Superintendencia de Industria y Comercio

ESPECIFICACIONES TÉCNICAS – LICENCIAS SSL

Las siguientes son las especificaciones técnicas mínimas que requiere la Entidad, para el cumplimiento del objeto contractual.

LAS ESPECIFICACIONES TÉCNICAS – FICHA TÉCNICA VAN DE ACUERDO CON LOS GRUPOS SEÑALADOS EN EL PLIEGO DE CONDICIONES.

<table>
<tr><th colspan="6">DENOMINACIÓN TÉCNICA: RENOVACIÓN DE SUSCRIPCIONES Y SOPORTE PARA LAS LICENCIAS DE SSL</th></tr>
<tr><th>PLATAFORMA</th><th>CLASIFICACIÓN DEL BIEN O SERVICIOS</th><th>DESCRIPCIÓN</th><th>CANTIDAD</th><th>UNIDAD</th><th>VENCIMIENTO</th></tr>
<tr><td rowspan="2">SSL</td><td rowspan="2"></td><td>Certificados de sitio seguro EV con vigencia de un (1) año</td><td>37</td><td>CERTIFICADO</td><td>21/12/2026</td></tr>
<tr><td>Certificado de sitio seguro Tipo Wildcard con vigencia de un (1) año</td><td>2</td><td>CERTIFICADO</td><td>21/12/2026</td></tr>
<tr><th>No.</th><th colspan="5">OBLIGACIONES TECNICAS</th></tr>
<tr><td>1.</td><td colspan="5">Realizar la revocación y renovación de los certificados de sitio seguro que la supervisión del contrato indique, realizando la reemisión sin costo para la Entidad durante la vigencia del certificado emitido inicialmente.</td></tr>
<tr><td>2.</td><td colspan="5">Realizar la entrega de los certificados de sitio seguro solicitados por la supervisión del contrato en los sistemas de información que se soliciten hasta que sean emitidos en su totalidad con vigencia de un (1) año.</td></tr>
<tr><td>3.</td><td colspan="5">Soporte técnico especializado en idioma español.</td></tr>
<tr><td>4.</td><td colspan="5">Garantizar la calidad y correcto funcionamiento de todos los elementos suministrados durante la ejecución del contrato y la vigencia de estos después de emitidos.</td></tr>
<tr><td>5.</td><td colspan="5">Las especificaciones técnicas esenciales para contratar son:
<table>
<tr><th>No.</th><th>ÍTEM</th><th>CANTIDAD</th></tr>
<tr><td>1</td><td>Certificados de sitio seguro EV con vigencia de un (1) año</td><td>37</td></tr>
<tr><td>2</td><td>Certificados tipo Wildcard con vigencia de un (1) año</td><td>2</td></tr>
</table></td></tr>
<tr><td>6.</td><td colspan="5">La entrega de los certificados objeto del contrato deberá soportarse con la presentación de la respectiva factura en cuyo contenido se debe discriminar la relación de los certificados suministrados con el respectivo valor.</td></tr>
</table>

