

**ANEXO 2**  
**FICHA TÉCNICA**

**OBJETO:**

**ADQUISICIÓN, INSTALACIÓN, CONFIGURACIÓN, PUESTA EN  
FUNCIONAMIENTO DE SOLUCIÓN DE SEGURIDAD MULTINIVEL CON  
GARANTÍA Y SERVICIO POSVENTA**

| SEGMENTO | FAMILIA  | CLASE    | PRODUCTO | NOMBRE                                              |
|----------|----------|----------|----------|-----------------------------------------------------|
| 43000000 | 43230000 | 43233200 | 43233205 | Software de Seguridad y protección contra virus     |
| 81000000 | 81110000 | 81112200 | 81112208 | Mantenimiento de software y protección de seguridad |
| 43000000 | 43220000 | 43222500 | 43222501 | Equipo de seguridad de red cortafuegos.             |

**ALCANCE:** La solución de seguridad debe constar de los siguientes aspectos.

1. Dispositivo físico de administración Unificada de Amenazas UTM (Unified Threat Management) con garantía de fábrica o garantía extendida por 3 años.
  - 1.1 Licenciamiento de las funcionalidades del UTM por el tiempo de la garantía de fábrica o garantía extendida del dispositivo.
2. Software de seguridad de correo electrónico: Email Security Gateway, con su respectivo licenciamiento por el mismo periodo de los demás elementos de la solución de seguridad.
3. Servicio posventa el cual incluye soporte remoto y/o en sitio para la configuración y normal funcionamiento de toda la solución de seguridad por el tiempo de la garantía de fábrica o garantía extendida del dispositivo.

## ESPECIFICACIONES TÉCNICAS

1. Dispositivo físico de administración Unificada de Amenazas UTM (Unified Threat Management) con garantía de fábrica o garantía extendida por 3 años, el cual consta de:

- a. Funcionalidades mínimas:

Solución física de propósito específico UTM (Unified Threat Management), de modo que reemplace las dos (2) soluciones actuales Microsoft TMG y cuyas funcionalidades mínimas contengan:

- **Dashboard:** Debe ser un tablero gráfico de fácil manejo que muestra las opciones disponibles en el UTM así como el resumen o estadísticas de la actividad de seguridad.
- **Monitoring:** Ver en tiempo real cómo se encuentra la Entidad frente a amenazas de Ciberseguridad, así como también generación de reportes, revisión de log y eventos de la actividad del UTM (generación de reportes periódicos de tráfico y amenazas en la red).
- **Intrusion Prevention System** (IPS o Sistema de prevención de intrusos): protección en tiempo real contra network threats, spyware, ransomware, SQL injections, cross-site scripting, buffer overflows; escaneo del tráfico en todo los protocolos.
- **URL Filtering (Motor de filtrado de URLs):** Bloqueo de sitios maliciosos y con contenido inapropiado y los sitios de Internet que determine la Entidad y que inspeccionen sitios de Internet que utilizan los protocolos HTTP, HTTPS, FTP y demás. Preferiblemente que contenga opción para establecer horarios de visita a ciertos sitios (calendario) y /o configuración por usuarios del directorio activo.
- **Gateway AntiVirus:** Identificar y bloquear spyware, virus, trojans, worms, rogware y blended threats – incluyendo nuevas variantes de

virus habidas y por haber.

