REPÚBLICA DE PANAMÁ
GOBIERNO NACIONAL

AIG
Autoridad Nacional para la Innovación Gubernamental

CONSULTA AL MERCADO (CAM)

“Implementación de Identidad Única y Seguridad de los usuarios del Directorio Activo de la Autoridad Nacional para la Innovación Gubernamental”

Contenido

1. PERÍODO DE PREGUNTAS Y ACLARACIONES SOBRE REQUERIMIENTOS DE LA CAM

Publicado el documento de CAM (Consulta al Mercado), a través del Sistema Electrónico de Contrataciones Públicas "PanamaCompra", los interesados podrán solicitar aclaraciones o realizar preguntas sobre el contenido o la información requerida en este documento, mediante correo electrónico: consultasmercado@aig.gob.pa, dirigido al Departamento de Compras de la Dirección de Administración y Finanzas de la Autoridad Nacional para la Innovación Gubernamental. El remitente del correo debe colocar en el sujeto del mensaje: "**Aclaraciones CAM: Iniciativa 2021087**".

Queda a criterio de esta entidad, dar respuesta a las preguntas que se reciban posterior a la fecha límite para la recepción de consultas de los interesados. Para tal fin, se establece el siguiente calendario:

Actividad	**Fecha**	**Hora**
Publicación de la CAM	19 de febrero de 2021	2:00 p.m.
Límite para la recepción de consultas a la CAM	4 de marzo de 2021	2:00 p.m.
Entrega de la documentación requerida por AIG a través del presente CAM. E-mail: consultasmercado@aig.gob.pa	5 de marzo de 2021	

2. PERFIL DE LAS EMPRESAS CONSUTADAS A TRAVES DE LA CAM

Esta CAM está dirigida a las empresas dedicadas a implementar soluciones con las características definidas en este documento, en el sector público y/o privado, y con experiencia en proveer servicios de implementación, soporte funcional (mantenimiento preventivo y correctivo, cambios y mejoras) y consultoría en Microsoft 365.

Podrán dar respuesta a esta CAM, las empresas debidamente constituidas para el ejercicio de la actividad comercial que puedan brindar el servicio, a través de su estructura empresarial o mediante Consorcio, y que se encuentren jurídicamente habilitadas para ser proveedores del Estado panameño.

Se espera que las empresas provean información sobre su constitución, conocimiento y experiencia. En ese sentido, los interesados deberán proporcionar la información sobre los datos de:

- Registro social y comercial de la empresa de su país de origen
- Nombre de su representante legal o apoderado
- Domicilio comercial
- Fecha o años de certificación como socio de Microsoft
- Los clientes previos donde hayan brindado implementado las soluciones definidas en este documento

- Brindar información que permita conocer la capacidad para desarrollar y cumplir con los servicios requeridos en la sección 7 (CUADRO DE EXPERIENCIA) de este documento.

La información que proporcione los interesados a la Autoridad Nacional para la Innovación Gubernamental, deberá ser veraz y alineada a los procedimientos que rige Microsoft, en aras de garantizar el principio de igualdad entre los posibles interesados para una mayor participación de proveedores y que cumpla con el objeto de la consulta.

3. COMUNICACIONES

Las comunicaciones o correspondencias con motivo del Periodo de Preguntas y Aclaraciones a la CAM, se realizarán a través del correo electrónico: consultasmercado@aig.gob.pa.

El remitente del correo debe colocar en el sujeto del mensaje: "**Respuesta CAM: Iniciativa 2021087**".

Las empresas (INTERESADOS) que respondan a esta Consulta al Mercado (CAM) deben proporcionar sus respuestas a las preguntas contenidas en el cuestionario que se presenta en la sección 8 (CUESTIONARIO DE SOLICITUD DE INFORMACION).

3.1. FECHA Y LUGAR DE RECEPECIÓN DE LAS RESPUESTAS A LA CAM

La Autoridad Nacional para la Innovación Gubernamental, recibirá las respuestas a la presente Consulta al Mercado (CAM) hasta el **día viernes 5 de marzo 2021 a las 05:00 p.m**.

Las empresas interesadas (INTERESADOS) podrán remitir su respuesta a la presente CAM a la dirección de correo electrónico: consultasmercado@aig.gob.pa. En el sujeto del correo debe decir: "**Atención Respuesta a CAM: Iniciativa 2021087**". Favor tener presente que el tamaño de los archivos digitales no debe superar los 25 MB.

A raíz de la pandemia ocasionada por el virus SAR-CoV-2 (COVID-19), como medida de prevención sanitaría, **no se estarán recibiendo documentos en respuestas a esta CAM de forma presencial en nuestras oficinas**.

