CARACTERÍSTICAS TÉCNICAS DEL BIEN O SERVICIO:

Objeto:

Adquirir la renovación la suscripción del licenciamiento ZTNA (Zero Trust Network Access) incluido soporte.

Clasificación UNSPSC

De acuerdo con la codificación de Bienes y Servicios del Código Estándar de Productos y Servicios de Naciones Unidas, el bien y/o servicio requerido se encuentra codificado de la siguiente manera:

Tabla. Códigos UNSPSC relacionados con el proceso.

SEGMENTO	FAMILIA	CLASE	PRODUCTO
43000000 Difusión de tecnologías de información y telecomunicaciones.	43230000 Software	43233200 software de seguridad y protección	43233205 software de seguridad de transacciones y de protección contra virus
81000000 Servicios basados en ingeniería, investigación y tecnología.	81110000 servicios informáticos	81112500 servicios de alquiler o arrendamiento de licencias de software de computador	81112501 servicio de licencias del software del computador
81000000 Servicios basados en ingeniería, investigación y tecnología.	81110000 servicios informáticos	81112200 mantenimiento y soporte de software	81112208 Mantenimiento de Software y protección de seguridad

Justificación de continuidad del servicio

La Entidad cuenta actualmente con la solución **Cloudflare Zero Trust implementada como su plataforma de VPN/ZTNA y filtrado de navegación web (SWG),** la cual es utilizada por los funcionarios para acceder de forma remota a las aplicaciones y recursos corporativos, así como para aplicar las políticas de filtrado y control de contenido web cuando el funcionario se encuentra fuera de la red corporativa institucional.

La renovación del licenciamiento busca garantizar la continuidad del servicio actualmente en producción, evitando:

- Interrupciones en el acceso remoto seguro de los funcionaros de la Entidad.

- Pérdida de las políticas de acceso, reglas de filtrado, integraciones (IdP, SIEM, SOC) y configuraciones ya maduradas en el entorno productivo.
- Costos y riesgos operativos asociados a un proceso de migración a una plataforma distinta (reconfiguración de agentes en endpoints, recapacitación de usuarios y administradores, período de estabilización).
- Afectación a la postura de seguridad de la Entidad durante una eventual ventana de transición entre soluciones.

Asimismo, la solución verifica continuamente la identidad del usuario, el estado del dispositivo y el contexto de la conexión antes de autorizar el acceso a cada aplicación, de forma que ningún usuario obtiene acceso general a la red interna, sino únicamente a los recursos específicos que su rol requiere. Esto reduce de manera significativa la superficie de ataque y limita el movimiento lateral de un eventual atacante, incluso en el caso de que llegue a comprometer las credenciales de un funcionario.

Igualmente, la plataforma valida además la postura de seguridad de cada equipo antes de permitir la conexión (antivirus activo y actualizado, disco cifrado, firewall habilitado, sistema operativo actualizado y equipo administrado por Intune y registrado en Entra ID), y aplica filtrado de navegación web incluso cuando el funcionario se encuentra fuera de la red corporativa, bloqueando sitios maliciosos, phishing y malware en el mismo punto de acceso remoto. Al operar como servicio en la nube, la solución no requiere infraestructura propia que la Entidad deba mantener, escala de forma natural con el crecimiento de la planta de funcionarios y terceros autorizados, y entrega registros de acceso y navegación que alimentan el SIEM y el monitoreo del SOC, ampliando la visibilidad disponible para la gestión de incidentes de seguridad.

Finalmente, en conjunto, estos elementos muestran que **Cloudflare Zero Trust** no es solo el reemplazo de una VPN tradicional, sino un control activo de seguridad que reduce el riesgo de intrusión y acceso no autorizado a los aplicativos institucionales, por lo que su renovación representa, además de continuidad operativa, una decisión que preserva y fortalece una capacidad de seguridad ya madura dentro de la SFC.

