Informe de supervisión Nro. 001 de 2024

Contrato u orden de compra No:	**DBS-140 -2023**
Contratista:	K&A COMPANY S.A.S
NIT:	901.167.197-8
Objeto:	ADQUIRIR LICENCIAS DE PROTECCIÓN DE SOFTWARE Y DATOS PARA LOS EQUIPOS DE CÓMPUTO DE LA UNIVERSIDAD DEL ATLÁNTICO.
Valor:	*CIENTO TREINTA Y DOS MILLONES SEISCIENTOS OCHENTA Y CINCO MIL PESOS ($132.685.000) MONEDA LEGAL COLOMBIANA IVA INCLUIDO Y TODOS LOS TRIBUTOS QUE SE GENEREN CON LA CELEBRACIÓN, LEGALIZACIÓN, EJECUCIÓN Y LIQUIDACIÓN DEL CONTRATO*
Plazo:	*HASTA EL HASTA EL 31 DE DICIEMBRE DE 2023, A PARTIR DE LA FECHA DE SUSCRIPCIÓN DEL ACTA DE INICIO, PREVIO CUMPLIMIENTO A LOS REQUISITOS DE PERFECCIONAMIENTO DEL CONTRATO*
Contratante:	UNIVERSIDAD DEL ATLÁNTICO
Póliza de Garantía No.	*53-44-101029903*
Aseguradora:	*SEGUROS DEL ESTADO S.A.*
NIT Aseguradora:	*860.009.578-6*
Fecha de Expedición:	*07/01/2024*
Fecha de acta de inicio:	*22/12/2023*
Fecha acta de suspensión:	*23/12/2023*
Supervisor:	*Alberto Redondo Salas – Jefe Gestión Tecnológica e Información*
***MODIFICACIONES** (Si aplica)*	
Otro si No:	*N/A*
Fecha Otro si:	*N/A*
Valor Adición:	*N/A*
Prórroga del Plazo:	*N/A*
Póliza ampliada No:	*N/A*
Concepto de la	*N/A*

Adición:	
EJECUCIÓN DEL CONTRATO	
% de Ejecución del Contrato:	*100%*
% de Pagos realizados:	*0%*
% de Pagos por realizar:	*100%*

En Puerto Colombia Atlántico, a los doce (12) días del mes de enero del año 2024, se reunieron en las instalaciones de la Universidad del Atlántico, ubicada en el km 7 antigua vía Puerto Colombia, reunidos ALBERTO REDONDO SALAS identificado con C.C. 72.312.728 Jefe de la Oficina de Gestión Tecnológica e Información de la UNIVERSIDAD DEL ATLÁNTICO, en calidad de SUPERVISOR del contrato y ANDRÉS DANIEL PEREIRA OSPINO identificado con la C.C. 1.047.035.951, en representación de K & A COMPANY S.A.S.

El suscrito supervisor del contrato certifica haber supervisado la ejecución del contrato DBS-140-2023 y deja constancia que el contratista K & A COMPANY S.A.S, cumplió con las actividades que se relacionan a continuación las que se ajustan al objeto y obligaciones pactadas

<table>
<tr><th>No de obligación</th><th>Obligación</th><th>Actividad realizada por el contratista</th></tr>
<tr><td>1</td><td>“Adquirir licencias de protección de software datos para los equipos de cómputo de la Universidad del Atlántico.”
Especificaciones técnicas:
<table>
<tr><th>ÍTEM</th><th>DESCRIPCIÓN</th><th>CARACTERISTICAS</th><th>CANT.</th></tr>
</table></td><td>Las licencias fueron recibidas satisfactoriamente</td></tr>
</table>

		1	Licencia para dispositivos endpoint	• Las licencias deben contar con tecnología EDR (Endpoint Detection ad Response) • El software debe ser compatible con los siguientes sistemas operativos: ✓ Windows XP SP3 (32-bit); ✓ Windows Vista; ✓ Windows 7; ✓ Windows 8 y 8.1; ✓ Windows 10; ✓ Windows Server 2008 R2 SP1, 2008 SP2; ✓ Microsoft Windows Server 2012; ✓ Microsoft Windows Server 2012 R2; ✓ Windows Server 2016, o superior. ✓ Mac OS X EL CAPITAN 10.11, o superior. ✓ RedHat 7 o superior, Centos 7 o superior, Debian 9 o superior, CentOS 7 o superior, Ubuntu 16 o superior, Suse 15, Amazon 2. • Debe tener la capacidad de protección en tiempo real para detectar, bloquear la ejecución, remover y enviar a la cuarentena programas maliciosos (como virus, spyware, adware, troyanos, rootkits, virus de macro, backdoors, gusanos, dialers, keylogger, ransomware, y todos los otros tipos) en el punto final. • Debe ser reconocido como anti- virus por MS Windows. • Debe tener la capacidad de bloquear su desinstalación o ejecución del servicio. • Debe tener la capacidad de alertar, prevenir y eliminar completamente los PUP (programas potencialmente no deseados), y PUM (modificaciones potencialmente no deseadas). • El sistema debe tener la capacidad de detener la comunicación con direcciones de IP/URL/Domínios conocidos por hospedar contenidos maliciosos en cada punto final para prevenir la conexión a sitios web infectados, phishing, comunicación con servidores C&C (comando y control) y CDN (reds) comprometidos. • Debe confiar en la tecnología heurística inteligente para la detección de amenazas, así como otras técnicas de detección basadas en el análisis del comportamiento de archivos y programas, sin la necesidad de conta tecnologías de detección basadas en firmas. • El sistema debe proporcionar un motor de control de comportamiento para la protección contra infecciones de Ransomware de día cero/hora cero que no están cubiertas por la	500 UND.		

				base de datos de reglas regulares. • El sistema debe tener un módulo especializado para la detección de nuevas muestras y anomalías de malware, basado en tecnología de aprendizaje automático (machine- learning). • Debe tener la capacidad de monitorear y bloquear los ataques a través de conexión de escritorio remoto (RDP) para workstations y servidores, y servicios SQL, IMAP/POP/SMTP y FTP para equipos servidores. • Debe tener la capacidad de prevenir y bloquear los ataques a través de explotación de vulnerabilidades del sistema, conocidos como ataques Exploits. • La protección contra Exploits debe proporcionarse deforma independiente de la vulnerabilidad, para las aplicaciones más comúnmente utilizadas como vectores de ataque, como los navegadores, aplicaciones de Office, lectores de PDF, Java o reproductores multimedios. • La lista de aplicaciones protegidas por el módulo de protección contra Exploits debe permitir la creación de entradas personalizadas por parte del usuario administrador. • El módulo de protección contra exploits no debe precisar recibir actualizaciones periódicas y debe proporcionar tecnologías de protección totalmente sin firmas que protejan de distintos vectores de entrega de explo its al final, basados en tecnologías de análisis del comportamiento y no por tecnologías de comparación de patrones, empleadas por software de protección tradicional. • Consola de administración centralizada basada en la nube funcionalidad mínima de: crear, administrar, desplegar políticas de seguridad en los dispositivos, gestionar infraestructura de instalación y soporte a equipos instalados, control de número de licencias instaladas, reportes y estadísticas de amenazas detectadas.		

Fuente: Elaboración propia

En constancia se firma a los doce (12) días del mes de enero de 2024, por quienes intervienen:

Alberto Redondo Salas
Supervisor

Andrés Daniel Pereira Ospina
Representante Legal