7.	Brindar asesoría y soporte técnico vía telefónica o correo electrónico 6X8 de los elementos suministrados al menos por el tiempo de su vigencia y un (1) año más, con la finalidad de que allí se concentren todos los mantenimientos tanto preventivos como correctivos y las posibles fallas que presenten los sistemas de información donde se encuentran implementadas los certificados de sitio seguro, reemplazo de certificados digitales SSL si hay lugar a ello, renovaciones si hay lugar a ello, etc., por el término de ejecución del contrato y la vigencia de los certificados una vez estos hayan sido emitidos. El alcance del servicio de soporte técnico a usuarios ofrecido deberá consistir en la asesoría y ayuda en la solución de problemas relacionados con el certificado digital, respecto a su instalación, configuración, integración, implementación y soporte técnico en los Sistemas de Información de la SIC. El proveedor de los certificados de sitio seguro tendrá que dar el soporte técnico necesario sobre los productos adquiridos durante el periodo de la garantía de estos. Al detectar fallas por parte de la Superintendencia de Industria y Comercio se deben llevar a cabo las siguientes actividades: ✓ Un diagnóstico inicial por medio de una conexión remota a los equipos.
	✓ El ingeniero de soporte a cargo del caso debe realizar todo el protocolo de pruebas necesario para validar cuál es el origen de la falla reportada y si es posible dar solución de manera remota. Brindar soporte en sitio si las condiciones lo ameritan con la finalidad de garantizar la adecuada y normal operación de la plataforma instalada.
8.	Proporcionar toda la documentación técnica necesaria y requerida por la Entidad durante la vigencia de los certificados SSL emitidos.
9.	Brindar asesoría y acompañamiento en las instalaciones de la SIC y los aplicativos de software necesarios para habilitar los certificados de sitio seguro.
10.	El contratista deberá ofrecer un soporte técnico permanente a los usuarios bajo las siguientes condiciones: ✓ Medios de acceso: Telefónico y vía Web a través de chat, FAQ's, documentación técnica de soporte, correo electrónico y aplicación de creación y seguimiento de casos de soporte. ✓ Disponibilidad: El servicio de soporte técnico vía telefónica y chat deberá estar disponible 6x8. Los demás canales de soporte técnico (FAQ's, documentación técnica de soporte, correo electrónico y aplicación de creación y seguimiento de casos de soporte) deben estar disponibles 7X24X365. ✓ El alcance del servicio de soporte técnico a usuarios ofrecido deberá consistir en la asesoría y ayuda en la solución de problemas relacionados con el certificado digital, respecto a su instalación, configuración, integración, implementación y soporte técnico en los Sistemas de Información de la SIC. ✓ Tiempos de respuesta: Los tiempos de respuesta para los casos de soporte técnico a usuarios se encuentran clasificados de acuerdo con la valoración del problema de soporte de la siguiente manera: • Soporte de 1er nivel: Tiempo de atención inmediata, consistente en casos de soporte técnico de 1er nivel todos aquellos que hagan parte de los problemas frecuentes de instalación, configuración, integración, implementación y soporte técnico de los certificados digitales en los Sistemas de Información de la SIC. • Soporte 2do nivel: Tiempo de atención de 2 a 24 horas y son aquellos casos que impliquen un proceso de investigación específico. Estos casos contarán con un proceso de registro y diagnóstico que le permitirá al usuario conocer el período de tiempo que tomará la respuesta, periodo en el cual podrá hacer seguimiento de su proceso de

