

	MACROPROCESO: GESTIÓN DE ABASTECIMIENTO	Código:	APO_10_1_2_FR08
	PROCESO: GESTIÓN PRECONTRACTUAL	Versión	02
	SUBPROCESO: ANÁLISIS EXTERNO E INTERNO	Clasificación	Pública clasificada
		Fecha:	19/04/2021
<b>FORMATO</b> <b>ANÁLISIS DEL SECTOR Y ESTUDIO DE MERCADO</b>			
Aprobó: <b>Sol Yadira Rojas Rivera</b> Gerente Abastecimiento Estratégico	Revisó: <b>Martha Cecilia Flórez Sánchez</b> Profesional Universitario Líder SIG	Elaboró: <b>Nicolás Martínez Benavides</b> Profesional Universitario	

DESCRIPCIÓN DE LA NECESIDAD	
1. ASPECTOS GENERALES	
<b>¿Cuál es su necesidad? Objeto</b>	Renovación del licenciamiento (1100 licencias) de Forcepoint para DLP en solución híbrida (nube privada fabricante y on premise), incluyendo soporte y garantía de fabricante para el licenciamiento Essential en modalidad 7x24.
<b>Valor de la necesidad plan de contratación</b>	\$213.631.180
1.1 CONTEXTO ECONÓMICO	
<p>En los últimos años se ha observado un cambio en la forma en que la información transita y se almacena en las empresas. Antiguamente era común el uso de medios físicos, como porta archivos, para almacenar papeles y documentos importantes. También era común que las empresas y los sectores se comunicaran a través de cartas y oficios. Actualmente, con los avances de la tecnología y la popularización del Internet, las empresas empezaron a reducir considerablemente el uso del papel y ampliar el uso de medios digitales para mejorar la comunicación y almacenar sus datos. Esta evolución ha traído una serie de beneficios para el día a día en las empresas, tales como:</p> <ul style="list-style-type: none"> <li>• Se acabaron las pilas de papeles en las oficinas, mejorando la organización y contribuyendo con la sostenibilidad y preservación.</li> <li>• Hay más espacio físico disponible en los entornos de trabajo.</li> <li>• Es posible encontrar y mantener documentos con mucha más facilidad, los documentos guardados en la nube se pueden acceder de forma remota.</li> <li>• La comunicación se da de forma más ágil y fácil, a través de e-mail y otros medios virtuales de comunicación.</li> </ul> <p>Éstos son algunos ejemplos de los beneficios que la informatización trajo a las empresas. Sin embargo, con la evolución tecnológica también surgieron los desafíos. Medios virtuales para almacenamiento e intercambio de informaciones contribuyeron al surgimiento de la necesidad de mantener la integridad de la información, un activo altamente relevante para los negocios. Evitar ataques virtuales y fuga de datos estratégicos, además de otros desafíos relacionados a la seguridad, pasa a ser preocupación en el día a día de las organizaciones, evidenciando la necesidad de inversiones de tiempo y recurso, para garantizar la integridad de los datos corporativos.</p> <p>La prevención de pérdida de datos (DLP) es una estrategia para asegurarse de que los usuarios finales no envíen información sensible o crítica fuera de la red corporativa.</p> <p>Los productos de software de DLP utilizan reglas de negocio para examinar el contenido de los archivos y etiquetar la información confidencial y crítica, para que los usuarios no pueden divulgarla. El software puede ser útil para identificar y etiquetar contenido bien definido (como los números de Seguro Social o de tarjetas de</p>	

crédito), pero tiende a quedarse corto cuando un administrador está tratando de identificar otros datos sensibles, tales como los de propiedad intelectual. Para implementar con éxito el software DLP corporativo, se necesita involucrar activamente a personal de todos los niveles de gestión en la creación de las reglas de negocio para las etiquetas.

## 1.2 CONTEXTO TÉCNICO

Positiva Compañía de Seguros S.A. desde el año 2017 tiene implementada la herramienta de DLP Forcepoint, la cual se ha venido ajustando y parametrizando de acuerdo con las necesidades y exigencias de la Compañía para garantizar la **Confidencialidad** de la información crítica de negocio.

