ANEXO TÉCNICO

SUSCRIPCIÓN DOBLE FACTOR DE AUTENTICACIÓN (MFA) DUO

La Fuerza Aeroespacial Colombiana requiere contratar servicios especializados de seguridad informática bajo la modalidad Software como Servicio (SaaS), orientados al fortalecimiento de los mecanismos de autenticación multifactor (MFA) y de gestión segura de identidad y acceso, mediante la ampliación del licenciamiento de la solución Cisco Duo MFA Essentials Edition actualmente implementada en la institución.

<table>
<tr><th colspan="2">ESPECIFICACIONES TÉCNICAS MÍNIMAS REQUERIDAS</th></tr>
<tr><td>1</td><td>Con el fin de garantizar la continuidad operativa, disponibilidad y fortalecimiento de los mecanismos de autenticación multifactor implementados en la Fuerza Aeroespacial Colombiana, se requiere la ampliación del licenciamiento de la solución Cisco Duo MFA Essentials Edition actualmente desplegada en la Entidad. La presente contratación comprende el suministro, activación y aprovisionamiento de las suscripciones requeridas, así como el soporte técnico, mantenimiento, actualizaciones y demás servicios asociados proporcionados por el fabricante durante la vigencia contratada, con el propósito de asegurar el adecuado funcionamiento de la plataforma de gestión de identidad y acceso.

En atención a lo anterior, se establecen las siguientes especificaciones técnicas y condiciones mínimas requeridas para la prestación del servicio:
<table>
<tr><th>Detalle</th><th>Descripción</th><th>Licencias</th><th>Cantidad AUTORIZADA PPTO</th><th>Periodo de suscripción</th></tr>
<tr><td>Suscripción Cisco Duo Essentials edictión en la modalidad de Enterprise Agreement (EA)</td><td>Solución de autenticación multifactor</td><td>2.352</td><td>2.352</td><td>Doce (12) meses contados a partir de la activación y recibo a satisfacción</td></tr>
</table>
</td></tr>
<tr><td>2</td><td>El contratista deberá prestar un servicio con el personal descrito en el cuadro referenciado al final de esta especificación técnica, durante el periodo de vigencia de la suscripción de la herramienta que incluya:

• Soporte técnico y garantía por parte del fabricante Cisco durante la vigencia de la suscripción, bajo un esquema de atención 7x24 a través de canales remotos o en línea, incluyendo como mínimo acceso al portal de soporte del fabricante, apertura y seguimiento de casos técnicos, actualizaciones y recursos técnicos asociados a la solución Cisco Duo Essentials Edition.
• Los incidentes técnicos podrán ser reportados al contratista mediante portal web, sistema de tickets, correo electrónico o vía telefónica.</td></tr>
</table>

<table>
<tr><td></td><td>

El contratista deberá garantizar la prestación continua de los servicios de soporte técnico, postventa y garantía para la solución ofertada durante toda la vigencia de la suscripción contratada.
El servicio técnico deberá incluir atención de incidentes relacionados con la activación, aprovisionamiento, autenticación de usuarios, enrolamiento de dispositivos, sincronización de directorios, integración con aplicaciones, autenticación multifactor (MFA), Single Sign-On (SSO), Trusted Endpoints y demás funcionalidades.
El servicio técnico deberá contemplar sesiones remotas de acompañamiento técnico cuando sean requeridas por la supervisión del contrato, tanto en horario hábil como no hábil, para actividades y/o novedades relacionadas con la plataforma objeto del contrato.
El contratista deberá realizar la gestión y escalamiento de incidentes ante Cisco cuando la complejidad del caso requiera intervención directa del fabricante, efectuando seguimiento hasta su solución definitiva
El contratista deberá brindar acompañamiento técnico especializado al personal designado por la Dirección de Seguridad Informática y Electrónica (DISIE), orientado al fortalecimiento de las capacidades de administración, operación, gestión de usuarios, aplicación de políticas de seguridad y aprovechamiento de las funcionalidades de la solución Cisco Duo. Este acompañamiento podrá realizarse de manera remota o presencial, según requerimiento de la Entidad, durante la vigencia del contrato y previa coordinación entre las partes. Las actividades se programarán de acuerdo con las necesidades operativas de la Fuerza Aeroespacial Colombiana, en horario laboral institucional.
Todas las actualizaciones, mejoras, correcciones y funcionalidades liberadas por el fabricante e incluidas dentro del licenciamiento contratado deberán encontrarse disponibles para la Fuerza Aeroespacial Colombiana durante la vigencia de la suscripción.
El contratista deberá garantizar la continuidad operativa de las suscripciones suministradas sobre la consola Cisco Duo actualmente utilizada por la Fuerza Aeroespacial Colombiana, preservando las configuraciones, políticas de seguridad, grupos de usuarios e integraciones existentes.

