LA PREVISORA S.A. COMPAÑÍA DE SEGUROS

RESPUESTA A OBSERVACIONES

INVITACIÓN ABIERTA No. 005 – 2023

GERENCIA DE TI
SUBGERENCIA DE INTRAESTRUCTURA Y SERVICIOS DE TI

OBJETO
"Implementación de una solución que permita la administración, identificación, detección, protección y respuesta frente a posibles brechas de seguridad a nivel de fuga de información DLP"

MARZO 2023

RESPUESTA A OBSERVACIONES PRESENTADAS AL DOCUMENTO DE CONDICIONES DEFINITIVAS DE LA INVITACIÓN ABIERTA No. 005 – 2023

OBJETO: "realizar la implementación de una solución que permita la administración, identificación, detección, protección y respuesta frente a posibles brechas de seguridad a nivel de fuga de información, como lo es la solución de DLP (en inglés Data Loss Prevention)"

Agradecemos a todos los oferentes por sus observaciones y a continuación daremos respuesta a las mismas:

I. OBSERVACIONES PRESENTADAS POR EL PROVEEOR ETEK

OBSERVACIÓN No 01:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_ MINIMOS		Quien envía la información? Donde están ubicados? Podrían compartir una arquitectura conceptual que permita identificar donde estan ubicados los activos críticos donde se almacena la información ? Onpremise (Ej. Fileserver), Herramientas colaboraitvas (Ej. Onedrive), Nubes (Ej. AWS S3 Bucket),

RESPUESTA: Para cada una de las observaciones, nos permitimos indicar lo siguiente:

a. La información y documentación de las políticas a aplicar sobre el servicio de DLP es revisado al interior de la compañía y somos nosotros quienes enviaremos los parámetros de configuración.
b. La ubicación de los archivos dependerá del proceso y área respectiva, las ubicaciones principales son los servidores de file server, sharepoint, onedrive e incluso en los equipos de usuario final.
c. No es posible compartir esta informacion, en razón a que se debe efectuar implementación de la solución teniendo en cuenta las fases de Gartnet para DLP ya que la solución es nueva en la compañía.

OBSERVACIÓN No 02:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_ MINIMOS		Cuáles son los medios de trasporte de la información? Compartir Casos de Uso. Por Ejemplo. Origen: Usuarios área financiera Destino: Usuarios finales / proveedores/ Gerencia Tipo de información: PII - Información de identificación personal de clientes como: Nombre, Apellido, CC, Ubicación, Sexo, celular. – PCI – Tarjetahabiente Medio de Transporte: Correo electrónico - O365

RESPUESTA: Nos permitimos indicar que los medios de transporte deben incluir correo electrónico, aplicaciones de nube, servicios web y en general todos los servicios en los que se comparte información. Con respecto al caso de uso, esta información se encuentra recolectada por el área interna de riesgos donde se especifican los mismos ítems descritos en el ejemplo entregado.

OBSERVACIÓN No 03:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_MINIMOS		Los grupos de usuarios al interior que manejan información más sensible estan configurados en grupos en el Directorio activo?

RESPUESTA: Nos permitimos indicar que no se cuenta con esta organización al interior de la compañía.

OBSERVACIÓN No 04:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_MINIMOS		Hay información o patrones específicos de información que solo se maneje al interior de la compañía que estén interesados en monitorear?

RESPUESTA: Nos permitimos indicar que si existen patrones específicos al interior de la compañía. A nivel de monitoreo, se confirma que se establecerán pautas en lo relacionado al alcance del al contrato.

OBSERVACIÓN No 05:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_MINIMOS	22. La solución debe ser capaz de integrarse y operar en diferentes plataformas de SO.	Compartir la versión y tipo de sistema operativo a integrar en la solución.

RESPUESTA: Nos permitimos aclarar que las integraciones a las que hacemos referencia son compatibilidades con sistemas operativos Windows 10 o superior para Pc´s, para servidores tenemos sistemas operativos server 2012 en adelante y Linux red hat entre otros, con el fin de que la plataforma soporte cualquier tema que pueda pasar por medio de estos sistemas operativos.

OBSERVACIÓN No 06:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_MINIMOS		Confirmar cuantos de los 1500 dispositivos son móviles, es decir que se necesite controlar fuera del perimetro, teletrabajo o celulares.

RESPUESTA: Nos permitimos indicar que los 1500 son por usuario y no por dispositivo, la información específica de dispositivos no es posible entregarla ya que lo que se requiere es controlar el acceso dependiendo las políticas establecidas, sin importar desde donde se efectué la conexión para el caso de Microsoft365.

OBSERVACIÓN No 07:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_MINIMOS		Que Firewall utilizan para control de seguridad perimetral?

RESPUESTA: Nos permitimos indicar que la marca de firewall que actualmente manejamos es Fortinet para el control perimetral.

OBSERVACIÓN No 08:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_MINIMOS		Como controlan la navegación Web de usuarios dentro del perimetro/oficinas y teletrabajo?

RESPUESTA: Nos permitimos indicar que el control de navegación dentro de la instalación y durante la conexión de VPN se efectúa por medio de perfiles de navegación, a nivel de teletrabajo se bloquean sitios a nivel de baja reputación y algunas url específicas, pero el acceso no es tan restringido.

OBSERVACIÓN No 09:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_ MINIMOS		Si el control utilizado es un Proxy para el control de nevegación perimetral y endpoint por favor compartir detalle de verioes, arquitectura, tipo de proxy?

RESPUESTA: Nos permitimos aclarar que el control de navegación se efectúa por medio del módulo de seguridad manejado en los firewall de nueva generación.

OBSERVACIÓN No 10:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_ MINIMOS	6. La solución debe incluir un módulo de protección contra amenazas, con el fin de evitar que los archivos validados contengan virus o alguna amenaza en particular	Aclarar la expectativa de este punto, podríamos decir que el objetivo es detectar y prevenir ataques de exfiltración basados en malware / ransomware? O Necesitan una solución adicional de Enpoint Protection / Antimalware.

RESPUESTA: Nos permitimos aclarar que la entidad cuenta con una solución de Endpoint protección, pero lo que se busca es que los documentos que se validen y sean objeto de análisis también se les pueda efectuar el nivel de protección ante cualquier virus en caso de que estos sean compartidos por medios móviles u otro dispositivo que no tengamos contemplado en nuestra solución.

OBSERVACIÓN No 11:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_ MINIMOS	22. La solución debe ser capaz de integrarse y operar en diferentes plataformas de SO.	Por favor precisar los SO objeto de integración en dispositivos móviles. Celulares, tablets, entre otros.

RESPUESTA: Nos permitimos aclarar que la solución requerida debe tener integración con Microsoft365, por lo que se busca que en cualquier dispositivo donde se efectué la apertura de los accesos no impida que por ser un dispositivo móvil las funcionalidades no sean manejadas.

OBSERVACIÓN No 12:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_ MINIMOS		Que información sensible o vectores requieres proteger en los dispositivos moviles? Ej. Correo electrónico, Navegación Web?