- ***Reputation-Based Threat Prevention:*** Sistema que actualiza la información automáticamente desde múltiples fuentes acerca de sitios maliciosos o amenazas de ciberseguridad. Listas negras, listas blancas.
- ***Remote Access Policy (VPN):*** A través del UTM se debe configurar el acceso por VPN a la Entidad como actualmente se hace por TMG.
- ***Networking configuration:*** Configuración del bloque de direcciones IP fijas que dispone la Entidad por canal y demás configuraciones de red externa - interna.
- ***Control y priorización de ancho de banda y calidad de servicio (QoS) en modo básico.***
- ***Protocolos IPV4 e IPV6.***
- EL UTM debe contar mínimo con ***certificación ICASA LAB o NSS Labs o ambas*** *(Puesto que es la Contraloría General de Antioquia quien vela por la seguridad de sus canales de internet y por ende de su información, buscamos una solución UTM ampliamente aceptada en el mercado y suficientemente probada (testeada) por laboratorios reconocidos en el medio de la seguridad informática como lo es el laboratorio ICASA. Así pues, se puede concluir que es la Contraloría quien asume el mayor riesgo y buscamos soluciones estables, que perduren en el tiempo y que no generen una carga en su ejecución. Por lo tanto se aceptan los UTM certificados en los laboratorios NSS Labs e ICASA Labs.).*
- El equipo deberá poder ser **configurado en modo gateway o en modo transparente en la red.**
- Por seguridad y facilidad de administración, para el UTM no se aceptan equipos de propósito genérico (PCs o Servidores físicos o virtuales) sobre los cuales puede ejecutarse o instalar un sistema operativo regular como Microsoft Windows o Linux, es decir, no se aceptan soluciones de propósito general en software para ser instaladas en servidores de propósito general.
- Es de resaltar que al ser una solución física, el Hardware o dispositivo UTM (llamado comúnmente “la caja”) en su última versión, será propiedad de la Contraloría General de Antioquia salvo un nuevo contrato que

permita disponer de una nueva “caja” mejorada. Así mismo, garantizar que los equipos suministrados a la Entidad sean de última tecnología, esto es, a partir del año 2016 en adelante. Se debe incluir ficha técnica del equipo.

- El equipos y sus especificaciones deben estar publicados en la página Web del fabricante, donde se pueda corroborar todas sus características, modelo superior al año 2016, y sobre todo que dicho UTM si corresponda a la última generación de UTM's de su familia.
- El proponente debe estar avalado por el fabricante para vender la solución UTM, en razón a esto, debe adjuntar certificación de su relación con el fabricante del dispositivo UTM.

**b. Características básicas:**

- Dispositivo de última generación.
- Bajos niveles de latencia.
- Disco duro de estado sólido.
- Tiempo de Respuesta muy aceptable para una solución de última generación.
- Tasa de transferencia alta.
- Capacidad de realizar SSL VPNs.
- Túneles VPN IPSec Gatewat-to-Gateway.
- Túneles VPN IPSec Client-to-Gateway.
- Inspección profunda en el protocolos https.
- Cantidad mínima de canales de Internet soportados: 2 canales de internet de 40Mb cada uno.

**c. Valores mínimos de Referencia:**

- Rendimiento mínimo de Firewall: 16 Gbps
- Cantidad de Sesiones Concurrentes: 6 Millones
- Rendimiento mínimo de IPS: 2 Gbps
- Rendimiento mínimo de NGFW: 1.7 Gbps
- Rendimiento mínimo de Protección de Amenazas: 1.5 Gbps
- Tiempo de Respuesta máximo : 3 Microsegundos
- Cantidad mínima de sesiones nuevas por segundo: 200.000

- Capacidad mínima VPN IPSEC: 80 Mbps
- Capacidad mínima de control de aplicaciones: 2.5 Gbps
- Capacidad mínima de Inspección de protocolos seguros: 1.9 Gbps
- Capacidad mínima VPN SSL: 350Mbps
- Posibilidad de formar parte de un cluster de alta disponibilidad.

Cantidad de usuarios de la Entidad. Entre 300 a 400.

- Se debe considerar al menos el tener una interface/puerto DMZ y 2 puertos para enlaces WAN.
- Soporte a políticas de enrutamiento (policy routing).
- Soporte a enrutamiento estático.
- Soporte a enrutamiento dinámico.
- El soporte a políticas de enrutamiento deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál tráfico sale por un enlace y qué tráfico sale por otro enlace o ambas situaciones o implementar dos dispositivos que son cubiertos por el proveedor dentro de ésta propuesta.
- Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.
- Las reglas del firewall deberán tomar en cuenta dirección IP fuente (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando.
- Las acciones de las reglas deberán contener al menos el aceptar o rechazar la comunicación
- Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a tiempo.
- Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año).
- Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.
- Capacidad de hacer traslación de direcciones dinámico, muchos a uno.
- Deberá soportar reglas de firewall que soporten autenticación por usuarios mediante repositorios locales o remotos (LDAP, RADIUS, TACACS+).