</td></tr>
<tr><td>3</td><td>
Los siguientes son los términos de respuesta del SERVICIO TECNICO.
<table>
<tr><th colspan="2">PRIORIDAD</th><th>DESCRIPCIÓN</th><th>TÉRMINO DE RESPUESTA</th></tr>
<tr><td>1</td><td>CRITICA</td><td>La producción está detenida o severamente impactada de manera que no se puede continuar trabajando. La operación es de misión crítica para la entidad y/o está en situación de emergencia.</td><td>De manera remota o la indicada por el supervisor del contrato (2) horas.</td></tr>
<tr><td>2</td><td>ALTA</td><td>Experimenta perdida del servicio, algunas</td><td>De manera remota o la indicada por el supervisor del contrato (4) horas.</td></tr>
</table>
</td></tr>
</table>

			características importantes no pueden ser utilizadas, sin embargo, la operación continua de manera restringida.	
	3	MEDIA	Experimenta una pérdida de servicio menor, el impacto es un inconveniente.	De manera remota o la indicada por el supervisor del contrato (8) horas.
	4	BAJA	No impacta la operación del programa, no se experimenta perdida del servicio y no se impide la operación de los sistemas.	De manera remota o la indicada por el supervisor del contrato (24) horas.

4	**ALCANCE**
4.1	Ampliación del licenciamiento de la solución Cisco Duo Essentials Edition bajo modalidad Software como Servicio (SaaS), integrada al esquema Enterprise Agreement (EA) actualmente vigente en la Fuerza Aeroespacial Colombiana, con el propósito de fortalecer los mecanismos de autenticación multifactor (MFA), gestión de identidad y control de acceso seguro a los aplicativos institucionales, sistemas de información, plataformas y demás recursos tecnológicos de la Entidad.
5	**LUGAR DE PRESTACIÓN DEL SERVICIO**
5.1	La prestación de los servicios objeto del contrato se realizará inicialmente de manera remota. Cuando las circunstancias técnicas, tecnológicas, operativas o de seguridad así lo requieran, la atención deberá ser prestada de manera presencial en las instalaciones de la Jefatura de Tecnologías de la Información y las Comunicaciones (JETIC), específicamente en la Dirección de Seguridad Informática y Electrónica (DISIE), ubicadas en el Comando Aéreo de Transporte Militar (CATAM), en Bogotá D.C., previa coordinación con el supervisor del contrato.
6	**ESPECIFICACIONES TÉCNICAS DE LOS PRODUCTOS**
6.1	**Especificaciones Generales**
6.1.1	**La solución de autenticación multifactor y gestión de identidad deberá contar como mínimo con las siguientes funcionalidades:** • Autenticación Multifactor (MFA) que permita validar la identidad de los usuarios antes de conceder acceso a los recursos protegidos. • Protección de acceso para aplicaciones locales (On-Premises), aplicaciones en la nube, VPN, servicios y recursos administrados mediante Active Directory. • Capacidades de autenticación resistente a phishing mediante tecnologías de verificación segura de identidad y soporte • Directorio de usuarios basado en la nube (Duo Directory) para administración centralizada de identidades y atributos de usuarios. • Capacidad de integración y sincronización con servicios de directorio como Active Directory, Microsoft Entra ID u otros mecanismos compatibles soportados por el fabricante. • Funcionalidad de Trusted Endpoints para verificar el estado y confianza de los dispositivos antes de autorizar el acceso a los recursos protegidos • Capacidad para monitorear y aplicar políticas de acceso basadas en el estado de confianza de los dispositivos utilizados por los usuarios. • Funcionalidad de Single Sign-On (SSO) para acceso centralizado a múltiples aplicaciones mediante una única autenticación.