RESPUESTA: Nos permitimos aclarar, lo que se requiere es el control de los accesos integrados con el Microsoftoffice365 (correo, sharepoint, onedrive, teams, entre otros manejados) sin importar el dispositivo desde donde se conecte, en la mayoría de los casos los dispositivos celulares cuentan con estos accesos y puede presentarse fuga de información en esta instancia.

OBSERVACIÓN No 13:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_ MINIMOS		Por favor ampliar la expectativa de protección y prevensión para dispositivos móviles tipo Smartphones, tablets, Vetores, Tipo de dispositivos, Ubicación, enrte otros.

RESPUESTA: Nos permitimos aclarar que la expectativa hacia los dispositivos móviles se limita a las aplicaciones de Microsoft365.

OBSERVACIÓN No 14:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_MINIMOS		Los dispositivos móviles salen a navegar por la red corporativa?

RESPUESTA: Nos permitimos aclarar que no se controla la navegación sobre los dispositivos móviles.

OBSERVACIÓN No 15:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_MINIMOS	23. La solución debe permitir efectuar excepciones en el tráfico en la descripción SSL	Por favor aclarar este requerimiento. No es claro

RESPUESTA: Nos permitimos aclarar que este literal hace alusión a tráfico que podría presentarse cifrado y que por su naturaleza no pueda ser validado.

OBSERVACIÓN No 16:

005_2023_ANEXO_REQUISITOS_TECNOLOGICOS_MINIMOS		Para la implementación de la solución, es posible considerar la implementación de 30% de los agentes por parte del oferente y 70% por Previsora? O el oferente debe garantizar el 100% de la implementación.

RESPUESTA: Nos permitimos indicar que el oferente debe efectuar el 100% de la implementación, de igual forma se esta solicitando personal dedicado para la operación durante la vigencia del contrato.

OBSERVACIÓN No 17:

005_2023_ANEXO_ASPECTOS HABILITANTES	Con el fin de cumplir con la experiencia mínima habilitante, EL PROPONENTE deberá adjuntar con su propuesta máximo tres (3) certificaciones de contratos suscritos con empresas públicas o privadas nacionales en las que se acredite experiencia de la siguiente forma: ➢ El objeto, actividades u obligaciones sean iguales o similares al de la presente invitación. Entendiéndose por similar que consista en la implementación y administración de la solución de DLP (fuga de Información) ➢ El valor de la sumatoria de las certificaciones deberá acreditar una cuantía igual o superior al 75% del valor del presupuesto. ➢ El plazo de ejecución de cada contrato certificado incluidas sus prórrogas deberá ser igual o mayor a 12 meses. ➢ Los contratos certificados deben haberse ejecutado en su totalidad y/o estar en ejecución como mínimo (6) seis meses en operación.	Se sugiere a la entiad que El valor de la sumatoria de las certificaciones deberá acreditar una cuantía igual o superior al 50% del valor del presupuesto.

RESPUESTA: Agradecemos su observación, confirmamos que se realiza ajuste sobre este aspecto el cual será aclarado mediante **Adenda No. 1**.

OBSERVACIÓN No 18:

005_2023_ANEXO_CRONOGRAMA DEL PROCESO		Se sugiere a la entidad que el plazo que hay entre la entrega de pregutas y el día de entrega de la oferta sea amploado mínimo tres (3) días hábiles, con la finalidad de que la entrega quede el día 15 de marzo.

RESPUESTA: Agradecemos su observación y la misma será tenida en cuenta, este aspecto será aclarado mediante **Adenda No. 1.**

II. OBSERVACIONES PRESENTADAS POR EL PROVEEDOR INFORTEC

OBSERVACIÓN No 01:

Con base en el asunto, como oferente interesado en el proceso en mención, solicito amablemente solicitamos **NO** pedir la Certificación ISO 27001 del Proveedor como requisito habilitante, permitiendo una pluralidad de Oferentes.

RESPUESTA: Agradecemos su observación, confirmamos que se realiza ajuste sobre este aspecto el cual será aclarado mediante Adenda No. 1.

III. OBSERVACIONES PRESENTADAS POR EL PROVEEDOR I2 SISTEMAS Y SEGURIDAD INFORMATICA LTDA

OBSERVACIÓN No 1:

1. Con relación al numeral 28. "*La solución debe soportar 1500 usuarios simultáneos (esta deberá contemplar usuarios móviles y servidores si es el caso)*", *pág 54* del documento *005_2023_Documento_condiciones_definitivas.pdf.*

   Observación: Con el fin de validar el soporte para los diferentes sistemas operativos, solicitamos amablemente a la entidad aclarar de esos 1500 usuarios/licencias cuántos corresponden a:

   - Servidores Windows (especificar en lo posible que versión)
   - Servidores Linux (especificar en lo posible que distribución)
   - Estaciones de trabajo Windows (especificar en lo posible que versión)
   - Estaciones de trabajo MAC
   - Dispositivos móviles Android
   - Dispositivos móviles IOS

RESPUESTA: Nos permitimos aclarar que debido a que la solución es nueva en la compañía, se desconoce el porcentaje y la forma en que se implementara dicha solución, pero se aclara que los servicios son Microsoftoffice365, servidores Windows server 2012 en adelante, servidores Linux red hat 7.0 y superiores, estaciones Windows 10 y dispositivos móviles en cualquier gama.

OBSERVACIÓN No 2:

2. Con relación al numeral 6. "*La solución debe incluir un módulo de protección contra amenazas, con el fin de evitar que los archivos validados contengan virus o alguna amenaza en particular", pág 53* del documento *005_2023_Documento_condiciones_definitivas.pdf.*

Observación: Solicitamos amablemente a la entidad la posibilidad de eliminar este ítem, ya que esta funcionalidad hace parte de una solución de seguridad antimalware, la cual se encarga de validar malware en los archivos que se descarguen o transfieran dentro de la entidad. Por tanto, teniendo en cuenta el objeto del presente documento, el cual tiene un enfoque relacionado a una solución DLP (Data Loss Prevention), este ítem en específico requeriría funcionalidades de una tecnología diferente.

RESPUESTA: Agradecemos su observación. La entidad mantiene lo definido en el pliego de condiciones definitivas en razón a que la entidad cuenta con una solución de Endpoint protección, pero lo que se busca es que los documentos que se validen y sean objeto de análisis también se les pueda efectuar el nivel de protección ante cualquier virus en caso de que estos sean compartidos por medios móviles u otro dispositivo que no tengamos contemplado en nuestra solución.