#### **1.1.    Licenciamiento de las funcionalidades del UTM por el tiempo de la garantía de fábrica o garantía extendida del dispositivo.**

Cumplir con la garantía contada a partir de la fecha entrega del mismo, es decir, el dispositivo debe funcionar con todas sus funcionalidades en condiciones

normales durante un periodo de garantía bien sea otorgada por el fabricante o extendida, **por 3 años.**

2. **Software de seguridad de correo electrónico: Email Security Gateway, con su respectivo licenciamiento por el mismo periodo de los demás elementos de la solución de seguridad (ítems 1 y 1.1) , el cual debe cumplir mínimamente con las siguientes características:**

Software de seguridad de correo electrónico (anti-spam, anti-malware y filtrado de contenido) para el correo electrónico Exchange 2010 o superior que incluye:

- Interfaz gráfica de fácil manejo.
- Motores de escaneo de malware, spam y contenido no deseado en tiempo real de los correos entrantes y salientes de cada buzón. El motor de escaneo debe trasladar los correos sospechosos o peligrosos a cuarentena para ser inspeccionados por un funcionario de la Contraloría, quien determinará si el correo debe ser aceptado o eliminado.
- Listas blancas personalizables (Whitelists)
- Lista Negras.
- Detección de spam mediante diferentes métodos.
- Generador de reportes.
- Filtrado y bloqueo de adjuntos ejecutables y comprimidos que contienen ejecutables peligrosos.
- Lista de bloqueo de direcciones de correo electrónico personalizables, direcciones IP, dominios, entre otras.
- Escáner de prevención de exploits de correo electrónico.
- Detector de scripts incrustados en código HTML.
- Módulo anti suplantación de identidad.

En cuanto al licenciamiento del Software de seguridad de correo electrónico, se debe proveer dicho licenciamiento por el tiempo de 3 años, con el fin de guardar uniformidad, economía y control sobre la solución completa.

3. **Servicio posventa el cual incluye soporte remoto y/o en sitio para la configuración y normal funcionamiento de toda la solución de seguridad por el tiempo de la garantía de fábrica o garantía extendida del dispositivo. El servicio posventa debe cubrir obligatoriamente los siguientes aspectos:**

- a. Cumplir con la garantía del dispositivo UTM contada a partir de la entrega del mismo, es decir, el dispositivo debe funcionar en condiciones normales durante el periodo de la garantía de fábrica o garantía extendida por 3 años.
- b. Mantener al día el licenciamiento de las funcionalidades del dispositivo UTM durante el periodo de la garantía de fábrica o garantía extendida por 3 años.
- c. El proveedor debe realizar una Auditoria de seguridad informática y de vulnerabilidades de la red de datos de la Entidad con su respectivo informe técnico detallado, informe ejecutivo y plan de remediación, con el objetivo de detectar y corregir tempranamente fallas de seguridad y vulnerabilidades en aplicaciones, servidores, estaciones de red y dispositivos de red una vez adjudicado el contrato. (Se realiza una vez al año).
- d. Se hará migración y depuración de las reglas del TMG al nuevo dispositivo por parte del proveedor. Así mismo, se debe garantizar que las reglas de navegación (salida a Internet de los aplicativos) entre otras, queden correctamente configuradas y funcionales. Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. El proveedor debe migrar las políticas de seguridad y de acceso web actuales. La Contraloría actualmente mediante el TMG hace pública las direcciones web de varios de sus servicios, como por ejemplo el portal institucional [www.cga.gov.co](http://www.cga.gov.co) el cual tiene una IP fija y está alojado en un servidor en el Datacenter interno. La nueva solución UTM debe permitir también publicar las aplicaciones web o servicios al exterior.