	• Disponibilidad de herramientas de análisis, monitoreo y administración proporcionadas por el fabricante para facilitar la gestión operativa de la plataforma. • Acceso al soporte oficial del fabricante Cisco durante la vigencia de la suscripción.
6.1.2	**La solución de Autenticación Multifactor (MFA) debe contar con las siguientes características de administración:** • La consola de administración bebe ser administrada mediante consola de gestión centralizada sin necesidad de instalar componentes hardware. • La consola de administración debe ser gestionada vía interfaz gráfica por protocolo seguro HTTPS. • La plataforma deberá permitir la administración centralizada de usuarios, grupos, dispositivos, aplicaciones protegidas, métodos de autenticación y políticas de acceso desde un único panel de control. • Restricción de acceso a la consola de administración centralizada. • La consola de administración debe contar con el mecanismo de doble factor de autenticación (MFA). • La consola de administración centralizada debe ofrecer diferentes roles de administración. • La solución de Autenticación Multifactor (MFA) debe contar con la capacidad de utilizar APIs para integración con software y/o aplicaciones propietarias de la Fuerza Aeroespacial Colombiana. • Permitir la verificación de proximidad entre el dispositivo de autenticación y el dispositivo utilizado para acceder al recurso protegido •
6.2	**Funcionalidades de administración y reportes.**
6.2.1	• Generar registros de auditoría relacionados con actividades administrativas realizadas sobre la plataforma. • Contar con herramientas de asistencia administrativa proporcionadas por el fabricante para facilitar actividades de configuración, operación, diagnóstico y gestión de la plataforma. • La solución deberá permitir la integración con plataformas SIEM (Security Information and Event Management) para el envío, correlación, almacenamiento y análisis de eventos de autenticación, auditoría, administración y acceso generados por la plataforma. • La solución deberá contar con mecanismos de integración mediante API, Syslog o métodos soportados por el fabricante que permitan la interoperabilidad con herramientas de monitoreo, operación y gestión de ciberseguridad de la Fuerza Aeroespacial Colombiana. • La solución deberá permitir la generación de eventos y alertas que puedan ser consumidos por plataformas SIEM y SOAR para procesos de correlación, análisis, monitoreo continuo y respuesta a incidentes de seguridad.
7	**ESPECIFICACIONES TÉCNICAS DE LOS SERVICIOS**
7.1	**Autenticación Multifactor (MFA)** • Combina dos o más factores de verificación de identidad (algo que el usuario sabe, tiene o es) para autorizar el acceso de forma rápida y no disruptiva. • Métodos soportados: Duo Push (aprobación con un toque desde Duo Mobile), verificación biométrica, tokens hardware (Duo D-100, YubiKey y otros dispositivos OATH-HOTP), passcodes/TOTP y códigos de bypass temporales para casos de contingencia.

	• Cobertura sobre aplicaciones on-premises y en la nube, VPN, recursos legacy administrados por Active Directory y dispositivos sin conectividad (offline).
7.2	**MFA resistente a phishing** • Proximity Verification: confirma que el dispositivo de autenticación y el dispositivo de acceso se encuentran físicamente cerca antes de aprobar el inicio de sesión. • Soporte para autenticadores FIDO2/WebAuthn, que eliminan el uso de secretos compartidos susceptibles de ser interceptados, sin requerir hardware adicional para su despliegue.
7.3	**Passwordless completo** • Autenticación sin contraseña basada en criptografía de clave pública, mediante los estándares FIDO2 (WebAuthn + CTAP). • Autenticadores de plataforma (Touch ID, Face ID, Windows Hello, biometría Android) y autenticadores itinerantes (llaves de seguridad FIDO2 como YubiKey o Feitian). • Duo Push disponible como autenticador passwordless para usuarios con Duo Mobile activado.
7.4	**Duo Directory** • Directorio de usuarios basado en la nube que actúa como fuente de verdad para autenticación primaria y gestión de atributos, sin requerir un almacén de identidad adicional. • Puede operar de forma autónoma o en paralelo con un IdP existente (Active Directory, Microsoft Entra ID, Google Workspace, OpenLDAP) mediante Directory Sync, con aprovisionamiento automatizado vía SCIM 2.0.
7.5	**Trusted Endpoints** • Verifica el estado de gestión del dispositivo de acceso antes de autorizar el ingreso a las aplicaciones protegidas. • En Windows, macOS y Linux, Duo Desktop reporta identificadores únicos del equipo; en iOS y Android se valida la presencia de Duo Mobile activado. • Permite monitorear el acceso desde dispositivos no confiables y, opcionalmente, bloquearlo mediante política.
7.6	**Single Sign-On (SSO)** • Permite el inicio de sesión solo una vez para acceder a múltiples aplicaciones con Duo SSO, actuando como proveedor SAML 2.0 y OpenID Connect (OIDC). • Incluye conectores preconfigurados para aplicaciones empresariales frecuentes y conectores genéricos SAML/OIDC, con políticas de reautenticación configurables por aplicación.
7.7	**Aplicaciones ilimitadas** • Sin límite en la cantidad de aplicaciones —SaaS, on-premises o desarrolladas a medida— que pueden protegerse bajo la licencia.
7.8	**Panel de Control** • Permite administrar la implementación desde un único panel de administración. Esto incluye configurar el inicio de sesión único, crear y administrar aplicaciones, inscribir y activar usuarios, emitir y administrar contraseñas de SMS y códigos de omisión, administrar dispositivos móviles y ajustar la experiencia del usuario. • Incluye Cisco AI Assistant, un asistente conversacional que ayuda a los administradores a diagnosticar problemas de acceso y encontrar guías de configuración.

