	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: SEGURIDAD EN EL CORREO ELECTRÓNICO**
Fecha:	**Octubre 2023**

SEGURIDAD EN EL CORREO ELECTRÓNICO

Introducción

La Universidad de San Buenaventura, institución comprometida con la excelencia académica y la innovación, reconoce la importancia de la digitalización en la educación contemporánea. A medida que nuestras operaciones académicas y administrativas se han trasladado al ámbito digital, la seguridad cibernética ha emergido como un pilar fundamental para garantizar la protección de la información y la integridad de nuestros procesos. El correo electrónico, como herramienta esencial en nuestra comunicación diaria, es susceptible a diversos riesgos, incluyendo ataques de phishing y malware. Por ello, en nuestro compromiso con la comunidad universitaria, buscamos fortalecer la seguridad de nuestro sistema de correo en Office 365, a fin de brindar un entorno seguro y confiable para todos los usuarios.

Objetivo general

El objetivo principal de esta RFP es seleccionar y adquirir herramientas de seguridad avanzada que se integren eficazmente con Office 365. Estas herramientas deben ofrecer soluciones de seguridad específicas que detecten, prevengan y respondan a amenazas como phishing, malware, aseguren el cumplimiento de las políticas de Prevención de Pérdida de Datos (DLP), entre otros.

	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: SEGURIDAD EN EL CORREO ELECTRÓNICO**
Fecha:	**Octubre 2023**

Alcance

La propuesta debe cubrir todos los buzones del personal administrativo, que en total serian unos 700

Opción	Descripción	Cumple	No Cumple
Detección y Prevención de Phishing	La solución debe ser capaz de identificar y bloquear intentos de phishing, protegiendo a los usuarios de correos electrónicos maliciosos.		
Protección contra Malware	La solución debe proporcionar una detección y eliminación eficaz de malware en tiempo real, incluyendo spam, virus, worms, troyanos, Ransomware, entre otros.		
Prevención de Pérdida de Datos (DLP)	La solución deberá identificar y proteger automáticamente la información sensible, garantizando que solo las personas autorizadas tengan acceso a ella. Además, debe permitir la creación y gestión de políticas para controlar el flujo de datos.		
Integración con Office 365	La solución seleccionada debe integrarse sin problemas con Office 365, optimizando la experiencia del usuario y garantizando la continuidad de las operaciones sin interrupciones.		
Capacitación y Soporte	El proveedor seleccionado deberá ofrecer capacitación inicial y soporte continuo para asegurar el correcto uso y aprovechamiento de la herramienta.		
Informes y Monitoreo	La solución debe ofrecer informes detallados y herramientas de monitoreo que permitan a nuestro equipo de seguridad evaluar la efectividad de las medidas		

	implementadas y tomar decisiones informadas sobre posibles ajustes.		
Altos porcentajes en tasa de captura y falsos positivos	La solución debe tenar tasas de captura de 99,5 % y falsos positivos del 0,003% aproximadamente		
Protección contra amenaza de Múltiples Capas	La solución debe contar con protección contra amenazas de múltiples capas para correos electrónicos entrantes, con protección contra suplantación de CEO, phishing y protección, análisis de URL, espacio aislado de archivos adjuntos, protección contra Ransomware, verificación y cifrado SPF/DKIM/DMARC.		
Uso de IA	La solución debe utilizar herramientas de seguridad basadas en IA		
Funcionalidades adicionales	La solución debe permitir "informar de phishing" directamente en los clientes de correo electrónico de los usuarios finales.		
	La solución debe permitir la protección contra enlaces y archivos adjuntos maliciosos en entornos de Microsoft Teams.		
	La solución debe manejar un cifrado AES de 256 bits para todos los correos electrónicos salientes		
	La solución debe permitir la extracción de mensajes con un solo clic, permitiéndole a los administradores eliminar correos electrónicos sospechosos directamente de las bandejas de entrada de los usuarios, defensa predictiva de URL, protección avanzada contra ataques de compromiso de correo electrónico empresarial y pancartas de advertencia predictivas, que se muestran en los mensajes de correo electrónico para advertir a los usuarios sobre actividades sospechosas.		