### **3.1. Modalidad del servicio posventa:**

- La solución de seguridad debe quedar configurada para estar disponible 24 horas al día los 7 días de la semana, y de requerirse atención en sitio y/o remoto, debe darse en horario laboral o de común acuerdo con un tiempo de respuesta mínimo de dos (2) horas.
- 
- Cuando el soporte técnico se requiera de manera presencial se debe brindar en las instalaciones de la Entidad en la ciudad de Medellín.
- 
- El servicio de soporte técnico debe garantizar una adecuada operación de los productos ofrecidos, de conformidad con las especificaciones técnicas y de funcionalidades señaladas en la documentación relacionada para la operación de los productos por el fabricante.

- El oferente debe entregar informes o documentación detallada de todos los procedimientos realizados después de los mantenimientos preventivos y correctivos, soporte por problemas presentados, actualizaciones, así mismo se debe detallar en el informe las causas, procedimientos preventivos y soluciones futuras inmediatas a los problemas o daños presentados en cualquiera de las herramientas.
- En caso de ser necesario el proveedor debe diseñar y ejecutar el plan de instalación más recomendado para la Entidad dando el soporte técnico adecuado con los niveles de servicio necesarios para el óptimo funcionamiento.
- El proveedor debe atender a la Entidad, todos los requerimientos técnicos a que haya lugar, durante el periodo de vigencia de la garantía, bien sean consultas técnicas sobre funcionamiento de las herramientas, reconfiguración de la solución y atención a los requerimientos técnicos.

3.2. **Atención en Sitio:** Cuando se haya determinado el problema y no se encuentre solución telefónica o remota, el proveedor debe asignar un ingeniero para que se desplace a las oficinas de la Entidad, en un tiempo no mayor de cuatro (4) horas.

3.3. **Contactos de soporte técnico:** La Entidad en conjunto con el proveedor, deberá identificar el número correspondiente de contactos, quienes serán el canal autorizado para acceder a los servicios de soporte técnico.

3.4. **Mantenimiento Preventivo:** Se deben realizar mínimo una (1) visita o revisión durante el tiempo de la garantía por cada año, dichas visitas se deben concertar entre el proveedor y La Entidad y el proveedor deberá entregar un cronograma de las actividades que va a realizar en dicho mantenimiento.

El mantenimiento preventivo para el hardware y software debe contemplar la revisión de todas las funciones básicas y operativas del Sistema y sus elementos. Los Ingenieros deberán estar dotados de las herramientas necesarias para el desempeño de sus labores y elementos de seguridad industrial.

De igual manera, cada Ingeniero deberá contar con el software de diagnóstico de cada uno de los equipos de acuerdo a su marca y modelo.

El mantenimiento preventivo de software debe contemplar actualizaciones, parches, fix o versiones liberadas por el fabricante durante el periodo de garantía sin costos adicionales.

Se debe contemplar mínimo una prueba de análisis de vulnerabilidad durante cada año de garantía.

- 3.5. **Mantenimiento Correctivo:** Se deberá realizar cuantas veces la Entidad lo requiera en modalidad de (7x24), con un tiempo de respuesta no mayor de ocho (8) horas, y deberá prestarse en las instalaciones en donde se encuentren instaladas el hardware y/o software.

Los repuestos que sean necesarios para efectuar la reparación y dejar en perfecto funcionamiento cualquiera de los elementos de hardware o software correrán por cuenta del proveedor.

El oferente debe hacer efectiva ante el fabricante la garantía de los componentes de hardware o software que deban ser reemplazados. No obstante, debe garantizar el cambio total e inmediato de cualquier parte de hardware o software que presenten defectos o fallas por método de fabricación, por otros nuevos de iguales características.

Los repuestos empleados para reemplazar elementos defectuosos serán de la misma calidad al existente y se realizara su reemplazo previa autorización de la Dirección de sistemas de la Entidad.