CERTIFICACION DISTRIBUIDOR AUTORIZADO

ANEXO TÉCNICO "SUSCRIPCIÓN DOBLE FACTOR DE AUTENTICACIÓN (MFA) DUO - CISCO DUO MFA ESSENTIALS EDITION"

El proponente debe presentar una carta de certificación vigente expedida por el fabricante, que acredite que es un Partner que cuenta con las siguientes acreditaciones de portafolio: Preferred Security Partner y Preferred Services Partner.

PERSONAL SOPORTE TÉCNICO Y GARANTÍA POR PARTE DEL FABRICANTE CISCO				
ÍTEM	**PERSONAL**	**CANT.**	**FORMACIÓN ACADÉMICA**	**EXPERIENCIA**
1	Ingeniero de Soporte Especializado	1	Profesional en Ingeniería de Sistemas, Electrónica, Telecomunicaciones o áreas afines, con tarjeta profesional cuando legalmente corresponda. Deberá contar con certificación vigente de nivel profesional del fabricante Cisco, relacionada con seguridad, redes o la solución objeto del contrato.	Experiencia profesional mínima de dos (2) años en implementación, administración o soporte de soluciones de seguridad informática, autenticación multifactor, gestión de identidades o tecnologías Cisco.

NOTA:

Atendiendo la necesidad institucional de garantizar la adecuada apropiación y administración de la solución de Múltiple Factor de Autenticación Cisco Duo MFA Essentials Edition o su equivalente según casa fabricante indique en su hoja de ruta, se considera procedente establecer como obligación del contratista que:
Atendiendo la necesidad institucional de garantizar la adecuada apropiación, implementación y administración de la solución de autenticación multifactor (MFA) Cisco Duo MFA Essentials Edition, o su equivalente, de conformidad con la hoja de ruta tecnológica definida por el fabricante correspondiente, se considera necesario establecer como obligación contractual del contratista lo siguiente:Durante la vigencia de la Suscripción, el contratista proporcionará actividades orientadas al fortalecimiento de habilidades en la administración autónoma de la solución ofrecida, impartidas por la casa matriz o fabricante, para hasta dos (02) personas técnicas de la Dirección de Seguridad Informática y Electrónica. En caso de que dichas actividades se realicen fuera de la guarnición de Bogotá, el contratista asumirá la totalidad de los gastos asociados, incluyendo transporte, alojamiento y alimentación del personal designado.

Lo anterior se justifica basado en lo expuesto en la circular No. FAC-S-2025-012565-CR del 12 de noviembre de 2025 / MDN-COGFM-FAC-COFAC-JEMFA-CODAF, cuyo asunto es el Análisis y evaluación para la inclusión de costos de comisiones al exterior dentro de la estructuración contractual de procesos, teniendo en cuenta lo anterior y en la necesidad de no afectar los recursos internos destinados a viáticos, garantizar la ejecución efectiva del componente de transferencia de conocimiento y dar cumplimiento a los lineamientos impartidos por el Comando de Apoyo de la Fuerza en materia de estructuración contractual, conforme a la normatividad vigente de contratación estatal.

Así mismo, el personal de soporte técnico especializado exigido en el presente anexo técnico deberá ser acreditado por el proponente con la presentación de la oferta, mediante la documentación que demuestre el cumplimiento de los requisitos mínimos de formación académica, certificaciones vigentes del fabricante y experiencia requeridos para cada perfil.

Transferencia de conocimiento y fortalecimiento de capacidades técnicas

Durante la vigencia de la suscripción, el contratista deberá proporcionar actividades de capacitación y transferencia de conocimiento impartidas por la casa matriz o por el fabricante de la solución ofertada, orientadas a fortalecer las competencias técnicas necesarias para la administración, operación y aprovechamiento de las funcionalidades de la solución de autenticación multifactor implementada en la Entidad. Estas actividades estarán dirigidas hasta a dos (2) funcionarios de la Dirección de Seguridad Informática y Electrónica.

En caso de que las actividades de capacitación o transferencia de conocimiento deban realizarse fuera de la guarnición de Bogotá D.C., el contratista asumirá la totalidad de los costos asociados a la participación del personal designado por la Entidad, incluyendo transporte, alojamiento y alimentación, sin que ello genere erogaciones adicionales para la Fuerza Aeroespacial Colombiana.

La presente obligación tiene como finalidad fortalecer la capacidad institucional para administrar adecuadamente la solución de autenticación multifactor, promover la transferencia de conocimiento especializado por parte del fabricante y garantizar el aprovechamiento de las funcionalidades contratadas durante la vigencia de la suscripción.



Subteniente FABIO ANDRES SOTO GOMEZ
Comité Estructurador Técnico



Capitán. DANIEL LEONARDO UMAÑA BAUTISTA
Gerente de Proyecto