3.2. CAM NO ES UN PROCESO FORMAL DE LICITACIÓN

Esta CAM se expide para efectos de la recopilación de información y **no pretende ser un proceso formal de licitación**. Sin limitar la generalidad de lo anterior, esta CAM no necesariamente dará lugar a una negociación subsiguiente, a una adjudicación directa, un proceso de licitación por invitación o el proceso de licitación abierto y no constituye un compromiso por parte de la Autoridad Nacional para la Innovación Gubernamental para adquirir algún bien o servicio. Todas las cifras de precios presentados por los interesados se destinarán a fines de información general y no será vinculante para las empresas privadas interesadas en responder a esta consulta al mercado.

3.3. EL DOCUMENTO CAM NO LIMITARÁ LOS DERECHOS DE LA AIG

Esta CAM no limitará los derechos de la Autoridad Nacional para la Innovación Gubernamental. Sin limitar la generalidad de lo anterior, la AIG se reserva expresamente el derecho, a su discreción:

A. Para buscar o solicitar información posteriormente

B. Para contactar a los interesados y/o fabricantes, y solicitar que se amplíe o aclare la información provista por ellos.

Estos derechos reservados expresados son en adición a cualquiera y todos los demás derechos de la Autoridad Nacional para la Innovación Gubernamental que existan antes de la emisión de esta CAM.

3.4. IDIOMA

La información que presenten los interesados en respuesta a esta CAM, así como toda la correspondencia o documentos relativos a éste, deben estar en el idioma español o traducirlo en este idioma, en caso de aplicar.

4. CONFIDENCIALIDAD

Toda la información proporcionada a la Autoridad Nacional para la Innovación Gubernamental, en cualquier forma, en relación con esta Consulta al Mercado, ya sea antes o después de la emisión de esta Consulta al Mercado: (a) es propiedad exclusiva de la AIG y **debe ser tratada como confidencial**, (b) no debe ser utilizada para cualquier otro propósito que no corresponda a esta Consulta al Mercado, y (c) serán devueltos por la AIG a los interesados cuando este último así lo solicite formalmente.

Los interesados no pueden, en ningún momento, directa o indirectamente, hacer uso indebido de esta información o aclaración que realice la Entidad Solicitante sin haber obtenido la autorización por escrito de la Autoridad Nacional para la Innovación Gubernamental. Está prohibido hacer un uso distinto del material publicado en la SDI o aclarado, salvo que la AIG otorgue autorización para un uso diferente y previa petición del interesado.

5. DESCRIPCIÓN GENERAL

La Autoridad Nacional para la Innovación Gubernamental (AIG) desde el año 2020, ha iniciado un proceso de modernización para proteger la identidad de los servidores públicos que laboran dentro de la Institución.

La identidad de todo funcionario inicia con el registro de un perfil dentro del Directorio Activo Institucional (Active Directory o AD), y esto le brinda los permisos de acceso a los recursos Institucionales disponibles dentro de la AIG (por ejemplo, le permite autenticarse al Gestor Documental).

Con el cambio de administración en el año 2019, la Dirección Nacional de Tecnología identificó la existencia de puntos de mejoras relacionadas a:

- Los métodos de autenticación del funcionario al momento de validarse al Dominio (Domain) del AD
- El control de acceso condicionado
- Trazabilidad de las acciones por parte de los usuarios autenticados al Dominio
- La protección de los dispositivos finales (endpoints) de la AIG
- Licenciamiento de herramientas ofimáticas en su versión más reciente
- La disponibilidad de herramientas colaborativas que permitieran trabajar de forma sincronizadas con otras personas (ya sean servidores públicos de la AIG o entes externos

a la Institución) de forma remota, así como tener la posibilidad de coordinar reuniones virtuales

A raíz de la pandemia ocasionada por el virus SARS-CoV2 (COVID-19), la AIG adoptó formalmente, en el mes de septiembre de 2020, las soluciones/aplicaciones incluidas en el licenciamiento E1 de Office 365, con la intención de solventar (de manera temporal) la necesidad de contar con aquellas herramientas colaborativas indicadas en el último punto listado anteriormente. Es importante resaltar que esta estrategia de licenciamiento vigente es transitoria. El objetivo final involucra otro esquema de licenciamiento con el fabricante, que cubra las necesidades de:

- Mantener vigente el derecho a actualizar a la versión más reciente del sistema operativo Windows 10 Enterprise (Windows es el sistema operativo por defecto de las estaciones de trabajo de la Institución).
- Contar con el derecho a descargar y actualizar la versión más reciente de las herramientas ofimática existente dentro de la Institución, para todos los equipos disponibles en el inventario de estaciones de trabajo de la AIG.
- Cubrir el licenciamiento para algunos servidores públicos que utilizan las herramientas de Inteligencia de Negocio (PowerBI). Estas licencias se renuevan anualmente a través de un proceso independiente de compra.
- Contar con el derecho a proteger las estaciones de trabajo con las soluciones de anti-virus y anti-malware que corren de forma nativa dentro del sistema operativo Windows Enterprise.
- Contar con una herramienta que permita controlar y asegurar los dispositivos móviles propiedad del Estado (laptops, teléfonos inteligentes, tabletas) dentro del perímetro de la Institución y fuera del mismo.
- Contar con una herramienta que permita controlar y asegurar los datos e información pertenecientes a la AIG que reposen en los dispositivos móviles personales o de propiedad del Estado (laptops, teléfonos inteligentes, tabletas).
- Contar con el derecho a implementar autenticación multifactor (MFA), acceso condicional, así como también la posibilidad de utilizar métodos de autenticación sin-contraseña (passwordless).
- Contar con una protección contra amenazas avanzadas, para detectar posibles ataques que atenten contra la seguridad informática de los servidores públicos de la AIG.

6. ALCANCE DE LA INICIATIVA

El alcance de la iniciativa abarca los siguientes puntos:

1. **ALCANCE 1**: contratar el licenciamiento de Microsoft 365 para los funcionarios de la AIG.

   Para la ejecución de este proyecto, se requieren un total de doscientas cincuenta (250) licencias Microsoft 365, las cuales se clasifican de la siguiente forma:

SKU	Licencias requeridas	Cantidad
T6A-00024	O365E1	25
AAA-12414	Core CAL Bridge para cada usuario Office 365	25
AAD-33168	M365 E5	15
AAD-33204	M365 E3	210
PEJ-00002	M365E5Security (paquete de seguridad para E3)	210

El esquema de contratación debe ser Enterprise Agreement Subscription (EAS) de Microsoft, bajo una concesión a un (1) año.

Se requiere un total de doscientas cincuenta (250) licencias ya que es el límite mínimo por parte del fabricante para adquirir un licenciamiento en base a un contrato EAS. Las licencias deben arrancar su vigencia a partir del 1 de junio de 2021.

El esquema de licenciamiento solicitado está contemplado para cubrir:

- Doscientos veinticinco (225) funcionarios de la Institución que requieren utilizar las características del licenciamiento Microsoft 365. Quince (15) licencias de este grupo serán asignadas a los usuarios que actualmente poseen licencia de PowerBI.
- Veinticinco (25) funcionarios o personal externo (posible colaboración con otras Instituciones Gubernamentales) que, por la naturaleza de sus funciones, no requieran todas las características incluidas en el licenciamiento de Microsoft 365. En este escenario se aplicaría licenciamiento E1 de Office 365.

2. **ALCANCE 2:** contratar los servicios profesionales que permitan integrar (sincronizar) la identidad existente en premisa (AD On-Premise) y en nube (Azure AD).

   Con la implementación de los servicios de Office 365 en el mes de septiembre del año 2020, se creó un dominio en Azure AD, que no guarda relación con el dominio que se encuentra configurado en el AD en premisa.

   Debido a esto, los servidores públicos de la AIG requieren una credencial para acceder a los servicios de Office 365, la cual difiere de la credencial que utilizan para validarse al Dominio del Directorio Activo en premisa.

   Se requiere que exista una única identidad que le permita al servidor público validarse con una sola credencial en ambos servicios, sin afectar los datos ya existentes en nuestro inquilino (tenant) en Office 365.

3. **ALCANCE 3**: contratar los servicios profesionales que permitan implementar métodos de autenticación multifactor (MFA) y sin-contraseña (passwordless), una vez la identidad de los usuarios del Directorio Activo haya sido unificada.

   El objetivo principal es habilitar los medios para que los servidores públicos de la AIG puedan auto-gestionar el desbloqueo de su usuario del Dominio o el cambio de las credenciales de acceso, de manera segura, con la intención de reducir el tiempo de respuesta por parte de la Mesa de Servicio para atender este tipo de solicitudes.

   De igual forma, se requieren establecer los métodos de autenticación multifactor (MFA) y sin contraseña (passwordless), como puede ser el uso de llaves FIDO2 (*Fast Identity Online*) para este último.

   El uso de autenticación multifactor (MFA) será un método para proteger los recursos que la AIG considere como privados, a través de la implementación de acceso condicionado (conditional access).

4. **ALCANCE 4**: contratar los servicios profesionales que permitan habilitar algunas de las funciones de Microsoft Defender for Identity (anteriormente conocido como Azure ATP-Advanced Threat Protection), para la protección de la identidad de los usuarios del Dominio contra amenazas avanzadas, las cuales están incluidas en el esquema de licenciamiento de Microsoft 365.