La fuga de datos puede tener consecuencias devastadoras, desde una reputación dañada hasta multas y sanciones reguladoras. Proteger a los usuarios contra las amenazas y el robo de datos sigue siendo un desafío de TI sumamente significativo. Forcepoint DLP protege a los usuarios remotos contra amenazas avanzadas y contra el robo de datos mientras están dentro y fuera de la red con una solución fácil de usar. Las tecnologías avanzadas le permiten identificar rápidamente la información confidencial y protegerla, brindándole información forense que puede utilizarse para actuar en respuesta a ataques a las terminales dentro y fuera de la red. Forcepoint DLP protege sus datos y permite que sus trabajadores móviles realicen sus tareas donde sea que se encuentren y cuando lo necesiten.

Forcepoint es la compañía líder en seguridad cibernética de protección de datos y usuarios, encargada de proteger a organizaciones a la vez que impulsa la transformación digital y el crecimiento. Las soluciones de Forcepoint se adaptan en tiempo real a la manera en que las personas interactúan con los datos, y proporcionan un acceso seguro a la vez que permiten que los empleados generen valor.

Forcepoint DLP – Endpoint protege los datos confidenciales en dispositivos finales Windows y Mac dentro y fuera de la red corporativa. Incluye control y protección avanzada de datos inactivos (detección), en movimiento y en uso. Se integra con Microsoft Azure Information Protection para analizar datos encriptados y aplicar los controles de DLP correspondientes. Permite la autocorrección del riesgo de datos por parte de empleados basándose en mensajes de asesoramiento de DLP. La solución monitorea las cargas en la web, incluidos los HTTPS, así como las cargas en servicios en la nube como Office 365 y Box Enterprise. Integración total con Outlook, Notes y clientes de correo electrónico.

### **Características clave de Forcepoint DLP**

1. Soporte para impresión digital (incluida la impresión digital parcial) para dispositivos finales dentro y fuera de la red.
2. Compatible con Mac OS X y Microsoft Windows.
3. Protege los datos confidenciales enviados a dispositivos USB, medios extraíbles, impresoras o servicios en la nube de Microsoft Office 365
4. Política basada en encriptación de archivos para proteger los datos confidenciales almacenados en medios extraíbles.
5. Detecta los registros de IP y del cliente que se envían usando clientes de correo electrónico y correo web.
6. Con su DLP “por goteo” (Drip DLP) evalúa la actividad de transmisión acumulativa de datos en el transcurso del tiempo para descubrir fugas de pequeñas cantidades de datos.
7. Controla eficientemente el tráfico de HTTP y su flexibilidad le permite decidir qué tipo de tráfico de SSL inspeccionar.
8. Identifica actividad en la web que implica una amenaza avanzada a través de toda la cadena de ataque en terminales que operan fuera del alcance de las defensas de la red.

9. Reconocimiento Óptico de Caracteres (OCR) que identifica datos integrados en imágenes cuando están en movimiento o inactivos.
10. Identificación robusta de información de identificación personal (PII) que ofrece verificaciones de validación de datos, detección de nombres reales, análisis de proximidad e identificadores de contexto.
11. Identificación de encriptación personalizada que expone datos ocultos para evitar su detección y los controles aplicables.
12. Integración con Microsoft Azure Information Protection que analiza archivos encriptados y aplica los controles de DLP correspondientes a los datos.
13. Localización (fingerprinting) de datos estructurados (como bases de datos) y no estructurados (como documentos) que permite a los propietarios de los datos definir tipos de datos e identificar coincidencias parciales y totales entre documentos comerciales, planes de diseño y bases de datos, y luego aplicar la política o el control adecuado para esos datos.
14. Aprendizaje automatizado que permite a los usuarios entrenar al sistema para identificar datos relevantes, nunca vistos. Los usuarios brindan al motor ejemplos positivos y negativos para señalar documentos comerciales, código fuente, etc. similares.

### **1.3 CONTEXTO REGULATORIO**

1. El sector de sistemas de la información está regulado por el Ministerio de las Tecnologías de la Información y las Comunicaciones conforme a la Ley 1341 de 2009, “Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC”
2. Ley 1341 de 2009 “Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones TIC-, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones”.
3. Decreto 2618 de 2012 “Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones y se dictan otras disposiciones”.
4. LEY 1273 DEL 5 DE ENERO DE 2009 “Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado de la protección de la información y de los datos- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
5. Circular externa 007 de 2018 de la Super Intendencia Financiera de Colombia.
6. MINTIC - Resolución No. 00500 de marzo 10 de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”
7. Manual para la Gestión de Abastecimiento de POSITIVA.