OBSERVACIÓN No 3:

3. Con relación al numeral 7. "*La solución debe integrarse con Office365 para el control del tráfico que cursa sobre el tenant sin importar el dispositivo desde donde se efectúa el acceso (el control se debe realizar sobre la suit de office365, SharePoint, Teams entre otros que maneje la herramienta).", pág 53* del documento *005_2023_Documento_condiciones_definitivas.pdf.*

Observación: Solicitamos amablemente a la entidad modificar parcialmente este ítem, con el fin de no requerir integración directa con office365. Teniendo en cuenta que al hacer este cambio, no se va a ver afectada la funcionalidad principal requerida para el control, detección y análisis del tráfico de datos, que proviene directamente desde el equipo o servidor de los usuarios hacia la suite de office 365, incluyendo aplicativos como Teams o Sharepoint. De acuerdo con lo anterior, de ser posible, sugerimos modificarlo de la siguiente manera:

> " 7. *La solución debe ofrecer* ***protección*** *a la suite Office365 para el control del tráfico que cursa hacia el tenant de Office365, sin importar el dispositivo desde donde se efectúa el acceso (el control se debe realizar sobre la suite de office365, SharePoint, Teams entre otros que maneje la herramienta)".*

RESPUESTA: Agradecemos su observación y la misma será tenida en cuenta, este aspecto será aclarado mediante **Adenda No. 1.**

OBSERVACIÓN No 4:

4. Con relación al numeral 12. *"La solución de Email DLP no debe almacenar correos electrónicos, sólo debe analizar y calificar la información en ellos (basados en perfiles DLP) para así etiquetarlos en una cabecera y de esta manera permitir que el servidor de correo electrónico accione." pág 53* del documento *05_2023_Documento_condiciones_definitivas.pdf.*

   Observación: Las soluciones DLP a nivel de endpoint no almacenan correos electrónicos ni pueden etiquetar la cabecera, ya que esta modificación afectaría propiamente dicho paquete. Este procedimiento solo se podría realizar con una solución a nivel de red y no de endpoint. Sin embargo, un DLP de endpoint, si puede realizar detecciones, monitoreo o bloqueos de correos electrónicos, para evitar la fuga de información. De esta manera, de ser posible, solicitamos modificar este requerimiento de la siguiente manera:

   > *"12. La solución de Email DLP no debe almacenar correos electrónicos, sólo debe analizar, monitorear y calificar la información en ellos (basados en perfiles DLP)"*

   En caso de no poder eliminar ese requerimiento la entidad tendría que contemplar que para algunos fabricantes, sería necesario incluir las dos soluciones DLP Endpoint y DLP de red, lo que incrementaría los costos.

RESPUESTA: Agradecemos su observación y la misma será tenida en cuenta, este aspecto será aclarado mediante **Adenda No. 1.**

OBSERVACIÓN No 5:

5. Con relación al numeral 16. "*La solución debe permitir implementar políticas para generar una alerta al usuario donde se indique los riesgos a tener en cuenta y con base a la actividad realizada por el usuario solicitar la justificación de su acción a fin de proceder o negar la actividad, permitiendo educar a los usuarios cuando consumen cierto tipo de aplicaciones." pág 53* del documento *005_2023_Documento_condiciones_definitivas.pdf.*

   Observación: Solicitamos a la entidad dejar como opcional el requerimiento correspondiente a la "justificación de acción" por parte del usuario, teniendo en cuenta que al ser una solución DLP, su fin es evitar que información sensible o confidencial sea utilizada de manera incorrecta o indeseada por los usuarios. Por lo anterior, no tendría sentido que los usuarios justifiquen las malas prácticas, con base a su desconocimiento sobre el uso, alcance y el objetivo de tener una solución DLP en la entidad.

RESPUESTA: Agradecemos su observación y la misma será tenida en cuenta, este aspecto será aclarado mediante **Adenda No. 1.**

IV. OBSERVACIONES PRESENTADAS POR EL PROVEEDOR MSL-LATAM

OBSERVACIÓN No 1:

1. En el Anexo N. 5 requisitos tecnológicos minimos en el item 1 indican siguiente:

La plataforma debe proveerse como un servicio SaaS

Solicitamos: muy respetuosamente a la entidad se modifique el presente numeral, para que la solución a ofrecer sea en perpetua, teniendo en cuenta la criticidad de la información para que no esté expuesta a filtraciones o vulnerabilidades que afecten la entidad y de esta manera poder mitigar el riesgo. Adicionalmente a esto en el mercado solo se tienen 2 o no más de 3 fabricantes que cumplen con este requerimiento y por ende se estaría sesgando el proceso sin permitir la pluralidad de oferentes.

RESPUESTA: Agradecemos su observación, la entidad mantiene lo establecido en los pliegos en razón a que la solución se solicita como servicio y no se cuenta con infraestructura interna para suplir las necesidades.

OBSERVACIÓN No 2:

2. En el Anexo N. 5 requisitos tecnológicos mínimos en el item 4, 12, 15 indican siguiente:

4. Debe permitir aplicar políticas basadas en el contexto de usuario, tipo de dispositivo y/o aplicación, instancia SaaS (ej.: Salesforce o coreo personal) e IaaS (eje: gestor documental OnBase, NAS), contenido del documento, entre otros, debe ser capaz de inspeccionar en profundidad y entender las diferentes actividades o políticas configuradas (bloquear, autorizar, eliminar, descargar, entre otros)

15. La solución debe disponer de una base de datos de Servicios SaaS, en la que se pueda ver el nivel de riesgo de los servicios consumidos y se debe actualizar de forma continua.

18. La solución debe conectar a los usuarios remotos directamente a las aplicaciones en entornos de nube pública sin la necesidad de pasar por la infraestructura corporativa

Solicitamos: muy respetuosamente a la entidad se eliminen los numerales mencionados, debido a que en el mercado solo 2 fabricantes de esta soluciones cumplen taxativamente con el presente requerimiento y por ende se estaría sesgando el proceso sin permitir la pluralidad de oferentes.

RESPUESTA: Agradecemos su observación, se mantiene lo solicitado en el pliego de condiciones del proceso de contratación. .

OBSERVACIÓN No 3:

3. En el capítulo III numeral 21 Certificado del proveedor indican lo siguiente:

EL PROPONENTE deberá allegar con su propuesta las siguientes certificaciones:

Certificación ISO 27001. Esta norma permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.
La certificación solicitada debe estar vigente a la fecha de presentación de oferta, la firma del contrato y mantenerla vigente durante la vigencia del contrato

Solicitamos: muy respetuosamente a la entidad se elimine este requerimiento, teniendo en cuenta que si bien este proyecto de seguridad debe contar con los estándares de seguridad, esto se puede corroborar con las certificaciones de seguridad que están solicitando para los dos perfiles que deben conformar el equipo de trabajo como recurso humano solicitado dentro del proceso, esto debido a que si el personal se encuentra certificado es un aval de que las personas que estarán implementando y administrando la solución cuentan con la experiencia y el conocimiento de seguridad necesario para cumplir con cada uno de los requerimientos solicitados por la entidad dentro del presente proceso.