Microsoft Defender for Identity brinda una gama de funciones que ayudan a proteger la identidad de los usuarios en ambientes alojados en premisa y nube. Por lo cual, se requiere habilitar funciones que permitan al equipo operativo de la Dirección Nacional de Tecnología a prevenir, detectar, investigar y responder ante posibles amenazas a la identidad de nuestros funcionarios.

Con esta implementación, la AIG busca atender:

Ámbito	**La AIG requiere:**
Prevenir	• Determinar las fuentes de vulnerabilidad que pueden ser explotadas, con el objetivo de mitigar riesgos de seguridad informática que puedan estar asociadas a malas configuraciones. • Tener visibilidad de riesgos potenciales asociado a la identidad de los usuarios del Dominio. • Visualizar las aplicaciones que, dentro de un ranking, tienen más exposición de ser vulneradas, de acuerdo a un criterio establecido de seguridad (por ejemplo, la exposición de sus credenciales sin ningún tipo de cifrado). • Descubrir cuentas inactivas o expiradas que pertenecen a grupos sensibles. • Analizar las acciones recomendadas a través del Puntaje de Seguridad (Secure Score) de Microsoft. • Habilitar parámetros para detectar y evitar el uso de contraseñas débiles (Password Protection)
Detectar	• El habilitar el sensor de Microsoft Defender Identity para inspeccionar el tráfico de red en tiempo real (NTLM, Kerberos, LDAP, RPC, DNS, SMB) • Inspeccionar eventos, dar trazabilidad a estos, y a las actividades de aquellas entidades que pertenecen al Directorio Activo. • Analizar el comportamiento de los usuarios en el Directorio Activo y determinar anomalías. • Clasificar las alertas de detección para que, dependiendo del puntaje o grado de severidad/importancia, sean escaladas para su atención a la Dirección Nacional de Tecnología de la AIG. Algunas alertas comunes pueden ser: o Autenticación por un medio u horario no habitual o Autenticación desde una dirección IP anónima o Una conexión sospechosa vía VPN o Filtración de datos del Controlador de Dominio o Acceso anómalo para proteger data o Elevación de privilegios o Credenciales (usuario y contraseña) filtradas en la red oscura (dark web)
Investigar	• Medir el grado de posible riesgo que pueda tener un usuario del Dominio, en base al puntaje obtenido en su perfil de investigación (investigation priority score) • Correlacionar las actividades que pueden estar ocurriendo a nivel de Office 365, el Directorio Activo (en-premisa y Azure) y Sistema Operativo Windows, para

	definir posibles eventos de seguridad que se estén desarrollando y deban ser investigado. Estos eventos deben de estar presenten en la cola de incidentes (Incident Queue).
Responder	• Aplicar automáticamente políticas a los usuarios al momento que se determine un riesgo elevado en la seguridad de la Identidad del Dominio.

5. **ALCANCE 5**: contratar los servicios profesionales que permitan habilitar las funciones de Microsoft Endpoint Manager (que utiliza los servicios de Microsoft Intune), para la administración y control de dispositivos móviles Institucionales y personales, las cuales están incluidas en el esquema de licenciamiento de Microsoft 365.

   Microsoft Intune es un servicio en Nube que se encarga de la administración de dispositivos móviles (MDM, *mobile device management*) y la administración de aplicaciones móviles (MAM, *mobile application management*). Se desea controlar la manera como se utilizan los dispositivos Institucionales (teléfonos móviles, tabletas y portátiles) a través de la configuración de políticas específicas para administración de las aplicaciones (por ejemplo, evitar que se envíen correos electrónicos a personas ajenas a nuestra Institución). Con Intune, la AIG desea permitir el uso de dispositivos personales (no Institucionales), pero con los controles que garanticen que los datos de la Institución permanezcan protegidos y aislados de los datos personales del individuo.

   Con esta implementación, la AIG busca atender:

Ámbito	**La AIG requiere:**

Gestión de dispositivos móviles (MDM)	• En el caso de los dispositivos propiedad de la AIG, se desee tener un control total de su configuración, funciones y los parámetros de seguridad.
	  ○ Para los dispositivos registrados, deben recibir las reglas y configuraciones a través de las políticas establecidas en Intune (por ejemplo, puede establecer un requerimiento de contraseña y PIN).
	• En el caso de los dispositivos personales (BYOD, *bring your own device*), se necesita contar con opciones que no sean invasivas para el usuario/funcionario público, pero que proteja los datos Institucionales.
	  ○ El usuario o funcionario público inscribe su dispositivo si desean tener acceso completo a los recursos de la Institución (por ejemplo, se requiere autenticación multifactor (MFA) para usar las aplicaciones de correo electrónico o Microsoft Teams).
	• Eliminar los datos Institucionales si un dispositivo se pierde, es robado o ya no esté en uso.
	• Ver los dispositivos registrados y obtener un inventario de aquellos dispositivos que acceden a los recursos de la Institución.
	• Configurar los dispositivos para que cumplan con los estándares de seguridad y salud definidos por la AIG (por ejemplo, bloquear dispositivos con jailbreak).

