**CONTENIDO**

[1 OBJETIVO 2](#_Toc44660425)

[2 DESTINATARIOS 2](#_Toc44660426)

[3 GLOSARIO 2](#_Toc44660427)

[4 REFERENCIAS 3](#_Toc44660428)

[5 DESCRIPCIÓN DE ACTIVIDADES Y RESPONSABILIDADES 3](#_Toc44660429)

[6 LISTADO DE CONTRATOS APLICABLES 3](#_Toc44660430)

[7 DOCUMENTOS RELACIONADOS 4](#_Toc44660431)

[8 RESUMEN CAMBIOS 4](#_Toc44660432)

[ANEXO A. REQUISITOS DE SEGURIDAD DE REFERENCIA 4](#_Toc44660433)

[REQUISITOS GENERALES 4](#_Toc44660434)

[REQUISITOS ESPECÍFICOS. 7](#_Toc44660435)

[REQUISITOS DE SEGURIDAD PARA LA ADQUISICIÓN DE INFRAESTRUCTURA TECNOLÓGICA 7](#_Toc44660436)

[REQUISITOS DE PRIVACIDAD 8](#_Toc44660437)

# OBJETIVO

Incorporar criterios de la seguridad de información en los procesos de contratación de bienes y servicios aplicables que se adelanten en la Superintendencia de Industria y Comercio.

# DESTINATARIOS

El presente documento es de aplicación para la Superintendencia de Industria y Comercio en su proceso de adquisición de bienes y servicios, así como los procedimientos que componen el mismo, el cual debe ser conocido y aplicado por todos los funcionarios y contratistas de la Entidad.

# GLOSARIO

Para los efectos del cumplimiento del protocolo, se adoptan las siguientes definiciones:

**DOCUMENTO:** Información registrada, cualquiera que sea su forma o el medio utilizado. (Colombia. Archivo General de la Nación, (2006) Acuerdo 027 de 2006 Por el cual se modifica el Acuerdo No. 07 del 29 de junio de 1994.)

**FORMATO ELECTRÓNICO:** Representación codificada como bytes de un objeto digital, la cual define reglas sintácticas y semánticas que permiten el mapeo o correspondencia de un modelo de información a una cadena de bits y viceversa. Definición de: nterPARES. The International Research on Permanent Authentic Records in Electronic Systems. TEAM México. “Glosario InterPARES de Preservación Digital”. Versión en español “Beta” 1.2. Marzo 2010. México

**BIENES Y SERVICIOS:** Los bienes están representados en objetos materiales, cuya utilidad permite satisfacer una necesidad de un modo directo o indirecto. Los servicios están considerados en aquellos trabajos que otras personas realizan para satisfacer necesidades.

**CONTRATO:** Acuerdo de voluntades entre entidades públicas y personas naturales, jurídicas, consorcios o uniones temporales, elevado a escrito, en el que se pactan las condiciones del negocio jurídico, objeto, obligaciones, precio plazo, entre otros aspectos.

**ESTUDIO PREVIO:** Los estudios y documentos previos son el soporte para elaborar proyecto de pliegos, pliego de condiciones y el contrato.

**SOPORTE:** Medios en los cuales se contiene la información, según los materiales o medios tecnológicos empleados. El cual puede ser físico como papel, óptico, magnético o formatos electrónicos. (Colombia. Archivo General de la Nación, (2006) Acuerdo 027 de 2006 Por el cual se modifica el Acuerdo No. 07 del 29 de junio de 1994.)

**OFERENTE O PROPONENTE:** Persona natural o jurídica que presenta ofertas o propuestas de bienes o servicios.

**SGSI:** Sistema de Gestión de Seguridad de la Información.

# REFERENCIAS

En el marco legal establecido para el desarrollo del presente documento se aplica lo referenciado en las políticas de seguridad de la Superintendencia de Industria y Comercio, establecidas en el documento SC05-I01 Políticas del Sistema de Gestión de Seguridad de la Información – SGSI.

# DESCRIPCIÓN DE ACTIVIDADES Y RESPONSABILIDADES

Se deberán tener en cuenta los siguientes pasos para la incorporación de criterios de seguridad de la información en los estudios previos:

| **ETAPA** | **NOMBRE DE ETAPA** | **DESCRIPCIÓN DE LA ETAPA** |
| --- | --- | --- |
| **1** | **SOLICITUD DE INCLUSIÓN DE CRITERIOS DE SEGURIDAD DE LA INFORMACIÓN** | El jefe de cada área o el funcionario asignado deberá realizar la solicitud al correo seguridaddigital@sic.gov.co, adjuntando estudios previos y anexos para analizar la pertinencia respecto a la inclusión de criterios de seguridad y privacidad. |
| **2** | **ESTUDIO DEL OBJETO CONTRACTUAL** | Una vez allegada la solicitud, los profesionales del Grupo de Trabajo de Informática Forense y Seguridad Digital en conjunto con el Oficial de Datos Personales, estudiarán si el estudio previo remitido requiere o no inclusión de criterios de Seguridad y Privacidad. Este análisis se realiza tomando como referencia el Modelo de Seguridad y Privacidad de la Información, las políticas de Seguridad de la Información y la Política de Protección de Datos personales de la Superintendencia, al igual que de otros documentos de consulta referentes al tema de seguridad y privacidad en la adquisición de bienes o servicios.Se dará respuesta dentro de los tres (3) días hábiles siguientes a la realización de la solicitud y siguiendo los lineamientos del siguiente paso.  |
| **3** | **ELABORACIÓN DE CRITERIOS DE SEGURIDAD Y PRIVACIDAD** | Durante esta etapa se definen los criterios de seguridad y privacidad, en consecuencia el Oficial de Seguridad de la Información de la entidad en conjunto con el Oficial de Datos Personales pueden utilizar los requisitos de referencia presentados en el anexo A del presente documento, seleccionando los pertinentes según el servicio a contratar. |
| **4** | **REVISIÓN DE CRITERIOS DE SEGURIDAD Y PRIVACIDAD** | El Grupo de Trabajo de Contratación debe confirmar que los requisitos de seguridad y privacidad fueron establecidos en los estudios previos, por lo que en caso de dudas, puede escribir a seguridaddigital@sic.gov.co o al correo electrónico del Oficial de Seguridad de la Información de la entidad.Una vez se adjudique el proceso contractual, el supervisor o la persona a quien este designe deberá realizar seguimiento estricto al cumplimiento de los requisitos de seguridad y privacidad establecidos. |

# LISTADO DE CONTRATOS APLICABLES

• Fábrica o adquisición de software.

• Servicios de diseño, desarrollo, implementación y mantenimiento de sistemas de información.

• Servicios de conectividad.

• Servicios de información o centro de datos en la nube o collocation.

• Adquisición de soluciones de infraestructura tecnológica y seguridad informática.

• Servicios integrales en Tecnologías de información y comunicaciones TIC (Mesa de servicios).

• Centro de Operaciones de Red (NOC).

• Centro de Operaciones de Seguridad (SOC).

• Renovación de plataformas tecnológicas.

• Desarrollo de soluciones tecnológicas basadas en tecnologías de 4ta generación.

• Servicios de Call Center.

• Servicios de publicidad y redes sociales.

**Nota:** Cabe resaltar que si un servicio es contratado por la Entidad puede tener relacionado un riesgo de seguridad de la información, a este se le deberá incluir criterios de seguridad independientemente que no se encuentren en el listado de contratos priorizados, para lo cual es importante seguir las actividades descritas en el numeral 5 de este documento.

# DOCUMENTOS RELACIONADOS

GA01-I02 Manual de Contratación.

SC05-I01 Políticas del Sistema de Gestión de Seguridad de la Información – SGSI.

#  RESUMEN CAMBIOS

|  |
| --- |
| Creación del documento. |

# ANEXO A. REQUISITOS DE SEGURIDAD DE REFERENCIA

Los requisitos de seguridad del presente anexo, son aquellos en los que el Oficial de Datos Personales y el Oficial de seguridad de la información pueden apoyarse para la elaboración de criterios de seguridad y privacidad de que trata la etapa 3 del flujo de actividades.