RESPUESTA: Agradecemos su observación, confirmamos que se realiza ajuste sobre este aspecto el cual será aclarado mediante **Adenda No. 1.**

V. OBSERVACIONES PRESENTADAS POR EL PROVEEDOR GMSSEGURIDAD

OBSERVACIÓN No 1:

1. En la pagina 64 del documento de condiciones definitivas- numeral 21 se menciona:

Certificaciones del proveedor
EL PROPONENTE deberá allegar con su propuesta las siguientes certificaciones:
Certificación ISO 27001. Esta norma permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.
La certificación solicitada debe estar vigente a la fecha de presentación de oferta, la firma del contrato y mantenerla vigente durante la vigencia del contrato.

OBSERVACION:
Teniendo en cuenta que la mayoría de empresas que distribuyen soluciones DLP no cuentan o están en proceso de obtener esta Certificación ISO 27001 y que a su vez esto podría limitar el proceso a una o dos empresas.
Se solicita por favor no sea un requisito habilitante o en su defecto aceptar que sea el fabricante de la solución quien cuente con la certificación:

Certificación del Proveedor o el fabricante
"El proponente o el Fabricante de la solución deben contar con la certificación ISO 27001"

RESPUESTA: Agradecemos su observación, y la misma será tenida en cuenta, se aclara mediante **Adenda No. 1.**

OBSERVACIÓN No 2:

2. OBSERVACION:
Se solicita a la Previsora extender la fecha de entrega de la propuesta hasta el 17 de marzo, esto dado la complejidad y cantidad de documentos que se solicita en el proceso.

RESPUESTA: Agradecemos su observación, confirmamos que se realiza ajuste sobre este aspecto el cual será aclarado mediante **Adenda No. 1.**

OBSERVACIÓN No 3:

3. En la pagina 64 del documento de condiciones definitivas- numeral 23 se menciona:

Clasificación de la solución
EL PROPONENTE deberá adjuntar la calificación y/o certificación donde se confirme que la solución de Fuga de información (DLP) o el servicio que lo refiera se encuentra entre los lideres o challenger del cuadrante de Gartner/Forrester o líder reconocido en aplicación para el último año referido.

OBSERVACION:
El ultimo cuadrante de gartner para DLP fue en el 2017, lo cual es demasiado lejos de la evolución de las tecnologias, por otra parte de acuerdo al alcance solicitado por la Previsora el requerimiento tecnico hace mas referencia a soluciones SSE; con lo cual se solicita modificar el requerimiento de forma que acepten el cuadrante de Security Service Egde (SSE).

RESPUESTA: Nos permitimos aclarar que el "Documento de Condiciones definitivas" indica lo siguiente: "**o el servicio que lo refiera**", a lo cual el proveedor puede entregar el registro de Garnert con la solución que integre dicha solución, para el caso mencionado SSE integra soluciones DLP.

OBSERVACIÓN No 4:

4. Respecto a la experiencia solicitada en la pagina 49 del documento de condiciones definitivas se menciona:

la experiencia que se acredite debe ser de la siguiente forma:
"El objeto, actividades u obligaciones sean iguales o similares al de la presente invitación. Entendiéndose por similar que consista en la implementación y administración de la solución de DLP (fuga de Información)".

OBSERVACION:

Al igual que la observación anterior y teniendo en cuenta la evolución de las tecnologias y sus nombres, se solicita a la Previsora por favor no cerrar la experiencia al nombre especifico DLP, siendo el objeto del proceso bastante amplio (*El proveedor se compromete con la Previsora S.A. a realizar la implementacion de una solución que permita la administración, identificacion, deteccion, protección y respuesta frente a posibles brechas de seguridad a nivel de Fuga de la información, como lo es la solcuion de DLP*).

Es decir se sugiere que acepten experiencia relacionada con:

Soluciones o plataformas o sistemas relacionadas con la proteccion de la informacion
y/o
soluciones o plataformas o sistemas relacionadas con seguridad de la información
y/ó
Soluciones o plataformas o sistemas relacionados con la fuga de información.
y/ó
Soluciones o plataformas o sistemas de DLP.

RESPUESTA: Agradecemos su observación y la misma será tenida en cuenta, este aspecto será aclarado mediante **Adenda No. 1.**

OBSERVACIÓN No 5:

5. Respecto a las hojas de vida mencionadas desde la pagina 56 del documento de condiciones definitivas:

OBSERVACIONES:

a. En relación al Gerente de Servicio se menciona:
Demostrar experiencia específica como Gerente de Servicio de tres (3) años.
Se solicita por favor aceptar experiencia como director o gerente o gestor de proyectos.

b. En relacion al Administrador Dedicado se menciona:
Demostrar experiencia como experiencia como administrador de soluciones DLP
Se solicita por favor aceptar experiencia en gestión o soporte o configuración o implementacion o soporte de soluciones DLP.

c. Tanto para el perfil de Gerente de Servicio como para el Administrador Dedicado se pide tener al menos 1 certificación de las mencionadas en la pagina 57 y 60.

Se solicita por favor tambien puedan aceptar una de estas certificaciones o especializaciones:
-Especialización en seguridad de la información.
-Especializacion en Gerencia de Proyectos.
- Auditor Interno ISO/IEC 27001:2013

RESPUESTA: Para cada una de las observaciones, nos permitimos indicar lo siguiente:

a. Agradecemos su observación y la misma será tenida en cuenta, este aspecto será aclarado mediante Adenda No. 1.
b. Agradecemos su observación, pero se mantienen las condiciones establecidas inicialmente en los pliegos de condiciones
c. Nos permitimos aclarar que:
    a. Para el gerente de servicio las especializaciones mencionadas se encuentran dentro del alcance solicitado, para la certificación ISO/IEC 27001:2013 Auditor Interno agradecemos su observación, pero se mantiene lo solicitado en los pliegos de condiciones definitivas. .
    b. Para el Administrador DLP, no se solicitó especializaciones, por lo tanto, se mantiene lo solicitado en los pliegos de condiciones, Para la certificación ISO/IEC 27001:2013 Auditor Interno indicamos que se efectuará modificación en Adenda No. 1.

OBSERVACIÓN No 6:

6. Respecto al numeral 2 del documento excel Anexo de requisitos Tecnologicos Minimos, que menciona:

" La solución debe contar con una consola centralizada, adicionalmente no solo se debe centrar en las soluciones de office365 (e-mail actual), sino que debe validar todo el tráfico que cursa sobre la red y la web en general"

OBSERVACION O INQUIETUD :
Por favor confirmar si el DLP debe estar en capacidad de bloquear fuga de informacion por medio de paginas WEB como foros WEB ??

RESPUESTA: Nos permitimos aclarar que el trafico web incluye sitios de baja reputación y/o Públicos que no se encuentren dentro de los estándares normales de las compañías, para el ejemplo los foros web no deben estar autorizados.