	• Enviar certificados a los dispositivos para que los usuarios o funcionarios puedan acceder fácilmente a la red Wi-Fi de la AIG o utilice una VPN para conectarse la red Institucional. • Generar informes sobre usuarios y dispositivos que estén en cumplimiento de las políticas establecidas de control.
Gestión de aplicaciones móviles (MAM)	• Integrarlo con la protección de identidad de Azure AD para aislar los datos de la organización de los datos personales. Los datos a los que se accede mediante credenciales de la Institución reciben protección de seguridad adicional. • Poder habilitar la restricción de acciones, como copiar y pegar, guardar y ver, en los dispositivos personales cuando se trate de aplicaciones Institucionales. • Agregar y asignar aplicaciones móviles a grupos de usuarios y dispositivos. • Configurar las aplicaciones para que se ejecuten con configuraciones específicas. • Actualizar las aplicaciones existentes que ya están en el dispositivo. • Generar informes sobre las aplicaciones se utilizan y hacer un seguimiento de su uso. • Realizar una limpieza selectiva, que permita eliminar solo los datos de la Institución de las aplicaciones.

6. **<u>ALCANCE 6</u>**: contratar los servicios profesionales que permitan habilitar algunas de las funciones de Microsoft Defender para Dispositivos Finales (anteriormente conocido como Defender ATP-Advanced Threat Protection), para la protección de los dispositivos finales (endpoints) contra amenazas avanzadas, las cuales están incluidas en el esquema de licenciamiento de Microsoft 365.

   Defender es más que una solución de antivirus o antimalware, es una protección de próxima generación (next-gen) para los dispositivos finales (estaciones de trabajo de escritorio y laptops), que ayuda a los equipos de operaciones de seguridad (SecOps) a administrar las amenazas y vulnerabilidades que atenten contra la salud e integridad del activo informático de la Institución.

   Lo que se busca explotar con las funciones de Microsoft Defender es:

Ámbito	**La AIG requiere:**
Gestión de amenazas y vulnerabilidades	Contar con la capacidad de descubrir, priorizar y corregir vulnerabilidades y configuraciones incorrectas de los dispositivos finales de la Institución.
Reducción de la superficie de ataque	Como Defender no se base en firmas, se busca utilizar la inteligencia que genera el poder en nube para proteger el activo informático contra amenazas que atenten contra la integridad de los archivos del dispositivo (por ejemplo, ransomware) También se requiere: • Restringir el tráfico a destinos con baja

	reputación • Mitigación de exploit • Prevención de intromisión a un equipo (host) • Aislar el acceso a sitios o archivos que no sean confiables
Protección de próxima generación	• Contar con una herramienta de análisis que siempre esté activa, mediante la supervisión del comportamiento de los archivos y procesos y protección en tiempo real. • Detectar y bloquear aplicaciones que se consideran inseguras (y pasen desapercibidas no se detecten como malware). • Protección en la nube, para la detección y bloqueo casi instantáneo de amenazas nuevas y emergentes.
Detección y respuesta de endpoints (EDR)	• Cuando se detecta una amenaza, se deben crear alertas en el sistema para que un analista de la AIG las investigue. • Las alertas con las mismas técnicas de ataque o atribuidas al mismo atacante se agregan un incidente. • Recopilar continuamente ciber-telemetría de comportamiento (información de proceso, actividades de red, óptica profunda en el kernel y administrador de memoria, actividades de inicio de sesión de usuario, cambios en el registro y el sistema de archivos). • Almacenar la información recolectada durante seis meses, para que un analista de AIG pueda trabajar desde un punto definido en el tiempo hasta el inicio del ataque. • Abordar una investigación a través de múltiples vectores.
Investigación y remediación automatizadas	• Recibir alertas y registrar una incidencia cada vez que se detecta un comportamiento sospechoso o malicioso para iniciar una investigación automatizada. • Permitir que el equipo de operaciones de AIG pueda iniciar manualmente una investigación automatizada (por ejemplo, el operador identifica que un dispositivo tiene un alto nivel de riesgo y luego seleccionar Iniciar investigación automatizada). • Generar un “veredicto” (*malicioso, sospechoso o no se encontraron*