	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: SEGURIDAD EN EL CORREO ELECTRÓNICO**
Fecha:	**Octubre 2023**

Criterios de evaluación

Ítem	Clasificación Propuestas	Peso
1	Requerimientos Técnicos	50%
2	Requerimientos Económicos	35%
3	Requerimientos Proveedor	15%
	Totales	100%

REQUERIMIENTOS TÉCNICOS	FORMA DE EVALUACIÓN
Seguridad y fiabilidad	Evalúa la robustez de la solución en cuanto a protección contra diferentes amenazas, su resistencia a fallos y la garantía de continuidad de servicio.
Compatibilidad con sistemas existentes	Considera cómo se integra la solución con otros sistemas y aplicaciones ya en uso en la universidad, para garantizar una implementación sin contratiempos.
Interfaz y administración	Considera la experiencia de administración de la herramienta, incluyendo paneles de control, reportes, y otras herramientas de gestión.
Personalización y configuración	Evalúa la flexibilidad de la solución para adaptarse a necesidades específicas, permitiendo configuraciones personalizadas y ajustes según las demandas de la universidad.

	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: SEGURIDAD EN EL CORREO ELECTRÓNICO**
Fecha:	**Octubre 2023**

REQUERIMIENTOS ECONÓMICOS	**FORMA DE EVALUACIÓN**
Costo de la solución	Evalúa el precio total de adquisición o licencia.
Valor agregado - Servicios adicionales	Evalúa el impacto de los valores agregados ofrecidos
Modelo de licenciamiento	Considera la estructura del licenciamiento. ¿Es por usuario? ¿Por volumen? ¿Hay descuentos a medida que se expande la solución?
Costos futuros previstos	Analiza los costos que se espera incurrir en el futuro, ya sea por renovaciones, expansión de licencias, adquisición de características adicionales, entre otros.

REQUERIMIENTOS PROVEEDOR	**FORMA DE EVALUACIÓN**
Equipo propuesto para el proyecto	Considera la estructura que propone el proponente Cantidad de personas de acuerdo a la implementación, despliegue, soporte pre y post proyecto
Metodología y procedimiento de prestación del servicio	Considera la metodología utilizada para el proceso de soporte, gestión, escalamiento de casos, manejo de incidentes, procesos de calidad y articulación de los mismos son claros, estructurados y apoyan la toma de decisiones y gestión de los procesos implícitos en el servicio Garantías y acuerdos de nivel de servicio (SLA).
Historial y estabilidad financiera	Evalúa la solidez financiera del proveedor para garantizar que pueda mantener y ofrecer soporte para sus productos a largo plazo.
Certificaciones y reconocimientos de la industria	Evalúa si el proveedor cuenta con certificaciones, premios o reconocimientos relevantes en el ámbito de seguridad o tecnología.
Referencias y testimonios de clientes	Considera las experiencias previas de otros clientes con el proveedor

	Universidad de San Buenaventura Cali Vicerrectoría Administrativa y Financiera Departamento de Tecnología Gestión de Infraestructura **RFP: SEGURIDAD EN EL CORREO ELECTRÓNICO**
Fecha:	**Octubre 2023**

Instrucciones

La fecha límite de entrega de las propuestas será el **lunes 30 de octubre hasta las 12:00 pm** y se hará a través del sitio web https://ti.usbcali.edu.co

Tener presente que después de esa hora ya no estará disponible la opción de cargue de documentos.

Todas las preguntas o aclaraciones sobre este RFP, pueden hacerlo directamente al correo jefe.infraestructura@usbcali.edu.co con el asunto “RFP: Seguridad en el Correo Electrónico”

Requisitos de la propuesta

1. Por políticas internas de la universidad, se debe realizar un contrato entre las partes, el cual, una vez firmado, se podrá proceder con el proceso de compra.
2. Presentar la propuesta con todos los elementos, bienes y servicios necesarios para la solución, de otro modo no se recibirán propuestas con soluciones parciales.
3. Contemplar los equipos a instalar (si los hay), servicios de instalación, puesta en operación y soporte para la solución.
4. Presentar las hojas de vida y certificaciones con las que cuenta el personal que realizará la instalación, configuración y soporte a la Universidad
5. Presentar las capacitaciones necesarias para su gestión
6. Presentar la propuesta a 1, 2 y 3 años, cronograma y un plan detallado de implementación

7. Indicar los reconocimientos que ha tenido la solución propuesta en el mercado, así como referencias de clientes donde se ha implementado tanto en el mercado nacional como internacional (si es el caso)
8. En la respuesta a esta propuesta deben adjuntar la tabla de si cumplen o no lo solicitado
9. Presentar la propuesta con opción de compra y como servicio, con el soporte incluido y el mantenimiento de la solución durante el tiempo contratado.