OBSERVACIÓN No 7:

7. Respecto al numeral 3 del documento excel Anexo de requisitos Tecnologicos Minimos que menciona:

" La solución debe brindar el monitoreo de extremo a extremo y garantizar que esta solución no afecte el rendimiento de los sistemas manejados y no se genere latencia en la entrega de la información emitida por la entidad, preferiblemente que el análisis de la información se efectué en la nube"

OBSERVACION O INQUIETUD :
Teniendo en cuenta que realizar el analisis, aplicación de controles e inspección del tráfico en un punto remoto afuera de Colombia puede ocasionar latencia alta en el tráfico tendría un efecto negativo en la experiencia de usuario e impactaría la productividad de la entidad, se requiere que el procesamiento de tráfico se realice en un centro de datos en el país y que garantice una latencia de procesamiento máxima??

Agradecemos confirmar la latencia aceptada por la entidad a nivel de procesamiento de trafico en la nube para trafico cifrado y trafico no cifrado.

RESPUESTA: Nos permitimos aclarar que debido a que el servicio no se encuentra implementado no es posible entregar los datos específicos, si se aclara que en lo posible se busca es una solución que no genere mayor traumatismo para los usuarios y los tiempos no se vean tan afectados.

OBSERVACIÓN No 8:

8. Respecto al numeral 4 del documento excel Anexo de requisitos Tecnologicos Minimos que menciona:

" Debe permitir aplicar políticas basadas en el contexto de usuario, tipo de dispositivo y/o aplicación, instancia SaaS (ej.: Salesforce o coreo personal) e IaaS (eje: gestor documental OnBase, NAS), contenido del documento, entre otros, debe ser capaz de inspeccionar en profundidad y entender las

diferentes actividades o políticas configuradas (bloquear, autorizar, eliminar, descargar, entre otros)"

OBSERVACION O INQUIETUD :
Considerando los riesgos de fuga de información que se pueden materializar a través del uso de instancias personales o diferentes a las institucionales, la entidad requiere que la solución esté en capacidad de aplicar políticas independientes no solo por aplicación sino por instancia de aplicación (personal vs corporativa vs de terceros?

Entendiendo que parte del alcance es poder controlar O365, agradecemos confirmar por la entidad si la tecnologia ofertada debe estar en capacidad de controlar la instancia corporativa de la entidad, la instancia personal de algun usuario y la instancia corporativa de un proveedor o tercero de Exchange, Onedrive, Sharepoint y teams y a cada una de ellas aplicarle controles granulares de DLP diferente segun los requerimientos de la entidad?

Entendiendo que parte del alcance es poder controlar O365, agradecemos confirmar por la entidad si la tecnologia ofertada debe estar en capacidad de controlar la aplicacion de Onedrive que se instala en el PC cuando intente conectarse a la instancia corporativa de la entidad o la instancia personal y aplicar controles de DLP segun lo que la entidad defina para cada caso?

RESPUESTA: Nos permitimos aclarar lo siguiente:

a. Se aclara que la implementación inicial de políticas se efectuara por instancias puntuales, si la aplicación de nuevas políticas es requerida, durante la vigencia del contrato se cuenta con personal que efectuara mejoras en la operación del servicio.
b. Se aclara que el servicio de offiice365, se solicita para instancias corporativas
c. Se aclara que el servicio requerido, requiere controlar la aplicación onedrive instalada en los equipos.

OBSERVACIÓN No 9:

9. Respecto al numeral 6 del documento excel Anexo de requisitos Tecnologicos Minimos que menciona:

" La solución debe incluir un módulo de protección contra amenazas, con el fin de evitar que los archivos validados contengan virus o alguna amenaza en particular"

OBSERVACION O INQUIETUD :
Teniendo en cuenta la diversidad de ataques que pueden afectar la entidad y los peligros inherentes a la navegación de los usuarios, se espera que la herramienta no solamente identifique archivos con malware sino también sitios con baja reputación?

Considerando que las soluciones de nube corporativas están siendo utilizadas como un vector adicional de propagación de archivos maliciosos, se espera que la inspección de archivos se realice tanto para la carga como la descarga de archivos?

RESPUESTA: Nos permitimos informar que el trafico debe validarse en ambos sentidos (carga y descarga)

OBSERVACIÓN No 10:

10. Respecto al numeral 9 del documento excel Anexo de requisitos Tecnologicos Minimos que menciona:

"La solución debe contar con el cumplimiento para la ley 1581 del 2012 de protección de datos personales del gobierno colombiano o las que la modifiquen"

OBSERVACION O INQUIETUD :

Debido a que la entidad es vigilada por la superfinanciera, es mandatorio que la tecnologia de DLP tenga plantilla nativa para la circular 05 de la superfinanciera?

RESPUESTA: Nos permitimos indicar que a nivel de la entidad no se han definido parámetros de plantillas, a lo cual por ahora no es requerida, pero en caso de solicitarla, esta deberá ser implementada.

OBSERVACIÓN No 11:

11. Respecto al numeral 12 del documento excel Anexo de requisitos Tecnologicos Minimos que menciona:

"La solución de Email DLP no debe almacenar correos electrónicos, sólo debe analizar y calificar la información en ellos (basados en perfiles DLP) para así etiquetarlos en una cabecera y de esta manera permitir que el servidor de correo electrónico accione."

OBSERVACION O INQUIETUD :

Agradecemos confirmar si la proteccion de fuga de informacion desde correo electronico corporativo es para cualquier dispositivo independiente si es un dispositivo personal (BYOD) o corporativo?

RESPUESTA: Nos permitimos indicar que la opción de Email DLP se requiere para cualquier dispositivo en el que se permita al login al correo.

OBSERVACIÓN No 12:

12. Respecto al numeral 14 del documento excel Anexo de requisitos Tecnologicos Minimos que menciona:

"La solución debe estar en la capacidad de generar alertas, validar comportamientos y notificar a terceros en caso de incidencias y/o mal uso de los servicios."

OBSERVACION O INQUIETUD :

Nos puden aclarar a que se refieren con notificar a terceros.

RESPUESTA: Nos permitimos aclarar que las notificaciones a terceros hacen alusión a que se envíen validaciones a cuentas externa de la previsora, en este caso a la plataforma SIEM de la entidad la cual se encuentra tercerizada.

OBSERVACIÓN No 13:

13. Respecto al numeral 15 del documento excel Anexo de requisitos Tecnologicos Minimos que menciona:

"La solución debe disponer de una base de datos de Servicios SaaS, en la que se pueda ver el nivel de riesgo de los servicios consumidos y se debe actualizar de forma continua"

OBSERVACION O INQUIETUD :
Teniendo en cuenta la diversidad de ángulos desde los cuales puede hacerse la evaluación de servicios de nube y la importancia de establecer un criterio aceptado en la industria, se espera que dicha evaluación se realice con base en los controles del Cloud Security Alliance?

RESPUESTA: Nos permitimos indicar que su observación es correcta. Se requiere contar con los controles de CSA (Cloud Security Alliance)

OBSERVACIÓN No 14:

14. Respecto al numeral 15 del documento excel Anexo de requisitos Tecnologicos Minimos que menciona:
"La solución debe conectar a los usuarios remotos directamente a las aplicaciones en entornos de nube pública sin la necesidad de pasar por la infraestructura corporativa"

OBSERVACION O INQUIETUD :
Se requiere que los controles de DLP sean implementados para accesos sobre aplicaciones IaaS gobernadas?