	amenazas) para cada evidencia investigada. • Tomar de acciones de reparación (enviar un archivo a cuarentena, detener un servicio, eliminar una tarea programada, entre otras) a medida que se alcanzan los veredictos. • Poder ejecutar acciones de corrección automáticamente o con la aprobación de un personal de AIG, dependiendo del nivel de automatización establecido, así como de otras configuraciones de seguridad.
Puntuación segura de Microsoft para dispositivos	• Visualizar, en el panel de administración de amenazas y vulnerabilidades del Centro de seguridad de Microsoft Defender, la puntuación de seguridad para dispositivos de la AIG. • Reflejar el estado de configuración de la seguridad colectiva de los dispositivos Institucionales en base a las categorías: aplicación, sistema operativo, red, cuentas, controles de seguridad. • En base a la puntuación obtenida de un análisis inicial, establecer un objetivo para mejorar en la escala de puntos de cada uno de las categorías.
Asesoría de Expertos en Amenazas de Microsoft	Poder interactuar con los expertos en seguridad en Microsoft directamente desde Microsoft Defender Security Center para una respuesta oportuna y precisa.

7. **ALCANCE 7**: contratar los servicios gestionados para la administración de los servicios activos de Microsoft 365.

La información relacionada a las versiones de los sistemas operativos de nuestros Controladores de Dominios (Domain Controllers), Directorio Activo, nombre de los Dominios configurados en premisa (on-premise) y en nube (Azure AD), información relacionada a las marcas y versiones de sistemas operativos de nuestros equipos finales (endpoints), el nivel que cuenta la AIG en base al modelo de Madurez en la Gestión de Vulnerabilidades, entre otras, **es considerada como confidencial y será entregada aquellas empresas interesadas en participar en esta Consulta al Mercado a través de un vía controlada**.

Los interesados deben hacer una solicitud formal para la entrega de esta información a través del correo electrónico: consultasmercado@aig.gob.pa. El remitente del correo debe colocar en el sujeto del mensaje: "**Información CAM: Iniciativa 2021087**".

Para esta solicitud formal aplicará las mismas normas establecidas en la sección 4 (CONFIDENCIALIDAD).

7. CUADRO DE EXPERIENCIA

Con el objetivo de conocer la experiencia del interesado en el alcance de la presente CAM, específicamente en la prestación de los servicios profesionales de implementación y adopción de las funciones incluidas en Microsoft 365, y en particular, la integración (sincronización) de identidades independientes de los Dominios Activos (Active Directory), se deberá listar la información general de servicios previamente brindados. Para tal fin, se presenta el cuadro que contiene la información mínima que la Autoridad Nacional para la Innovación Gubernamental desea conocer, en esta etapa del proceso.

ID	Empresa	Proyecto	Descripción	Fechas	Contacto
1	Compañía ABC	Proyecto ABC	Migración Office 365	Mayo 2019 a julio 2020	Nombre. E-mail/Teléfono
2	Ministerio ABZ	Proyecto ABZ	Implementación de Microsoft Defender	Diciembre 2019 a abril 2020	Nombre. E-mail/Teléfono

8. CUESTIONARIO DE SOLICITUD DE INFORMACION

Favor de responder a las siguientes preguntas:

1. Información de la Empresa	
Pregunta	**Respuesta**
1.1. Nombre legal de la empresa y cualquier otro nombre que se use para acarrear actividades comerciales	
1.2. Datos del registro social y comercial de la empresa (lugar escrituras públicas, aviso o permiso de operación, etc.)	
1.3. Nombre de su Representante Legal o Apoderado	
1.4. Fecha o años de certificación como proveedor o socio de Microsoft. Se recomienda aportar copia de la misma.	
1.5. Dirección comercial y número de teléfono.	
1.6. Nombre, cargo y dirección e-mail de dos contactos.	
2. Sobre licenciamiento de Microsoft 365	
Pregunta	**Respuesta**
2.1. ¿El licenciamiento solicitado por la AIG se considera un servicio (SaaS) o licencia? Explique su respuesta.	
2.2. En base a la pregunta anterior, ¿el licenciamiento solicitado tiene un cargo por ITBMS?	
2.3. ¿Existe un beneficio considerable en contratar estas licencias bajo un EAS (Enterprise Agreement Subscription) en comparación a un CSP (Cloud Service Provider)?	
2.4. ¿Las licencias E1 de Office 365 pueden ser escaladas (*upgraded*) a Microsoft 365 E3 o E5 en cualquier momento?	