### **1. ESTUDIO DE LA OFERTA**

En primer lugar, se buscó el servicio de renovación de licenciamiento de Forcepoint DLP en los acuerdos marco de TI que se encuentran disponibles en la tienda virtual del estado colombiano (TVEC) abril 2021. Como resultado de la búsqueda *No* se encuentra el producto como tal.

En segundo lugar, se procede con el envío de la invitación a participar del estudio de mercado a 3 Partner de Forcepoint. A continuación, se relacionan las ofertas presentadas:

PROVEEDOR	VALOR	IVA	TOTAL	Diferencia % Con Respecto al más bajo
GMS SEGURIDAD	\$ 247,235,370	\$ 46,974,720	\$ 294,210,090	27.38822119
SAFEID-SAS	\$ 204,900,000	\$ 38,931,000	\$ 243,831,000	12.38555393
GLOBALTEK	\$ 179,522,000	\$ 34,109,180	\$ 213,631,180	

## 2. ESTUDIO DE LA DEMANDA

¿Ha contratado la necesidad previamente?	Si <input checked="" type="checkbox"/>	No <input type="checkbox"/>
--	--	-----------------------------

Contratará nuevamente con el mismo proveedor	Si <input checked="" type="checkbox"/>	No <input type="checkbox"/>
--	--	-----------------------------

En caso de haber respondido afirmativamente, justifique su respuesta	<p>GLOBALTEK SECURITY nos brindó el servicio de implementación de esta herramienta y desde entonces nos ha ofrecido el servicio de mantenimiento con niveles especializados óptimos. Esta firma es autorizada por el fabricante ForcePoint, para darnos la atención y el mejor descuento ofrecido teniendo en cuenta la certificación del fabricante donde se identifica el proveedor como el registrado para Positiva, por lo tanto, consideramos viable hacer nuevamente la contratación con ellos.</p> <p>Técnicamente se ha realizado una labor de configuración de la herramienta que ha demandado un largo periodo de entendimiento y configuración, teniendo una curva de aprendizaje entre el proveedor y Positiva que se vería en riesgo operativo en caso de cambiar a este, considerando que la metodología establecida podría verse afectada, generando desmejoras en la productividad, generando nuevos riesgos de fuga de información mientras se adopta un nuevo método operativo.</p>	
--	---	--

<p>¿Existe Instrumentos de Agregación de Demanda? ¿Hará uso de Acuerdo Marco para la Contratación algún Acuerdo Marco que se ajuste a su necesidad de contratación? <a href="https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/acuerdos-marco">https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/acuerdos-marco</a></p>	Si <input type="checkbox"/>	No <input checked="" type="checkbox"/>
---	-----------------------------	--

En caso de existir Instrumentos de Agregación de Demanda "Acuerdo Marco" ¿el objeto de contratación y la vigencia cubren la necesidad prevista?	<p>Plazo del Acuerdo Marco      Fecha Inicio: Fecha Fin: N/A</p>
---	--

¿Hará uso de los instrumentos de Agregación de Demanda “Acuerdo Marco” para contratar su necesidad?	Si <input type="checkbox"/>	No <input checked="" type="checkbox"/>
---	-----------------------------	--

En caso de que exista Instrumentos de Agregación de Demanda “Acuerdo Marco” y de haber respondido negativamente la pregunta anterior, justifique técnicamente ¿por qué no hará uso de este?	se buscó el servicio de renovación de licenciamiento de Forcepoint DLP en los acuerdos marco de TI que se encuentran disponibles en la tienda virtual del estado colombiano (TVEC) abril 2021. Como resultado de la búsqueda No se encuentra el producto como tal.	
---	--	--

A continuación, presentamos un cuadro de los contratos realizados por Positiva con objetos similares, para las anteriores vigencias:

CONTRATO	MODALIDAD	PROVEEDOR	ALCANCE	VALOR
252 - 2017	DIRECTA	GLOBALTEK	Renovación de Websense Data Security Suite (DLP) Incluye Soporte Premiun con el fabricante. Acuerdo de servicio, soporte y mantenimiento	\$ 742,374,255
365-2020	DIRECTA	GLOBALTEK	renovación de la solución Forcepoint DLP (DLP 1100 licencias) incluyendo soporte y garantía de fabricante para el licenciamiento Essential en modalidad 7x24.	\$ 209,440,000

### 3. FIRMAY FECHA

NOMBRE DE QUIEN ELABORÓ	FIRMA	FECHA DE ELABORACIÓN
LEONARDO ESTRADA CASTRO		28 de abril de 2021