RESPUESTA: Nos permitimos aclarar que esta funcionalidad se solicita para aplicaciones que pudieran estar en nube y que no se requiere la interacción de la conexión hacia la red de previsora, por ahora la principal aplicación en nube es office365.

OBSERVACIÓN No 15:

15. Respecto al numeral 18 del documento excel Anexo de requisitos Tecnologicos Minimos que menciona:
"La solución debe tener la capacidad de entender el comportamiento de los usuarios, distinguiendo la actividad normal anómala, creando índices de comportamiento (IoBs)"

OBSERVACION O INQUIETUD :
se requiere que la actividad anómala de los usuarios se refleje en un indicador numérico que pueda emplearse dentro de las políticas de control de acceso?

RESPUESTA: Nos permitimos indicar que su apreciación es correcta, se busca validar la capacidad del comportamiento de los usuarios a las aplicaciones integradas, para entender y generar acciones y políticas nuevas ante actividades inusuales.

VI. OBSERVACIONES PRESENTADAS POR EL PROVEEDOR NEWNETSA

OBSERVACIÓN No 1:

1. Solicitamos por favor aclarar si la entidad requiere detección a nivel de agente en vectores locales (print, usb, etc).

RESPUESTA: Nos permitimos indicar que esta funcionalidad no es requerida, ya la suplimos con otra aplicación.

OBSERVACIÓN No 2:

2. Solicitamos por favor aclarar si la entidad requiere protección para móviles.

RESPUESTA: Nos permitimos indicar que lo que se busca es proteger las aplicaciones en las que integre el DLP, en este caso como principal funcionalidad se debe proteger Office365 por lo cual desde cualquier dispositivo en el que se conecte se deben aplicar las políticas del sitio, sin importar el dispositivo en el que se conecte.

OBSERVACIÓN No 3:

3. Confirmar por favor si la solución que se busca es una combinación de CASB, DLP Endpoint y SWG para control de DLP en los vectores de Correo O365, Navegación Web y vectores de endpoint.

RESPUESTA: Nos permitimos informar su afirmación es correcta, a razón de que las aplicaciones que se requieren validar en su mayoría son en nube.

OBSERVACIÓN No 4:

4. Punto 8, confirmar si es posible cubrir los dispositivos móviles a partir de integración del SWG con tecnologías de MDM especializadas en este tipo de dispositivos y cubrir así DLP sobre el tráfico de navegación.

RESPUESTA: Nos permitimos indicar que las herramientas adicionales a DLP pueden ser implementadas, con el fin de que el objeto y sus obligaciones para la fuga de informacion sea cumplido.

OBSERVACIÓN No 5:

5. Puntos 17 y 19, confirmar si con bloquear el acceso a instancias no corporativas de servicios de nube se pueden cubrir estos numerales.

RESPUESTA: Nos permitimos indicar que estos bloqueos podrían realizarse en equipos en los que se cuente con el control, pero equipos externos no habría cubrimiento, por lo cual no cumpliría la funcionalidad solicitada.

OBSERVACIÓN No 6:

6. Punto 18, confirmar si se requiere una solución de ZTNA como parte de la propuesta, o si solo se requiere procesar el tráfico a las consolas de servicios como AWS, Azure o GCP a nivel de HTTP/S.

RESPUESTA: Nos permitimos aclarar que esta funcionalidad se solicita para aplicaciones que pudieran estar en nube y que no se requiere la interacción de la conexión hacia la red de previsora, por ahora la principal aplicación en nube es office365.

OBSERVACIÓN No 7:

7. Punto 27, al ser un servicio en línea donde una indisponibilidad puede generar gran impacto en los usuarios finales, confirmar que la disponibilidad del servicio mínima definida por SLA deba ser de 99.999% para los elementos online.

RESPUESTA: Agradecemos su observación y confirmamos que este aspecto será aclarado mediante **Adenda No. 1.**

OBSERVACIÓN No 8:

8. En la experiencia técnica, la entidad solicita: "El objeto, actividades u obligaciones sean iguales o similares al de la presente invitación. Entendiéndose por similar que consista en la implementación y administración de la solución de DLP (fuga de Información)",

- **Observación:** Con el objetivo de ampliar y dar pluralidad de oferentes en el proceso y no limitar la participación en el mismo de compañías cuyo objeto se centra en temas de ciberseguridad, gentilmente solicitamos permitir la experiencia con soluciones similares como son Antimalware, y/o Cumplimiento de políticas, y/o Protección de información y/o Gestión de Identidades y/o Filtrado de Contenido.

RESPUESTA: Agradecemos su observación y la misma será tenida en cuenta, este aspecto será aclarado mediante Adenda No. 1.

OBSERVACIÓN No 9:

9. En la experiencia técnica, la entidad solicita: "El valor de la sumatoria de las certificaciones deberá acreditar una cuantía igual o superior al 75% del valor del presupuesto.",
Observación: Gentilmente solicitamos que la sumatoria de las certificaciones pueda acreditar una cuantía igual o superior al 50% del valor del presupuesto.

RESPUESTA: Agradecemos su observación, confirmamos que se realiza ajuste sobre este aspecto el cual será aclarado mediante **Adenda No. 1.**

OBSERVACIÓN No 10:

10. Solicitamos que por favor amplíen el plazo de presentación de propuestas para el siguiente 17 de Marzo de 2023.

RESPUESTA: Agradecemos su observación y la misma será tenida en cuenta, este aspecto será aclarado mediante **Adenda No. 1.**

OBSERVACIÓN No 11 (Extemporánea):

1. En la experiencia técnica, la entidad solicita: "El objeto, actividades u obligaciones sean iguales o similares al de la presente invitación. Entendiéndose por similar que consista en la **implementación y administración** de la solución de DLP (fuga de Información)", "El objeto, actividades u obligaciones sean iguales o similares al de la presente invitación. Entendiéndose por similar que consista en la implementación y administración de la solución de DLP (fuga de Información)"

   Observación: Agradecemos a la entidad validar experiencias que consistan en la implementación **y/o** administración de la solución de DLP (fuga de información).

RESPUESTA: Agradecemos su observación y la misma se modifica, este aspecto será aclarado mediante Adenda No. 1.

VII. OBSERVACIONES PRESENTADAS POR EL PROVEEDOR GLOBALTEK SECURITY

OBSERVACIÓN No 1:

1. Numeral 11. La solución DLP debe tener la habilidad para cubrir todos los métodos de acceso (navegadores, apps móviles, apps de escritorio, entre otros).

   Se entiende que el alcance de protección de DLP está orientado a servicios en la nube y no a servicios de punto final, por favor confirmar que nuestro entendimiento es correcto

RESPUESTA: Nos permitimos indicar que su entendimiento es correcto.