2.5. En caso que la respuesta 2.4. sea afirmativa, ¿se reconoce el costo de las licencias al momento de escalar hacia una versión de Microsoft 365 E3 o E5? Favor explicar su respuesta.	
3. Servicios profesionales para integrar (sincronizar) las identidades existentes	
Pregunta	**Respuesta**
3.1. ¿Por qué usted considera que su empresa está capacitada para proveer el servicio de integración (sincronización) de la identidad existente en premisa (AD On-Premise) y en nube (Azure AD)?	
3.2. En base a la información presentada, ¿Cuál es el nivel de complejidad técnica para realizar el servicio solicitado? Favor sustentar su respuesta.	
3.3. Favor detallar en un cronograma las macro-tareas o hitos más relevantes para realizar el servicio solicitado.	
3.4. ¿Cuál es el tiempo estimado para realizar el servicio solicitado?	
3.5. ¿Qué número de recursos (personal) considera que son necesarios para realizar el servicio solicitado?	
3.6. En base a la pregunta 3.5, se solicita detallar las competencias que debe poseer (experiencia y certificaciones) el personal. Presentar esta información en una tabla con los valores: certificación, experiencia (en años) y número de recursos.	
3.7. Proporcione su oferta de negocio que sean relevantes a las exigencias de la Autoridad Nacional para la Innovación Gubernamental.	
4. Servicios profesionales para implementar métodos de autenticación multifactor (MFA) y sin-contraseña (passwordless)	
Pregunta	**Respuesta**
4.1. Liste al menos dos (2) métodos MFA recomendados para ser habilitados en un ambiente de trabajo corporativo (considerando la seguridad y comportamiento típico de los usuarios finales).	
4.2. ¿Ha implementado métodos de autenticación *passwordless*? De ser así, brinde más información sobre las recomendaciones para su implementación y adopción por parte de los usuarios finales.	
4.3. Mencione recomendaciones que debemos considerar al momento de habilitar herramientas y procedimientos que permitan al funcionario de la AIG auto-gestionar el cambio de contraseña o desbloqueo de su usuario en el Directorio Activo.	
4.4. Mencione otras recomendaciones	

relevantes, relacionadas al punto 4 de la sección del cuestionario.	
4.5. En base a la información presentada, ¿Cuál es el nivel de complejidad técnica para realizar el servicio solicitado? Favor sustentar su respuesta.	
4.6. Favor detallar en un cronograma las macro-tareas o hitos más relevantes para realizar el servicio solicitado.	
4.7. ¿Cuál es el tiempo estimado para realizar el servicio solicitado?	
4.8. ¿Qué número de recursos (personal) considera que son necesarios para realizar el servicio solicitado?	
4.9. En base a la pregunta 4.8, se solicita detallar las competencias que debe poseer (experiencia y certificaciones) el personal. Presentar esta información en una tabla con los valores: certificación, experiencia (en años) y número de recursos.	
4.10. ¿Por qué usted considera que su empresa está capacitada para proveer el servicio solicitado en esta sección?	
4.11. Proporcione su oferta de negocio que sean relevantes a las exigencias de la Autoridad Nacional para la Innovación Gubernamental.	
5. Servicios profesionales para habilitar funciones de Microsoft Defender for Identity	
Pregunta	**Respuesta**
5.1. Por favor liste otras funciones adicionales a los mencionados para Microsoft Defender for Identity que usted considere relevantes y que esté en capacidad de habilitar.	
5.2. En base al *Vulnerability Management Maturity Model*, ¿qué acciones recomienda implementar para una Institución que se encuentra en un nivel 0 (*non-existent*) hacia un nivel 2 (*assessment and compliance*)?.	
5.3. En base a la información presentada, ¿Cuál es el nivel de complejidad técnica para realizar el servicio solicitado? Favor sustentar su respuesta.	
5.4. Favor detallar en un cronograma las macro-tareas o hitos más relevantes para realizar el servicio solicitado.	
5.5. ¿Cuál es el tiempo estimado para realizar el servicio solicitado?	
5.6. ¿Qué número de recursos (personal) considera que son necesarios para realizar el servicio solicitado?	
5.7. En base a la pregunta 5.6, se solicita detallar las competencias que debe poseer (experiencia y certificaciones) el personal. Presentar esta información en una tabla con	

