

## **ANEXO A1**

### **SUSCRIPCIÓN DE LICENCIA DE SOLUCIÓN DE CIBERASISTENTE INTELIGENTE**

#### **Funcionalidades de la solución de ciberasistente Inteligente**

1. La solución debe ser desplegado en el ambiente virtual de la entidad, donde proporcionará una interfaz para interactuar con los usuarios de TI para la gestión y respuesta ante atenciones de usuarios finales. La solución estará integrada con las plataformas de identidad de la entidad y con la plataforma de integración de herramientas de seguridad digital, donde están embebidas las soluciones de ciberseguridad de la entidad. Además, la solución deberá admitir entrada tanto de texto como de audio. En caso de requerirse se podrá realizar el desarrollo de los componentes que sean necesarios para cumplir con lo solicitado.
2. Debe estar licenciada por un periodo de mil noventa y cinco (1095) días calendario, a partir del día siguiente de emitida la conformidad de la prestación principal.

#### **3. Requisitos Funcionales:**

##### **a. Interfaz de Usuario:**

- La solución debe proporcionar una interfaz intuitiva para que los usuarios de TI puedan interactuar con él.
- La interfaz debe admitir entrada de texto y de voz para la comodidad del usuario.
- La interfaz de usuario deberá permitir un número ilimitado de interacciones sin costos adicionales y estar preparada para su publicación en plataformas públicas como Android e iOS. Los componentes internos deberán garantizar una capacidad mínima de 250 mil casos anuales, considerando que cada caso puede incluir múltiples flujos de entrada y salida necesarios para su adecuada resolución. Deberá ser capaz de manejar un volumen aproximado de 90 millones de intentos de intrusión mensuales provenientes de diversas amenazas. Para gestionar estos casos y consolidar respuestas precisas, se integrará un componente de IA generativa tipo dentro del asistente, que permitirá analizar y brindar un resumen para la respuesta mediante un protocolo estándar.
- La interfaz de usuario deberá contener componentes como mínimo para los siguientes Sistemas Operativos como mínimo Windows, Linux, Mac, Android, iOS

##### **b. Integración con Plataformas de Identidad:**

- La solución debe integrarse con las plataformas de identidad de la entidad (componente del Directorio Activo y Componente MFA (multifactor)) para acceder a la información de usuarios y garantizar la seguridad en las interacciones. Se debe usar protocolos estándar de autenticación, tales como LDAP para la integración con el Directorio Activo, y SAML o OAuth 2.0 para la implementación de Single Sign-On (SSO) y autenticación federada. Además, para la autenticación multifactor (MFA), se deben considerar protocolos como RADIUS y TOTP, o equivalentes.

##### **c. Integración con Plataforma de integración de herramientas de seguridad digital:**

- Debe ser capaz de integrarse con la plataforma de seguridad digital de la entidad mediante API's de integración y ejecución de tareas autorizadas.
- Debe proveer un componente onpremise o nube privada dedicada para la ejecución de actividades relacionada a la IA. Este componente podrá ser entregado como maquina virtual en un formato estándar. La entidad proporcionará el espacio para alojarlo.
- Debe integrarse a componentes de IA de terceros mediante opciones de selección para su derivación.
- Debe tener la capacidad de aprender a partir de grandes volúmenes de datos utilizando técnicas de aprendizaje profundo, como redes neuronales.
- Debe permitir realizar la creación de contenido nuevo solicitado durante la interacción con el usuario.
- Debe tener la capacidad de combinar elementos conceptualizados mediante la interacción con el usuario.
- Debe poder interactuar de manera natural con los usuarios, comprendiendo y respondiendo preguntas, y generando conversaciones coherentes.
- Debe ser capaz de adaptar sus respuestas o creaciones según las preferencias y necesidades del usuario.
- Debe poder realizar múltiples tareas generativas.
- Debe poder imitar estilos específicos de escritura, basándose en ejemplos proporcionados.
- Debe ser capaz de ser entrenada o afinada para mejorar en tareas específicas o adaptarse a nuevos dominios de conocimiento.
- Debe poder operar en diferentes escalas, desde generar pequeñas piezas de contenido hasta manejar grandes volúmenes de creación en tiempo real.
- Debe utilizar técnicas de retroalimentación para mejorar su rendimiento con el tiempo.
- Debe estar diseñada con consideraciones éticas y mecanismos de control para evitar la generación de contenido inapropiado, dañino o sesgado.