	consulta a través de la aplicación de creación y seguimiento de casos de soporte.
11.	Para los certificados de sitio seguro SSL EV cumplir con las siguientes condiciones: • Sello de Seguridad, que permita visualizar que el sitio está libre de malware, que se analiza periódicamente en búsqueda de vulnerabilidades, que el flujo de información entre navegador y servidor es 100% confidencial y que la identidad propietaria del sitio ha sido verificada por un tercero de confianza. Para lo cual se debe presentar el certificado del tercero de confianza. • Verificación de la propiedad de Dominio, barra de direcciones verde **(**en los navegadores en los que sea posible**)**, validación extendida EV, que permite desplegar el nombre del titular del certificado SSL en cualquier navegador. • Activación de candado de seguridad en el navegador. • El Proveedor debe garantizar que el servicio soporta la Autenticación comercial completa, verificación de la identidad comercial y la propiedad del dominio. • Escaneo automático semanal en búsqueda de vulnerabilidades con reportes detallados en PDF. • Escaneo automático diario de malware para detectar códigos maliciosos en el código fuente del sitio asegurado con el certificado SSL. • Compatibilidad con algoritmos de cifrado: RSA (4096 bits mínimo), ECC. • Los certificados SSL deberán contar con una garantía económica, expresada en dólares estadounidenses (USD), que cubra las pérdidas ocasionadas por errores o incumplimientos atribuibles a la entidad emisora, de acuerdo con las condiciones y los límites establecidos. • Compatibilidad con SAN • El proveedor debe volver a generar un certificado (reemitir) en caso de que se presente una migración de servidores o daño de hardware. • El Proveedor debe garantizar que el servicio es compatible con el estándar de seguridad PKCS (Public Key Cryptography Standards)
	• Monitoreo LOG CT • Servicio de lista negra de URL / Dominio • Reemisión sin costo durante la vigencia del certificado. • Emisión sin costo de un certificado SSL que se haya emitido y con una URL diferente durante el primer mes después de su emisión • Soporte técnico especializado con disponibilidad telefónica y/o vía Web en la modalidad 6x8 (lunes a sábado en el horario laboral de la SIC, durante el período de ejecución del contrato y la vigencia de los certificados de sitio seguro emitidos, cuando la Entidad lo requiera, las líneas de soporte deberán estar ubicadas en Colombia. • Compatibilidad universal con navegadores y dispositivos móviles. • Disposición de un portal para que la SIC pueda realizar la administración de los certificados de sitio seguro (consola de administración), para lo cual el proveedor brindará capacitación tanto al administrador del portal como al equipo técnico para la instalación de los certificados de sitio seguro con la respectiva cadena de confianza • Tamaño de llave: Mínimo de 2048bits • Herramienta de verificación SSL/TLS que permita comprobar la correcta instalación y configuración del certificado, así como identificar errores o configuraciones criptográficas inseguras. • Compatibilidad de Navegadores mínimo: Edge, Safari, Opera, Firefox, Chrome, navegadores basados en Chromium, todos estos en sus diferentes versiones multiplataforma • El certificado SSL tipo EV debe ser emitido por alguna de las siguientes autoridades de certificación internacionales autorizados

<table>
<tr><td></td><td>
por el IRS (Internal Revenue Service) y debe cumplir con las características del enlace https://www.irs.gov/pub/irs-pdf/p5190.pdf:

<table>
<tr><th>AUTORIDAD DE CERTIFICACIÓN</th><th>TIPO DE CERTIFICADO</th></tr>
<tr><td>Sectigo (formerly Comodo)</td><td>EV SSL</td></tr>
<tr><td>Digicert</td><td>Standard SSL EV SSL</td></tr>
<tr><td>GoDaddy</td><td>EV SSL</td></tr>
<tr><td>GlobalSign</td><td>Organización SSL
Extended SSL</td></tr>
<tr><td>IdenTrust</td><td>Standard Server SSL</td></tr>
</table>

En atención a que la Entidad cuenta con herramientas tecnológicas que proveen condiciones de seguridad de manera transversal a los sistemas de información, página web y sede electrónica de la SIC, las siguientes características se consideran como opciones y no obligatorias:

• Escaneo SPAM: herramienta útil para proteger la reputación del sitio web y garantizar que los correos electrónicos enviados desde el sitio web sean legítimos y no se consideren SPAM.
• Escaneo inyección SQL: Herramienta útil para proteger los sitios web contra posibles ataques de inyección SQL y prevenir la exposición de información confidencial o la realización de acciones maliciosas en el sitio web.
• Escaneo Cross Site Scripting (XSS): Esta herramienta se utiliza para identificar vulnerabilidades en un sitio web que podrían permitir a un atacante ejecutar código malicioso en el navegador de los usuarios.
</td></tr>
<tr><td>12.</td><td>
Para los certificados de sitio seguro SSL OV Wildcard cumplir con las siguientes condiciones:

• Sello de Seguridad, que permita visualizar que el sitio está libre de malware, que se analiza periódicamente en búsqueda de vulnerabilidades, que el flujo de información entre navegador y servidor es 100% confidencial y que la identidad propietaria del sitio ha sido verificada por un tercero de confianza.
• Para lo cual se debe presentar el certificado del tercero de confianza.
• Compatibilidad con algoritmos de cifrado: RSA (2.048 bits mínimo), ECC.
</td></tr>
<tr><td></td><td>
• Verificación de la propiedad de Dominio, que permite desplegar el nombre del titular del certificado SSL en cualquier navegador.
• Activación de candado de seguridad en el navegador.
• Autenticación empresarial completa OV.
• Escaneo automático semanal en búsqueda de vulnerabilidades con reportes detallados en PDF.
• Escaneo automático diario de malware para detectar códigos maliciosos en el código fuente del sitio asegurado con el certificado SSL.
• Los certificados Web SSL OV tipo Wildcard deben ser Compatibles con algoritmos de cifrado RSA.
• Se contempla el certificado SSL Wilcard con un número ilimitado de subdominios con un solo certificado.
• Compatibilidad con SAN (URL adicionales) hasta 100 URL.
• El proveedor debe volver a generar un certificado (reemitir) en caso de que se presente una migración de servidores o daño de hardware.
• El Proveedor debe garantizar que el servicio es compatible con el estándar de seguridad PKCS (Public Key Cryptography Standards).
• Cola de Validación: Prioridad.
• Compatibilidad de Navegadores: Edge, Safari, Opera, Firefox, Chrome, navegadores basados en Chromium, todos estos en sus diferentes versiones multiplataforma
</td></tr>
</table>

13.	Los certificados de sitio seguro deben contar con el sello de Web Trust para Autoridades de Certificación, que es un sello de confianza, calidad y seguridad que se concede a las entidades prestadoras de servicios de confianza tras obtener un informe favorable de auditoría independiente, el cual constata el cumplimiento de los principios y criterios Webtrust indicados por el Instituto Americano de Auditores Públicos de Cuentas (AICPA) y el Instituto Canadiense de Auditores de Cuentas (CICA).
14.	Reemplazar los certificados de sitio seguro que se encuentren defectuosos durante la entrega y durante su vigencia, o en el caso que no cumplan con las especificaciones exigidas, en un término no superior a 24 horas, siguientes a la fecha de la comunicación efectuada por la Superintendencia de Industria y Comercio.
15.	El contratista debe describir detalladamente los procedimientos y coordinará estos procedimientos con el funcionario encargado de ejercer el control de ejecución al contrato. Debe permitirse la reemisión sin costo durante la vigencia del certificado.
16.	Si durante la ejecución del contrato o durante la vigencia del certificado emitido para la SIC con motivo de este, la respectiva autoridad de certificación es removida del listado de entidades de certificación autorizada por la IRS de FATCA, y el certificado entregado pierde su vigencia, el contratista nuevamente deberá generar y sin ningún costo para la SIC, un nuevo certificado emitido por alguna de las entidades de certificación autorizadas por la IRS de FATCA, con vigencia por el tiempo restante del inicialmente pactado
17.	Realizar jornada de transferencia de conocimiento de los procesos de generación y/o revocación de certificados de sitio seguro.
18.	Integrar alertas automáticas de expiración de certificados en la infraestructura de monitoreo (si esta aplica o se le traslada al tercero que emite o certifica).
19.	Establecer un inventario centralizado y actualizado con estado, ubicación y renovación de cada certificado (si esta actividad aplica o se le traslada al tercero que emite o certifica).
20.	Incluir dentro del documento una especificación de notificación obligatoria ante cambios en políticas de la CA o brechas de seguridad conocidas.
21.	Verificar que los certificados no permitan el uso de algoritmos inseguros como SHA-1 (deprecado / obsoleto), se entiende que al solicitar algoritmos más recientes no se deberían utilizar este tipo de funciones, sin embargo, no sobraría recomendarlo en las especificaciones.
22.	Implementar HSTS (HTTP Strict Transport Security) en todos los dominios asegurados por los certificados contratados

Adriana Cetina Hernández

Jefe Oficina de Tecnología e Informática

Proyectó: Julio César León Rojas – Contratista G. de Informática Forense y Seguridad Digital
Revisó: Magda Julieth Zarrate Saldaña - Coordinadora G. de Informática Forense y Seguridad Digital
Nelson Romero Muñoz– Contratista OTI.
Mauricio Salgado Guzman – Contratista OTI.
Aprobó: Adriana Cetina Hernández – Jefe OTI