###

### REQUISITOS GENERALES

* El contratista debe cumplir los lineamientos, directrices y políticas de seguridad de la información de la SIC en el ejercicio y cumplimiento de sus obligaciones contractuales.
* El contratista debe informar los cambios de personal que presta servicios para SIC. La notificación se realizará formalmente mediante correo electrónico al supervisor del contrato, dentro de 24 horas calendario de realizado el suceso. El supervisor debe verificar que el perfil cumpla con los requisitos de estudio y experiencia requeridos contractualmente.
* El contratista debe gestionar y confirmar la eliminación de los accesos del personal que sea dado de baja. Esta gestión deberá ser realizada dentro de las 24 horas de haber sucedido la salida del personal.
* Los recursos tecnológicos e Información proporcionada por la Superintendencia de Industria y Comercio deben ser usados por el contratista únicamente para los fines contratados por la Entidad. Por lo cual el contratista debe implementar los controles necesarios para mitigar los riesgos de uso no autorizado, robo, uso inadecuado, modificación accidental o no autorizada, revelación, transferencia o destrucción.
* El contratista debe permitir al personal de la SIC autorizado a realizar inspecciones de seguridad, previa autorización del supervisor del contrato; ya sea que se utilicen equipos de propiedad de la SIC, arrendados o controlados por el Contratista.
* El contratista debe presentar a la supervisión del contrato los siguientes procedimientos relacionados con su operación, los cuales deberán ser coherentes con las disposiciones legales y estándares internacionales.
* Procedimiento de devolución o destrucción de la información a la finalización del acuerdo, incluyendo la entrega de los backups de los correos electrónicos con registro de la SIC usados para la ejecución de las obligaciones contractuales.
* programa de sensibilización y capacitación en cuanto a normas de seguridad de la información con sus soportes de participación.
* Procedimiento de gestión de cambios del proveedor.
* Procedimiento de notificación y gestión de los incidentes de seguridad.
* Procedimiento de escalado en la resolución de problemas.
* Procedimiento de actualización de antivirus.
* Procedimiento de gestión de parches y actualizaciones de seguridad.
* Plan de continuidad del negocio que incluya planes de contingencia y recuperación de desastres.
* Programa Integral de Protección de Datos Personales.
* El contratista debe realizar periódicamente un ejercicio de análisis de riesgos de seguridad y privacidad de la información del servicio contratado e informar a la SIC la matriz de riesgos y los controles que ha adoptado para su prevención y mitigación.
* El contratista deberá garantizar controles de acceso a la información del servicio contratado, tales como:
* Seguridad en el acceso a documentos físicos.
* Requerimientos de control de acceso lógico.
* Implementación de redes seguras.
* Seguridad en bases de datos.
* Cuando el contratista requiera conectarse de manera remota a los recursos tecnológicos de la SIC, este debe garantizar que la transferencia de datos utilice protocolos cifrados.
* El contratista debe estar en capacidad de generar reportes basados en los registros de las transacciones y actividades realizadas en la prestación de sus servicios.
* El contratista debe contar con una política de protección de datos personales, no obstante, deberá cumplir las políticas de protección de datos de la SIC, en cuanto al manejo de documentos e información personal a la cual tenga acceso.
* El contratista debe guardar reserva y confidencialidad de la información que se le suministre o llegase a tener acceso o conocimiento, incluyendo la información relacionada con datos personales, la información pública clasificada y pública reservada, de que tratan el artículo 3 de la Ley 1581 de 2012 y el artículo 6 de la Ley 1712 de 2014 respectivamente.
* La información confidencial sólo podrá usarse para la ejecución de las obligaciones contractuales, salvo que expresamente la SIC autorice lo contrario en forma previa y escrita.
* El contratista no debe efectuar acuerdos, de naturaleza alguna con terceros que manifiesten interés en los trámites o decisiones que adelanta la SIC.
* El contratista debe salvaguardar la información a la que tenga acceso, con ocasión de su interacción con los aplicativos y servicios tecnológicos de la SIC, documentos y expedientes físicos o electrónicos, de tal forma que se asegure su confidencialidad, autenticidad, integridad, disponibilidad y privacidad.
* El contratista no debe permitir el acceso a la información confidencial, ni tampoco divulgarla por sí mismo o por tercera persona o por falta de custodia de la misma, de manera parcial o total, sin previo consentimiento por parte de la SIC. Como contratista debe contemplar las medidas de seguridad establecidas en las políticas de seguridad de la información de la Entidad.
* El contratista no debe emitir copias, modificar, comunicar, divulgar total o parcialmente a terceros, emplear indebidamente, o reproducir por cualquier medio, datos o información contenida en los aplicativos, bases de datos personales o de otra índole, sistemas de información y documentos y expedientes físicos o electrónicos, a los cuales se le haya otorgado acceso.
* Una vez concluido o terminado el contrato, por la razón que fuese, el contratista debe:
* Entregar formalmente al supervisor del contrato, las cuentas de usuario genéricas que tenga a su cargo.
* Verificar que los accesos personales otorgados a los aplicativos y servicios tecnológicos de la SIC y a las instalaciones físicas de la entidad, hayan sido efectivamente removidos y en caso de seguirlos manteniendo, debe informarlo al supervisor del contrato.
* Devolver o entregar a la SIC todos los documentos y expedientes físicos o electrónicos, bases de datos, listados y en general cualquier información recibida independientemente de su formato y no puede conservar ninguno de ellos en su poder. En caso de no poder devolver todas las copias de la información, previa autorización del supervisor del contrato, el contratista debe destruirlas o borrarlas e informar de forma escrita sobre ello.
* El contratista debe informar oportunamente al supervisor del contrato, cualquier evento o debilidad que identifique y pueda afectar la confidencialidad, integridad, disponibilidad o privacidad de la información de la SIC, a través de los canales formalmente establecidos en el procedimiento de gestión de incidentes de la Entidad.
* El contratista no debe dar lugar al acceso o exhibir expedientes, documentos o información a personas no autorizadas.

