



Recomendaciones para ser tenidas en cuenta dentro del pliego de condiciones

Teniendo en cuenta que la Entidad requiere contratar servicios de emisión, gestión y administración de certificados de firma digital, los cuales serán utilizados para la suscripción de documentos electrónicos con valor legal, actos administrativos, trámites internos y servicios digitales dirigidos a la ciudadanía y que dichos servicios involucran el tratamiento de información sensible y crítica, por lo que resulta indispensable garantizar altos estándares de seguridad de la información, confiabilidad operativa y cumplimiento normativo, en concordancia con las mejores prácticas internacionales, para ello solicitamos respetuosamente, a la Entidad considerar la inclusión dentro de los requisitos habilitantes o técnicos del proceso, la exigencia de la Certificación ISO 27001, ONAC y la Certificación Sello WebTrust.

Estas certificaciones representan estándares internacionales ampliamente reconocidos en materia de gestión de la seguridad de la información. En particular:

- ❖ **ONAC** El Organismo Nacional de Acreditación de Colombia (ONAC) es la entidad designada por el Estado colombiano para acreditar a los prestadores de servicios de certificación digital, verificando el cumplimiento de los requisitos técnicos, operativos, de seguridad y legales exigidos por la normativa vigente.

En este sentido, la acreditación ONAC constituye el mecanismo oficial de habilitación para que un proveedor pueda prestar servicios de certificación digital con plena validez jurídica frente a las entidades del Estado.

- ❖ **La norma ISO 27001** proporciona un marco robusto de buenas prácticas orientado a garantizar la confidencialidad, integridad y disponibilidad de la información. Adicionalmente:
 - Garantiza que el proveedor cuenta con controles formales y auditados para proteger la confidencialidad, integridad y disponibilidad de la información.
 - Reduce los riesgos de incidentes de seguridad, tales como accesos no autorizados, alteración de documentos electrónicos o pérdida de información.
 - Asegura la gestión sistemática de riesgos, incluyendo controles criptográficos, seguridad física, continuidad del negocio y gestión de incidentes.



- Contribuye al cumplimiento de la normativa vigente en materia de protección de datos, gobierno digital y seguridad de la información aplicable al sector público.
- ❖ **El Sello WebTrust** certifica el cumplimiento de principios y controles de seguridad, confidencialidad y privacidad en entornos digitales, fortaleciendo la confianza en los sistemas tecnológicos implementados.

Su exigencia se fundamenta en :

- Verifica que la Autoridad de Certificación cumple con controles estrictos en la emisión, administración, suspensión y revocación de certificados digitales.
- Asegura la correcta validación de identidad de los titulares de los certificados.
- Garantiza el uso adecuado de infraestructura criptográfica, claves privadas, módulos de seguridad (HSM) y políticas de certificación.
- Permite la interoperabilidad y reconocimiento internacional de los certificados emitidos.
- Minimiza el riesgo de fraude, suplantación de identidad o emisión indebida de certificados, lo cual podría comprometer la validez legal de documentos oficiales.

Dado que los certificados serán utilizados en actos administrativos y documentos con efectos jurídicos, el cumplimiento de WebTrust resulta indispensable para garantizar la confiabilidad y validez legal del servicio contratado.

Principios de Proporcionalidad y No Restricción de la Competencia

Aclaramos que la exigencia de la ISO/IEC 27001 y WebTrust no van en contra de los Principios de Proporcionalidad y No Restricción de la Competencia toda vez que:

- Se encuentran alineadas con estándares internacionales ampliamente adoptados.
- No constituyen una barrera injustificada a la competencia, dado que se trata de certificaciones directamente relacionadas con el objeto del contrato.



- Responde a criterios de razonabilidad, proporcionalidad y pertinencia técnica, considerando el impacto y criticidad del servicio.

En virtud de lo expuesto, resulta técnicamente justificado y necesario que la Entidad exija, como requisito mínimo en el proceso:

- Certificación ONAC
- Certificación vigente ISO/IEC 27001, emitida por un organismo acreditado.
- Cumplimiento del estándar WebTrust for Certification Authorities o equivalente reconocido internacionalmente.

En resumen, dicha exigencia permite a la Entidad contratar con una empresa que le garantice la seguridad, confiabilidad, validez legal y continuidad operativa de los servicios de certificación de firma digital, protegiendo los intereses tanto de la Entidad como la de los ciudadanos.

Cordialmente

GESTION DE SEGURIDAD ELECTRONICA S.A.-GSE