El oferente deberá contar con puntos de contacto para la recepción de solicitudes de servicios, en donde se respondan y solucionen todas las peticiones de soporte de la Entidad, resolviendo los casos o direccionándolos inmediatamente al fabricante.

En los casos de soporte en sitio, el proveedor deberá hacer un seguimiento de la solicitud del servicio, desde el momento de recibo de la solicitud hasta la prestación del servicio, para asegurar y verificar que el trabajo de los ingenieros de campo se está haciendo de acuerdo con los estándares técnicos y de servicio ofrecidos a la Entidad.

Se define que un Requerimiento de Servicio ha sido solucionado mediante un acuerdo entre el proveedor y el líder técnico de la Entidad, cuando

típicamente la Entidad ha recibido información o indicaciones que resuelve el problema de configuración.

### 3.6. Tiempo de respuesta de solución

El proponente deberá cumplir con los tiempos de respuesta y solución de acuerdo a la severidad asignada a cada incidente, la cual se establece en función a la urgencia y el impacto.

| PRIORIDAD | DETALLE                                                                                                                       | TIEMPO DE RESPUESTA | TIEMPO DE SOLUCIÓN |
|-----------|-------------------------------------------------------------------------------------------------------------------------------|---------------------|--------------------|
| CRÍTICO   | Falla en la solución de seguridad que impide el que ésta arranque o se inicie.                                                | inmediata           | inmediata          |
| ALTO      | Problema de gran impacto que afecta la operación y el normal funcionamiento de cualquier componente del sistema de seguridad. | 2 horas             | 4 horas            |
| MEDIO     | Observación de desempeño irregular en la solución de seguridad.                                                               | 4 horas             | 8 horas            |
| BAJO      | Consulta técnica y/o de uso, solicitud de cambios                                                                             | 8 horas             | 16 horas           |

#### Soporte Técnico

- **Soporte telefónico:** De Lunes a Viernes en horario de oficina, suministrar una línea de soporte para casos urgentes fuera del horario establecido.
- Suministrar un correo electrónico para efecto de formular peticiones de soporte.
- Soporte presencial en horarios de oficina.
- Asistencia técnica vía internet en horario de oficina y en caso de no solución el soporte deberá presentarse en sitio de acuerdo a la severidad asignada.

#### CONDICIONES GENERALES PARA TODOS LOS ÍTEMS:

Los ofertados por el proponente en respuesta a las **Cantidades y especificaciones técnicas**, deben ser dispositivos y software ampliamente aceptados y comercializados en el mercado (generalmente los productos UTM se encuentran

relacionados en alguno de los cuadrantes mágicos de Gartner -reconocidos a nivel mundial-), lo cual pueden demostrar aportando el documento del cuadrante mágico de Gartner en donde aparezca el fabricante, entregando la relación de las empresas que ya poseen dicha solución a la fecha, la empresa ofertante debe acreditar la ejecución, de máximo tres (3) contratos con objeto igual o similar, que sumen el valor dispuesto para esta contratación, los cuales hayan sido suscritos y ejecutados dentro de los dos (2) años anteriores a la fecha de presentación de las propuestas, para lo que allegará las respectivas certificaciones debidamente evaluadas como proveedor. Adjuntar dicha información en la carta de presentación de la oferta. Dicha información es tratada con estricta confidencialidad y confrontada en el RUP.