A continuación, se presentan las características que debe cumplir la ficha técnica, las cuales se relacionan a continuación:

FICHA TECNICA – ZTNA CLOUDFLARE	
CANTIDAD DE USUARIOS	1265
DENOMINACIÓN TÉCNICA	Renovación del licenciamiento de la Solución basada en seguridad Zero Trust, con la que cuenta la Superfinanciera de Colombia
SUSCRIPCIÓN Y SOPRTE TÉCNICO	12 meses
SUBÍTEM	**MÍNIMO REQUERIDO**
1.1	**El contratista deberá:** • Garantizar la **protección frente a ataques y amenazas cibernéticas**, mediante las capacidades de seguridad de la solución. • Implementar y mantener **controles de acceso a las aplicaciones**, considerando criterios de identidad, contexto y postura de seguridad del dispositivo (Device Posture). • Garantizar el **acceso remoto seguro** a las aplicaciones y recursos institucionales para los usuarios autorizados. • Disponer de un **plan de soporte técnico con cobertura 7x24**, durante la suscripción del licenciamiento. • Brindar **soporte técnico en idioma español y en horario de Colombia**, de acuerdo con las condiciones establecidas para la prestación del servicio.
1.2	El contratista deberá garantizar la solución ofertada deberá ser de licencia exclusiva de la Entidad, no se aceptarán soluciones de uso compartido, licenciamiento open source y reúso de licenciamiento.
1.3	El contratista deberá proveer una visibilidad completa sobre toda la superficie de ataque, sobre un único portal que proporcione una vista unificada.

1.4	De acuerdo con la solicitud que determine el supervisor del contrato durante su ejecución, el contratista deberá adaptarse a los requerimientos de la Entidad, en el marco del objeto, alcance y condiciones técnicas establecidas contractualmente.
1.5	El contratista deberá disponer de un soporte continuo para evitar interrupciones en la operación de la Entidad.
1.6	La solución ofertada debe ser de propiedad y operada como un servicio en la nube para garantizar una mejor experiencia del usuario final y proteger a los usuarios autorizados que acceden a los servicios que se ejecutan en la nube pública, privada y On-premise.
1.7	La solución ofertada debe garantizar la autenticación, autorización y acceso de mínimo privilegio a aplicaciones privadas (tráfico User-to-App), así como la capacidad de integración o convivencia nativa con módulos/soluciones de filtrado de URL y protección de navegación web (SWG) para hacer cumplir las políticas de uso de Internet de la entidad.
1.8	La solución ofertada debe proporcionar controles consolidados de acceso seguro a servicios e infraestructura en la nube (SaaS privado, IaaS y PaaS), mediante la verificación de identidad, contexto de usuario y políticas de mínimo privilegio para garantizar el uso seguro de las aplicaciones.
1.9	La solución ofertada debe crear un límite lógico basado en la identidad y el contexto que abarque un usuario empresarial y una aplicación o un conjunto de aplicaciones alojados internamente.
1.10	La solución ofertada debe restringir el acceso a través de la verificación de la identidad, el contexto y el cumplimiento de las políticas de los usuarios antes de permitir el acceso.
1.11	La solución debe contribuir a la reducción del riesgo mediante la evaluación continua de la postura de seguridad del dispositivo (Device Posture) y la verificación contextual de amenazas antes de otorgar el acceso, minimizando la superficie de ataque para evitar que la operación se vea afectada.

1.12	La solución ofertada debe minimizar las opciones de movimiento lateral a otras partes de la red.
1.13	La solución debe admitir la protección de los usuarios autorizados en los puntos de conexión permitidos para los servicios adecuados.
1.14	La solución deberá contar con la capacidad de convivir e integrarse con la infraestructura y dispositivos perimetrales existentes de la Entidad mediante conectores ligeros de software y/o integraciones vía API / Syslog.
1.15	La solución ofertada debe poder mantener compatibilidad e integración con las plataformas de Ciberdefensa Avanzada y Analítica Avanzada, con fin de contribuir a la convergencia de información de brechas y apoyar tareas de identificación de riesgos.
1.16	Con el fin de garantizar el cumplimiento de los requisitos plasmados en el presente documento, el contratista deberá entregar al momento de la suscripción del acta de inicio los datasheet u hojas de datos y/o manuales de usuario que avalen el cumplimiento técnico de la solución ofertada.
1.17	La solución ofrecida debe estar basada en arquitectura Anycast, para que todas las solicitudes entrantes se puedan enrutar a una variedad de diferentes ubicaciones o nodos.
1.18	La capacidad de perímetro de la plataforma debe ser de al menos 280Tbps
1.19	La solución ofertada debe proveer una alta disponibilidad que garantice tiempos de recuperación de máximo 1 hora en caso de fallas críticas
1.20	La solución ofertada debe garantizar la protección del correo electrónico corporativo mediante la inspección y análisis del tráfico de entrada/salida de las bandejas de correo mediante integración nativa por API, para la detección de phishing, malware y suplantación de identidad.
2	**Zero Trust Network Access**
2.1	La solución debe:

	Verificar el contexto (como la identidad y la posición del dispositivo) para asegurar el acceso a las aplicaciones
2.2	Debe permitir la conexión a recursos privados vía TCP/UDP/ICMP
2.3	Debe permitir la gestión del control de acceso a las aplicaciones con base en identidad de usuarios, postura de seguridad del dispositivo y otros factores contextuales del usuario y dispositivo
2.4	Mantener operativa la integración existente con Azure Active Directory y otros proveedores de identidad basados en SAML y OIDC
2.5	La conexión de dispositivo de usuario final puede ser con agente ó sin agente
2.6	El acceso a las aplicaciones desde el borde/perímetro se hace a través de túneles
2.7	Debe permitir gestión de acceso del usuario basado en identidad de usuarios individuales y grupos de usuarios
2.8	Debe permitir la configuración de reglas de acceso al menos para: correo electrónico, dominio de correo, rango de dirección IP, país, método de login, método de autenticación y postura de seguridad del dispositivo
2.9	El contratista deberá tener una consola centralizada
2.10	La solución deberá debe soportar SCIM y caching de grupos y usuarios AD
2.11	La solución deberá mantener la interoperabilidad con la infraestructura actual (firewalls, IDP, SIEM, etc.)
2.12	La solución deberá ser compatible con entornos híbridos y multi-nube (Azure, AWS, GCP).
2.13	El contratista deberá permitir la aplicación de las políticas de acceso Zero Trust y de seguridad de red sobre la infraestructura y cargas de trabajo desplegadas en los proveedores de nube pública utilizados por la Entidad, incluyendo como mínimo Microsoft Azure, Google Cloud Platform (GCP) y Oracle Cloud Infrastructure (OCI), garantizando protección uniforme independientemente del proveedor de nube donde residan las aplicaciones o recursos.

3	Secure Web Gateway
3.1	Debe permitir configurar políticas para inspeccionar el tráfico DNS, de red, HTTP y tráfico de egreso
3.2	Las políticas de DNS deben inspeccionar las consultas de DNS y poder bloquear dominios y direcciones IP a los dispositivos
3.3	Las políticas de red deben inspeccionar paquetes TCP/UDP/GRE individuales. Debe poder bloquear el acceso a puertos específicos en los servidores de origen, incluidos los recursos que no son HTTP como SSH y RDP
3.4	Las políticas HTTP deben inspeccionar solicitudes HTTP y poder bloquear la carga de URL específicas, no solo el dominio en sí.
3.5	Las políticas de resolución inspeccionan las consultas de DNS para permitir la resolución mediante servidores de nombres (nameservers) autorizados personalizados
3.6	Las políticas de DNS deben consistir en acciones y expresiones lógicas que determinan su alcance.
3.7	Debe permitir la configuración de políticas de resolución para acceder a dominios enrutados no públicamente, por ejemplo, servicios de red privados o recursos internos.
3.8	Debe permitir crear políticas DNS, de red y HTTP basadas en aplicaciones y tipos de aplicaciones. Puede seleccionar aplicaciones individuales o grupos de tipos de aplicaciones para filtrar tráfico específico en la red
3.9	Debe permitir bloquear riesgos de seguridad potenciales y conocidos en la Internet pública por Categorías de Contenido, Riesgos de Seguridad y Amenazas de Seguridad
3.10	Debe permitir establecer políticas de filtrado de tráfico saliente basadas en la identidad del usuario
3.11	Debe permitir la creación de listas de URL, nombres de host, Números seriales, Direcciones de correo electrónico de los usuarios, Direcciones IP, Números de identificación del dispositivo
4	**Requerimientos de Servicios**