OBSERVACIÓN No 2:

2. Numeral 16. La solución debe permitir implementar políticas para generar una alerta al usuario donde se indique los riesgos a tener en cuenta y con base a la actividad realizada por el usuario solicitar la justificación de su acción a fin de proceder o negar la actividad, permitiendo educar a los usuarios cuando consumen cierto tipo de aplicaciones.

   Este punto tiene un objetivo similar al punto 5. ¿Por favor indicar si este punto al igual que el punto 5 es opcional?

RESPUESTA: Agradecemos su observación y la misma será tenida en cuenta, este aspecto será aclarado mediante **Adenda No. 1.**

OBSERVACIÓN No 3:

3. Numeral 21. La solución debe tener la capacidad de entender el comportamiento de los usuarios, distinguiendo la actividad normal anómala, creando índices de comportamiento (IoBs).

   Por favor confirmar nuestro entendimiento sobre el objetivo de este punto, ¿El objetivo es tener los índices de comportamiento del usuario frente a las aplicaciones web y office 365?

RESPUESTA: Nos permitimos aclarar que lo que se busca, es validar el comportamiento de los usuarios a las aplicaciones integradas, para entender y generar acciones y políticas nuevas ante actividades inusuales

VIII. OBSERVACIONES PRESENTADAS POR EL PROVEEDOR O4IT

OBSERVACIÓN No 1:

REQUERIMIENTO	OBSERVACIÓN
4. Debe permitir aplicar políticas basadas en el contexto de usuario, tipo de dispositivo y/o aplicación, instancia SaaS (ej.: Salesforce o coreo personal) e IaaS (eje: gestor documental OnBase, NAS), contenido del documento, entre otros, debe ser capaz de inspeccionar en profundidad y entender las diferentes actividades o políticas configuradas (bloquear, autorizar, eliminar, descargar, entre otros)	Se solicita respetuosamente a la entidad aclarar/modificar el requerimiento indicando a que se refiere con politicas basadas en contexto que permitan entre otras "eliminar, descargar" ya que dentro de las funcionalidades asociadas a soluciones de DLP DataLoss Prevention se encuentran asociadas entre otras a detección, analisis, clasificación y etiquetado de información, más no evitar su borrado o descarga, aun cuando sea posible monitorear estos estados, que en cambio deben ser establecidos por la entidad mediane politicas de permisos de edición.

RESPUESTA: Agradecemos su observación y nos permitimos aclarar que el contexto es donde se aplicaran las políticas de DLP, por otro lado, para las funcionalidades, indicamos que este aspecto será aclarado mediante **Adenda No. 1.**

OBSERVACIÓN No 2:

6. La solución debe incluir un módulo de protección contra amenazas, con el fin de evitar que los archivos validados contengan virus o alguna amenaza en particular	Se solicita respetuosamente a la entidad aclarar/modificar el requerimiento para permitir la pluralidad de Oferentes ya que se da a entender por "Modulo de protección contra amenazas" que se deban incluir tecnologías que son propiamente de soluciones Antimalware (o que estas incluyan como addon DLP Basico) con las que con las que ya pueda contar la entidad y por ende podrian entrar en conflicto con soluciones de DLP DataLoss Prevention especificamente creadas para este propósito, aunque DLP pueda establecer Blacklist y notificar al equipo final.

RESPUESTA: Nos permitimos aclarar que la entidad cuenta con una solución de Endpoint protección, pero lo que se busca es que los documentos que se validen y sean objeto de análisis también se les pueda efectuar el nivel de protección ante cualquier virus en caso de que estos sean compartidos por medios móviles u otro dispositivo que no tengamos contemplado en nuestra solución, a lo cual su observación no será tenida en cuenta.

OBSERVACIÓN No 3:

8. La solución debe garantizar que el agente del DLP debe actuar en todo momento de conexión aplicando las políticas del servidor DLP descritas en la nube, con eso cubriría equipos locales dentro de las instalaciones, equipos portátiles fuera de las instalaciones en modo teletrabajo y equipos celulares o móviles que estén también fuera de la red controlando el tráfico de información aun cuando el dispositivo no cuente con un dominio.	Se solicita respetuosamente a la entidad aclarar/modificar el requerimiento para permitir la pluralidad de Oferentes para tener como opcional equipos celulares ya que el control de datos en este tipo de dispositvos va orientados a Soluciones Mobile Device Management y no Data Loss Prevention

RESPUESTA: Agradecemos su observación, se mantienen las condiciones establecidas en los pliegos de condiciones en razón a que lo que se requiere es el control de los accesos integrados con el office365 (correo, sharepoint, onedrive, teams, entre otros manejados) sin importar el dispositivo desde donde se conecte, en la mayoría de los casos los dispositivos celulares cuentan con estos accesos y puede presentarse fuga de informacion en esta instancia.

OBSERVACIÓN No 4:

11. La solución DLP debe tener la habilidad para cubrir todos los métodos de acceso (navegadores, apps móviles, apps de escritorio, entre otros).	Se solicita respetuosamente a la entidad aclarar/modificar el requerimiento para permitir la pluralidad de Oferentes para tener como opcional equipos celulares ya que el control de datos en este tipo de dispositvos va orientados a Soluciones Mobile Device Management y no Data Loss Prevention.

RESPUESTA: Agradecemos su observación, se mantienen las condiciones establecidas en los pliegos de condiciones en razón a que lo que se requiere es el control de los accesos integrados con el office365 (correo, sharepoint, onedrive, teams, entre otros manejados) sin importar el dispositivo desde donde se conecte, en la mayoría de los casos los dispositivos celulares cuentan con estos accesos y puede presentarse fuga de informacion en esta instancia.

OBSERVACIÓN No 5:

18. La solución debe conectar a los usuarios remotos directamente a las aplicaciones en entornos de nube pública sin la necesidad de pasar por la infraestructura corporativa	Se solicita respetuosamente a la entidad aclarar el requerimiento puesto que dentro de las funcionalidades asociadas a soluciones de DLP DataLoss Prevention se encuentran asociadas entre otras a detección, analisis, clasificación y etiquetado de información, y no sirven de "proxy" desviando el trafico de la información analizada, protegida y clasificada.

RESPUESTA: Nos permitimos aclarar que esta funcionalidad se solicita para aplicaciones que pudieran estar en nube y que no se requiere la interacción de la conexión hacia la red de previsora, por ahora la principal aplicación en nube es office365.

OBSERVACIÓN No 6:

19. La solución debe permitir identificar una instancia personal en una aplicación corporativa para así ejercer un control granular sobre ella.	Se solicita respetuosamente a la entidad indicar si es correcto el entendimiento sobre instacia es igual a dispositivo final de usuario.