los valores: certificación, experiencia (en años) y número de recursos.	
5.8. ¿Por qué usted considera que su empresa está capacitada para proveer el servicio solicitado en esta sección?	
5.9. Proporcione su oferta de negocio que sean relevantes a las exigencias de la Autoridad Nacional para la Innovación Gubernamental.	
6. Servicios profesionales para habilitar funciones de Microsoft Endpoint Manager (Intune)	
Pregunta	**Respuesta**
6.1. Por favor liste otras funciones adicionales a los mencionados para Microsoft Endpoint Manager (Intune) que usted considere relevantes (especialmente para una Institución que se encuentra en un nivel 0 (*non-existent*) de madurez) y que esté en capacidad de habilitar.	
6.2. En base a la información presentada, ¿Cuál es el nivel de complejidad técnica para realizar el servicio solicitado? Favor sustentar su respuesta.	
6.3. Favor detallar en un cronograma las macro-tareas o hitos más relevantes para realizar el servicio solicitado.	
6.4. ¿Cuál es el tiempo estimado para realizar el servicio solicitado?	
6.5. ¿Qué número de recursos (personal) considera que son necesarios para realizar el servicio solicitado?	
6.6. En base a la pregunta 6.5, se solicita detallar las competencias que debe poseer (experiencia y certificaciones) el personal. Presentar esta información en una tabla con los valores: certificación, experiencia (en años) y número de recursos.	
6.7. ¿Por qué usted considera que su empresa está capacitada para proveer el servicio solicitado en esta sección?	
6.8. Proporcione su oferta de negocio que sean relevantes a las exigencias de la Autoridad Nacional para la Innovación Gubernamental.	
7. Servicios profesionales para habilitar funciones de Microsoft Defender para Dispositivos Finales (Endpoints)	
Respuesta	**Respuesta**
7.1. ¿Las funciones de Microsoft Defender para Endpoints pueden ser implementadas en equipos con MacOS Big Sur, Catalina o Mojave? Explique su respuesta.	
7.2. Por favor liste otras funciones adicionales a los mencionados para Microsoft Defender para Endpoints que usted considere relevantes	

y que esté en capacidad de habilitar.	
7.3. En base al *Vulnerability Management Maturity Model*, ¿qué acciones recomienda implementar para una Institución que se encuentra en un nivel 0 (*non-existent*) hacia un nivel 2 (*assessment and compliance*)?	
7.4. En base a la información presentada, ¿Cuál es el nivel de complejidad técnica para realizar el servicio solicitado? Favor sustentar su respuesta.	
7.5. Favor detallar en un cronograma las macro-tareas o hitos más relevantes para realizar el servicio solicitado.	
7.6. ¿Cuál es el tiempo estimado para realizar el servicio solicitado?	
7.7. ¿Qué número de recursos (personal) considera que son necesarios para realizar el servicio solicitado?	
7.8. En base a la pregunta 7.7, se solicita detallar las competencias que debe poseer (experiencia y certificaciones) el personal. Presentar esta información en una tabla con los valores: certificación, experiencia (en años) y número de recursos.	
7.9. ¿Por qué usted considera que su empresa está capacitada para proveer el servicio solicitado en esta sección?	
7.10. Proporcione su oferta de negocio que sean relevantes a las exigencias de la Autoridad Nacional para la Innovación Gubernamental.	
8. Servicio gestionados para la administración de los servicios activos de Microsoft 365	
Pregunta	**Respuesta**
8.1. Sírvase proporcionar información de cómo prevé brindar el Servicio Gestionado, considerando que se requiere atención 24x7 (para solicitudes e incidencias). Describa su metodología de trabajo y oferta de valor.	
8.2. ¿Qué número de recursos (personal) considera que son necesarios para brindar el servicio solicitado?	
8.3. En base a la pregunta 8.2, se solicita detallar las competencias que debe poseer (experiencia y certificaciones) el personal. Presentar esta información en una tabla con los valores: certificación, experiencia (en años) y número de recursos.	
8.4. ¿Por qué usted considera que su empresa está capacitada para proveer el servicio solicitado en esta sección?	
8.5. Por favor, indique el canon mensual (incluyendo ITBMS) para la contratación de un servicio gestionado.	
9. Otros	

9.1. Por favor indique si su empresa provee el rango completo de servicios profesionales de implementación mencionados en este CAM. De lo contrario, indique qué servicios profesionales está en capacidad de brindar.	
9.2. ¿Su empresa proporciona estos servicios o será usado un subcontratista? Favor especificar.	
9.3. La Autoridad Nacional para la Innovación Gubernamental requerirá entrenamiento para los funcionarios en el uso de las nuevas funciones habilitadas con el cambio hacia Microsoft 365 (en especial al momento de contar con otras opciones de autenticación y manejo de los dispositivos finales). Basado en su experiencia, ¿cuál sería su enfoque recomendado?	
9.4. Además de la información contenida en la presente CAM, ¿qué otra información considera usted relevante que debe ser incorporada en el pliego de cargos, a fin de que los proveedores tengan información suficiente, para la presentación de la propuesta técnica y económica en la siguiente etapa del proceso?	