usuaria.

15. GARANTÍA COMERCIAL

No aplica

16. VICIOS OCULTOS

La recepción conforme de la prestación por parte de LA ENTIDAD CONTRATANTE no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 69 de la Ley N° 32069, Ley General de Contrataciones Públicas y el artículo 144 de su Reglamento.

17. RESPONSABILIDAD DEL CONTRATISTA

- Deberá proporcionar los medios de comunicación para atención de incidentes por fallas (Correo electrónico, teléfono u otro)

- El contratista será responsable por todos los desperfectos causados por su personal, y deberá reparar o reponer las instalaciones y bienes dañados por su personal.

- El contratista deberá asegurar a sus trabajadores que ingresen a las instalaciones de SEDAPAR S.A. mediante el Seguro Complementario de Trabajo de Riesgo (SCTR) por la cobertura de accidentes de trabajo y enfermedades ocupacionales.

18. PENALIDADES

18.1. PENALIDAD POR MORA EN LA EJECUCIÓN

Artículo 120 del Reglamento

Penalidad por Mora en la ejecución de la prestación:

En caso de retraso injustificado del proveedor en la ejecución de las prestaciones objeto del contrato, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable.

La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:
Penalidad diaria = 0.10 x monto
F x plazo en días
Donde F tiene los siguientes valores:
Para bienes y servicios: F = 0.40.
Para obras:
a) Para plazos menores o iguales a sesenta días: F = 0.40
b) Para plazos entre sesenta y uno a ciento veinte días: F = 0.25
c) Para plazos mayores a ciento veinte días: F = 0.15
Para consultorías de obras:
a) Para plazos menores o iguales a sesenta días: F = 0.40
b) Para plazos mayores a sesenta días: F = 0.25

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato, componente o ítem que debió ejecutarse o, en caso de que estos involucren entregables cuantificables en monto y plazo, al monto y plazo del entregable que fuera

materia de retraso.

En el caso de sistemas de entrega de obra y consultoría de obra que contenga más de un componente el monto y plazo corresponde al componente que se ejecuta.

En caso no sea posible cuantificar el monto de la prestación materia de retraso, la entidad contratante establece en las bases la penalidad a aplicar.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobada. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando el contratista acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso, la calificación del retraso como justificado por parte de la entidad contratante no da lugar al pago de gastos generales ni costos directos de ningún tipo.

18.2. OTRAS PENALIDADES

No aplica

19. ADELANTOS

No aplica

20. GARANTÍAS DE FIEL CUMPLIMIENTO

No aplica

21. CLAUSULA ANTICORRUPCIÓN Y ANTISOBORNO

A la suscripción de este contrato, EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante.

Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación[1] y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las

[1] Artículo 9 de la Ley N°32069, Ley General de Contrataciones Públicas.

autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato[2]. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco[3]. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar[4].

22. SOLUCIÓN DE CONTROVERSIAS

La solución de controversias será a través Centro de Conciliación designado por las partes.

23. RESOLUCIÓN DE CONTRATO POR INCUMPLIMIENTO

Se aplicará el Artículo 122 del Sub Capitulo III Incumplimiento del contrato del Capitulo V Disposiciones generales de ejecución contractual para bienes y servicios del Reglamento de la Ley General de Contratación Públicas

24. GESTIÓN DE RIESGOS

Conforme al artículo 128 del Reglamento en caso NO se realice este servicio puede ocasionar:

- Interrupción de la operatividad institucional, afectando la disponibilidad de las aplicaciones informáticas críticas de SEDAPAR S.A.
- Caída del portal web institucional, impidiendo el acceso de los usuarios internos y externos a los servicios digitales de la Entidad.
- Indisponibilidad del servicio de correo electrónico corporativo, afectando la comunicación interna y externa.
- Pérdida o corrupción de información institucional, ante la inexistencia de copias de seguridad actualizadas y mecanismos de recuperación.
- Afectación a los servicios de pago electrónico y oficina virtual, generando retrasos en la atención a los usuarios y potenciales reclamos.
- Incremento del riesgo de ciberataques (DoS, fuerza bruta, spam, malware), ante la

[2] Literal d) del Numeral 68.1 del Artículo 68 de la Ley N°32069, Ley General de Contrataciones Públicas.
[3] Literal d) del artículo 274 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas
[4] Numeral 122.6 del artículo 122 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas.

falta de plataformas de seguridad perimetral, WAF y AntiSpam.

- Incumplimiento de los niveles de servicio (SLA) requeridos, afectando la imagen institucional y la confianza de los usuarios.