1. Entregar los bienes objeto del contrato, debidamente instalados y en condiciones adecuadas para prestar el servicio. Una vez adjudicado el contrato y a partir del Acta de inicio, el contratista tendrá un plazo de dos (2) meses para su entrega.
2. Entregar con pruebas de funcionamiento los equipos y software instalados.
3. El proponente deberá contar con certificaciones en la comercialización de soluciones de seguridad por parte del fabricante.
4. Prestar soporte telefónico y/o en sitio para los incidentes presentados en el servicio. Tiempos de respuesta: Prioridad Alta 2 horas, Prioridad Media 4 Horas, Prioridad Baja 8 Horas. Por el tiempo que dure el servicio posventa.
5. El proponente debe contar como mínimo con una persona profesional ( con estudios afines al objeto del contrato) certificado en la solución UTM, cuya certificación o diploma es expedido por el fabricante del UTM. Además debe aportar los certificados técnicos de las personas que van a apoyar a implementar la solución completa de seguridad, expedidos por cada uno de los fabricantes, y la tarjeta profesional y/o acta de grado de dicho profesional quien será un ingeniero informático, o de sistemas, o electrónico o afín, que será el líder y responsable del proyecto por parte del Contratista.  
Es de aclarar, que es válido que una persona posea los dos certificados. Para ello, deben aportar los certificados y copia de la tarjeta profesional o copia del diploma.
6. El mantenimiento y garantía de la solución debe ser entregado por el proponente por tres (3) años.
7. Todos los equipos y materiales serán nuevos, de primera calidad y en ningún momento deberán ser partes o productos re manufacturados.

8. Los dispositivos y software se solicitan con especificaciones mínimas acorde a estándares institucionales y estudios de mercado pero el proponente puede cotizar mejores características siempre y cuando estas sean 100% compatibles con las características mínimas exigidas y se ajuste al presupuesto.
9. El soporte técnico posventa debe incluir todos los costos de operación en los que debe contemplar mano de obra, transporte y los repuestos, sin generar costo adicional para la Entidad.
10. Entregar los reportes de los mantenimientos o reparaciones técnicas realizadas en el equipo o equipos en el periodo de garantía.
11. El proveedor deberá anexar documento firmado por el fabricante que respalde el soporte técnico ofrecido a los productos a contratar por el tiempo de la garantía.
12. El proveedor deberá garantizar la continuidad del servicio ofrecido por las distintas plataformas tecnológicas, para la Contraloría General de Antioquia.
13. En caso de que el equipo UTM (la caja) falle, el proveedor debe suministrar una solución alternativa durante el mismo día de la falla o máximo el día siguiente hasta restablecer el servicio de forma normal.
14. Se debe proveer el respectivo Licenciamiento y actualización de toda la solución por 3 años.
15. Soporte técnico, que incluye instalación, configuración óptima, monitoreo y soporte técnico preventivo y correctivo, remoto y/o en sitio 5 x 8 durante 3 años sin límite de horas.
16. Capacitación a mínimo 3 funcionarios de la Dirección de Sistemas de Buen Gobierno y TIC de la Contraloría General de Antioquia.
17. Entrega respectiva de manuales y videos sobre instalación, funcionamiento, creación y modificación de políticas o características y solución de errores más comunes.

**Documentos entregables:**

- Entrega de instaladores y manuales del fabricante en medios magnéticos.
- Evidencia de la capacitación a los funcionarios de la Dirección de Sistemas para el Buen Gobierno y las Tic's de la Contraloría General de Antioquia.

|                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Documentos técnicos para el desarrollo del proyecto.</b></p> | <ol style="list-style-type: none"> <li>1. El proponente debe anexar certificación expedida por el fabricante, que lo acredite como <b>canal autorizado del equipo y software</b> de los ítems descritos en el <b>Alcance</b>, cuya expedición no sea superior a un (1) año, con relación a la fecha de la solicitud de la propuesta. En caso de uniones temporales esta certificación la debe anexar al menos uno de los integrantes de la unión temporal. Acreditar experiencia en soluciones de seguridad mediante la verificación de contratos hechos con otras empresas.</li> <li>2. El valor ofertado por parte del proponente, debe incluir todos los gastos, costos, derechos, impuestos, tasas y demás contribuciones que se causen con ocasión de la presentación de la oferta, de la suscripción y ejecución del contrato por el tiempo del mismo, de acuerdo con las normas legales vigentes, ya que los mismos se entienden por cuenta del contratista.</li> <li>3. El proponente debe presentar su oferta técnica atendiendo la totalidad de las especificaciones técnicas y condiciones generales del servicio, garantía y demás requerimientos establecidos en los presentes estudios.</li> </ol> |
|--------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