4.1	El contratista debe implementar planes de transferencia de conocimiento para el equipo interno como mínimo dos (2) sesiones por el año de la suscripción del licenciamiento de acuerdo con la solicitud que realice el supervisor del contrato.
4.2	El contratista deberá informar el plan de mantenimiento y actualización de la solución durante la suscripción del licenciamiento realizados por el fabricante con un tiempo prudencial de 48 horas para tomar las medidas necesarias frente a la disponibilidad del servicio. Las actividades previstas en dicho plan deberán ser realizadas por personal con experiencia y conocimientos técnicos en la solución, debidamente certificado o avalado por el fabricante de la solución ofertada.
4.3	La solución debe permitir integración con el SOC de la Entidad para su monitoreo (vía API/Syslog/SIEM)
4.4	El contratista deberá realizar como mínimo dos (2) jornadas de transferencia de conocimiento técnica avanzada durante la suscripción del licenciamiento, dirigidas a los administradores de la plataforma de la Superintendencia Financiera de Colombia, cubriendo administración, operación, solución de incidentes, mejores prácticas, nuevas funcionalidades y optimización de políticas.
4.5	El fabricante o partner deberá suministrar material de capacitación, laboratorios prácticos y memorias de las sesiones realizadas.
4.6	El contratista deberá brindar acompañamiento técnico para la adopción de nuevas funcionalidades liberadas durante la suscripción del licenciamiento.
5	**SOPORTE TÉCNICO**
5.1	Tiempo de actividad (Uptime): 99.99% de disponibilidad mensual.
5.2	Latencia de red: máximo 50 ms para conexiones a través del proveedor SASE
5.3	Velocidad de resolución DNS: <30 ms en consultas.
5.4	Tiempo de respuesta del servicio: Máx. 5 segundos para el establecimiento de sesiones seguras.

5.5	Tiempo de verificación de identidad: <2 segundos para autenticación multifactor.
5.6	Frecuencia de evaluación de políticas ZT: Evaluación continua cada 5 minutos o menos.
5.7	Detección de amenazas: Detección de anomalías en menos de 1 minuto.
5.8	**Tiempo de respuesta/atención del soporte:** Para los incidentes clasificados como **críticos**, el contratista deberá brindar una primera respuesta en un tiempo máximo de **treinta (30) minutos**, con disponibilidad **(24/7).** Este término se contabilizará a partir del momento en que el **supervisor del contrato comunique formalmente al contratista la ocurrencia del incidente**, a través de los canales de soporte establecidos, indicando o aportando la información que permita evidenciar y gestionar el incidente reportado.
5.9	Tiempo de diagnóstico y plan de acción/mitigación para incidentes mayores: Máximo 2 horas.
5.10	Actualizaciones de seguridad: Aplicación de parches críticos en menos de 24 horas.
Nota: Los términos y tiempos establecidos para la atención, respuesta y gestión de los requerimientos, solicitudes o incidentes se contabilizarán a partir del momento en que el **supervisor del contrato comunique formalmente al contratista la respectiva situación**, a través de los canales definidos para tal fin, suministrando la información necesaria que permita su identificación, validación, atención y gestión.	

En constancia de lo anterior se firma por,

CARLOS ARTURO D ´OTERO BISCARDI
Firmado digitalmente por CARLOS ARTURO D´OTERO BISCARDI
Fecha: 2026.11.06 17:09:15 -05'00'

Carlos Arturo D'Otero Biscardi
Grupo de Ciberseguridad Institucional y Continuidad Tecnológica

EDGAR YESID GARAY MEDINA
Firmado digitalmente por EDGAR YESID GARAY MEDINA
Fecha: 2026.11.06 17:12:55 -05'00'

Edgar Yesid Garay
Coordinador Grupo de Ciberseguridad Institucional y Continuidad tecnológica

SAUL ARMANDO PEDRAZA MORENO
Firmado digitalmente por SAUL ARMANDO PEDRAZA MORENO
Fecha: 2026.11.06 18:09:37 -05'00'

Saul Armando Pedraza Moreno
Subdirector de Operaciones