RESPUESTA: Nos permitimos aclarar que su entendimiento no es correcto, instancia personal hace alusión a accesos ajenos a temas laborales (ejm correo personal, blogs, entre otros)

OBSERVACIÓN No 7:

20. La solución debe permitir la ingesta y exportación de Indicadores de Compromiso (IOCs) de forma automática y ser aplicados únicamente en las instancias de las aplicaciones donde se quiere bloquear o permitir. Este ítem se puede presentar de manera opcional.	Se solicita respetuosamente a la entidad aclarar sí el requerimiento hace referencia hacia la capacidad de integración con soluciones de SIEM que permitan alertar incidencias de nivel Alto, Medio, Bajo según la clasificación de datos establecidos por politicas.

RESPUESTA: Nos permitimos aclarar que es correcto su entendimiento

OBSERVACIÓN No 8:

21. La solución debe tener la capacidad de entender el comportamiento de los usuarios, distinguiendo la actividad normal anómala, creando índices de comportamiento (IoBs).	Se solicita respetuosamente a la entidad aclarar sí el requerimiento hace referencia User and Entity Behavior Analytics

RESPUESTA: Nos permitimos aclarar que su entendimiento no es correcto, lo que se busca, es validar el comportamiento de los usuarios a las aplicaciones integradas, para entender y generar acciones y políticas nuevas ante actividades inusuales.

OBSERVACIÓN No 9:

22. La solución debe tener capacidad de integración y operaciones sobre distintas plataformas de SO.	Se debe especificar por parte de la entidad los sistemas operativos requeridos dado que las soluciones de DLP se integran a los terminales finales de acuerdo al desarrollo y soporte por parte de fabrica y soporte sobre fallos soportados por los fabricantes de los sistemas operativos sobre los cuales corren este tipo de soluciones.

RESPUESTA: Nos permitimos aclarar que las integraciones a las que hacemos referencia son compatibilidades con sistemas operativos Windows 10 o superior para Pc´s, para servidores tenemos sistemas operativos server 2012 en adelante y Linux red hat entre otros, con el fin de que la plataforma soporte cualquier tema que pueda pasar por medio de estos sistemas operativos. Es de aclarar que se debe tener claridad que la integración principal es a la suit de office365, por lo que allí podrían interactuar otros sistemas operativos en los que un usuario pueda ejecutar un login.

OBSERVACIÓN No 10:

26. La solución propuesta debe contar con soporte por parte del fabricante 24x7.	Se solicita modificar el requerimiento para que el soporte pueda ser prestado por el canal autorizado en la modalidad 7x24

RESPUESTA: Agradecemos su observación y confirmamos que este aspecto será aclarado mediante **Adenda No. 1.**

OBSERVACIÓN No 11:

27. La disponibilidad del servicio debe estar garantizada por un acuerdo de nivel de servicio (SLA) de 99,99% para los servicios en línea.	Se solicita respetuosamente a la entidad modificar el requerimiento para pemitir la pluralidad de oferentes el porcentaje de disponiblidad a 99,982% o caracteristicas Tier III de la infraestructura para los servicios en linea.

RESPUESTA: Agradecemos su observación y confirmamos que este aspecto será aclarado mediante **Adenda No. 1.**

OBSERVACIÓN No 12:

28. La solución debe soportar 1500 usuarios simultáneos (esta deberá contemplar usuarios móviles y servidores si es el caso)	Se solicita respetuosamente a la entidad aclarar la cantidad de dispositivos moviles que deba tratar con información confidencial y que tengan acceso a esta información o los usuarios que sí deban tener esta funcionalidad en esta clase de dispositivos representen un peso significativo frente a la totalidad de usuarios de la solución.

RESPUESTA: Nos permitimos indicar que los 1500 son por usuario y no por dispositivo, la información específica de dispositivos no es posible entregarla ya que lo que se requiere es controlar el acceso dependiendo las políticas establecidas, sin importar desde donde se efectué la conexión para el caso de Office365.

OBSERVACIÓN No 13:

31. El servicio entregado debe contar con personal externo si así lo considere para soportar la operación en caso de que el soporte dedicado no se encuentre disponible por un caso esporádico.	Se solicita respetuosamente a la entidad indicar a que se refiere con externo. Sí es correcto nuestro entendimiento, el servicio contará con soporte dedicado remoto tanto por parte del canal como fabrica.

RESPUESTA: Nos permitimos aclarar que en la invitación se solicita soporte dedicado, pero en caso de presentar alguna eventualidad, el proveedor deberá contar con soporte adicional (externo a la previsora) para suplir la operación.

OBSERVACIÓN No 14:

32. El objeto, actividades u obligaciones sean iguales o similares al de la presente invitación.Entendiéndose por similar que consista en la implementación y administración de la solución de DLP (fuga de Información)	Se solicita respetuosamente a la entidad aceptarcomo válidas las certificaciones de experiencia de controles comparables con DLP o que lo incluyan, por ejemplo las de SSE.

RESPUESTA: Agradecemos su observación y la misma será tenida en cuenta, este aspecto será aclarado mediante **Adenda No. 1.**

OBSERVACIÓN No 15:

33. El valor de la sumatoria de las certificaciones deberá acreditar una cuantía igual o superior al 75% del valor del presupuesto.	Se solicita a la entidad disminur el porcentaje a acreditar que la experiencia sea igual o mayor al 50% del valor del presupuesto.

RESPUESTA: Agradecemos su observación, confirmamos que se realiza ajuste sobre este aspecto el cual será aclarado mediante Adenda No. 1.

IX. OBSERVACIONES EXTEMPORÁNEAS PRESENTADAS POR EL PROVEEDOR SOFTWARE ONE

OBSERVACIÓN No 1:

- Por favor aclarar si se debe incluir la herramienta o si la Previsora ya cuenta con la herramienta de DLP

RESPUESTA: Nos permitimos aclarar que la solución es nueva en la compañía, se debe incluir la herramienta.

OBSERVACIÓN No 2:

- Por favor informar si la Previsora cuenta con un Gobierno de información

RESPUESTA: Nos permitimos aclarar que la previsora no cuenta con un gobierno de información, pero si contamos con un comité de datos personales y por medio de políticas descritas por parte del área de riesgos se validan los procesos de etiquetado de información.

OBSERVACIÓN No 3:

- Por favor informar el nivel de información clasificada y en porcentaje de avance cuanta información de toda la organización se encuentra ya clasificada

RESPUESTA: Nos permitimos indicar que a nivel de office365 se manejan tipos de clasificación de la informacion, pero esta es manejada de forma manual.

OBSERVACIÓN No 4:

- Por favor indicar si La Previsora cuenta con una solución de gestión de identidades seguras.

RESPUESTA: Nos permitimos indicar que La Previsora se encuentra en etapa de implementación de la misma.

OBSERVACIÓN No 5:

- Agradecemos si nos pueden compartir la información de las diferentes aplicaciones o información de los repositorios de información que cuenta actualmente la Fiduprevisora.

RESPUESTA: Nos permitimos indicar que esta información es entregada al proveedor seleccionado, por otro lado, se indica que la invitación que se adelanta es para La Previsora Seguros. ora