**d. Gestión de Atenciones de Usuarios Finales:**

- La solución debe ser capaz de gestionar y responder a las atenciones de tres mil (3000) usuarios finales de manera eficiente y oportuna.
- La solución debe ser capaz de gestionar mediante un componente de atenciones sobre las solicitudes realizadas.
- La solución debe ser capaz de verificar los estados de los requerimientos y responder basados en ellos.

**e. Análisis de Lenguaje Natural:**

- Debe contar con capacidades avanzadas de procesamiento de lenguaje natural para comprender y responder de manera inteligente a las consultas de los usuarios.

**f. Seguridad y Privacidad:**

- Seguridad y Privacidad: La solución debe cumplir con normas, estándares y buenas prácticas de seguridad ampliamente conocidas, para proteger la información confidencial de los usuarios y de la entidad. Los componentes deben contar con sus propios certificados digitales.

**g. Disponibilidad:**

- La solución inteligente debe estar disponible las 24 horas del día, los 7 días de la semana, para atender las necesidades de los usuarios en cualquier momento.

**h. Escalabilidad:**

- La solución debe ser capaz de escalar automáticamente para manejar un aumento repentino en la carga de trabajo sin afectar el rendimiento.

**i. Fiabilidad:**

- De contar con una alta fiabilidad de la solución para garantizar que las interacciones con los usuarios sean consistentes y libres de errores.

**j. Compatibilidad con Múltiples Plataformas:**

- Compatibilidad con Múltiples Plataformas. La solución debe ser compatible con una variedad de dispositivos y plataformas, incluyendo dispositivos móviles, computadoras de escritorio y dispositivos de voz. Esta compatibilidad podrá ser provista mediante componentes de software como aplicación e integraciones respectivas.

**4. Arquitectura Técnica:**

**a. Componente Cloud:**

- La solución será desplegada en una plataforma de nube como ejemplo AWS, Azure o Google Cloud Platform para garantizar la escalabilidad y disponibilidad.

**b. Servicios de Identidad:**

- Se deberá de integrar con los servicios de identidad de la entidad utilizando protocolos estándar como OAuth para la autenticación y autorización.

**c. Integración:**

- Se deberán establecer conexiones API con la plataforma de automatización de respuestas de seguridad para la comunicación bidireccional y la ejecución de acciones de seguridad. Es importante precisar que para el caso de la plataforma de respuesta será la encargada de realizar las acciones de seguridad, mientras que el API de integración se utilizará para realizar el llamado e interactuar con las solicitudes

**d. Procesamiento de Lenguaje Natural:**

- Se deberán utilizar modelos de procesamiento de lenguaje natural avanzados, posiblemente basados en redes neuronales, para comprender y generar respuestas inteligentes.

**e. Seguridad:**

- Se deberán implementar medidas de seguridad como encriptación de datos, autenticación de usuarios y auditoría de acceso para proteger la confidencialidad e integridad de la información.

**5. Integraciones Adicionales:**

**a. Plataformas de Mensajería Instantánea:**

- Debe poder integrarse con plataformas de mensajería instantánea como ejemplo Slack, Microsoft Teams o WhatsApp para facilitar la comunicación con los usuarios.

**b. Plataformas de Correo Electrónico:**

- Debe poder integrarse con plataformas de correo electrónico como ejemplo Outlook, Office 365 o Gmail para permitir la gestión de solicitudes de soporte a través de correo electrónico.