### REQUISITOS ESPECÍFICOS.

* El contratista debe presentar un documento con el resultado de las pruebas de penetración y ethical hacking del software contratado, realizado por un tercero independiente, en el cual se demuestre que software no tiene vulnerabilidades técnicas ni de seguridad.
* El contratista debe entregar documentada la arquitectura de la solución tecnológica que utiliza para la prestación del servicio así como los procesos y procedimientos administrativos para su mantenimiento.
* Todo equipo de cómputo del contratista o proveedor conectado a la red de la SIC debe mantenerse libre de virus y otros códigos dañinos de computadores, debiendo los usuarios de estos sistemas adoptar las medidas necesarias para el efecto.
* Todo equipo del contratista, proveedor o distribuidor conectado a la red de la SIC, deberá usar un software para protección de virus debidamente licenciado.
* El contratista debe contar con políticas, normas y procedimientos de seguridad de la información oficializada y divulgada hacia sus empleados, terceros y proveedores.
* El contratista debe asegurar la ejecución de controles en el acceso de dispositivos inalámbricos, equipos portátiles y/o medios de almacenamiento portátil sobre las áreas de trabajo asignadas al proyecto de la SIC.
* El contratista debe contar con un plan de contingencia y continuidad del servicio contratado, debidamente documentado y probado por lo menos una (1) vez al año. El plan de contingencia y continuidad del servicio contratado debe ser revisado por la OTI a través del supervisor del contrato.
* El contratista debe garantizar que, durante la transferencia y el almacenamiento de datos, se encuentren ilegibles las contraseñas de aplicaciones mediante criptografía sólida basada en normas aprobadas.
* El contratista debe establecer un proceso formal de respaldo de la información en formato digital o electrónico que le sea entregada, el cual sea validado y aceptado por la SIC.
* Al finalizar el vínculo contractual y previa devolución de información de la SIC, el contratista debe realizar un borrado seguro de la información, entregando las debidas evidencias al supervisor del contrato.

### REQUISITOS DE SEGURIDAD PARA LA ADQUISICIÓN DE INFRAESTRUCTURA TECNOLÓGICA

* Cumplir con las políticas de seguridad de la información de la Superintendencia de Industria y Comercio, establecidas en el documento SC05-I01 Políticas del sistema de gestión de seguridad de la información – SGSI.
* El proveedor de infraestructura, servicio de tecnología o comunicaciones debe difundir los lineamientos establecidos en el documento SC05-I01 Políticas del sistema de gestión de seguridad de la información – SGSI a todos los empleados que participen en la ejecución del contrato con la SIC.
* El proveedor de infraestructura, servicio de tecnología o comunicaciones y la SIC deben firmar un acuerdo de confidencialidad para contratos celebrados con personas naturales o un acuerdo de seguridad en la cadena de suministro para proveedores de productos y servicios para contratos celebrados con proveedores.
* El proveedor de infraestructura, servicio de tecnología o comunicaciones debe presentar resultados de pruebas de pentesting, en el cual se demuestre que el servicio de tecnología o comunicaciones adquirido no cuenta con vulnerabilidades que pueden llegar a afectar la seguridad de la información.
* Si durante el desarrollo del contrato, el proveedor de infraestructura, servicio de tecnología o comunicaciones requiere almacenar en la nube información de carácter personal a cargo de la SIC, ésta debe encontrarse en países que cuenten con los niveles adecuados de protección de datos personales, de acuerdo con los estándares definidos en la SIC.
* El servicio de tecnología o comunicaciones adquirido debe utilizar protocolos seguros para la transferencia de información, haciendo uso de algoritmos robustos de cifrado.
* El proveedor de infraestructura, servicio de tecnología o comunicaciones debe entregar los manuales de usuario y realizar las capacitaciones necesarias a los distintos tipos de usuarios para asegurar una adecuada trasferencia de conocimiento.

### REQUISITOS DE PRIVACIDAD

* El proveedor/contratista tendrá sumo cuidado para que sus actos o acciones, no se tipifiquen en una conducta descrita en la Ley 1273 de 2009, como en la Ley 1581 de 2012 acorde con el proceso objeto de la prestación del servicio a la entidad. Las partes contratantes podrán utilizar todas las acciones administrativas, civiles y penales, para resarcir daños y perjuicios que se puedan ocasionar por el mal manejo de datos e información personales o empresariales.
* Cuando en desarrollo del contrato y en el evento en el cual el proveedor/contratista realice cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión (en adelante el Tratamiento) por cuenta y bajo las instrucciones de la SIC (quien como RESPONSABLE define los medios y las finalidades de las bases de datos) debe cumplir las siguientes obligaciones como ENCARGADO DEL TRATAMIENTO:
1. Dar Tratamiento, a nombre de la SIC, a los datos personales conforme a los principios que los tutelan;
2. Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales. 3. Guardar confidencialidad respecto del tratamiento de los datos personales. En el caso de datos personales regulados por la ley 1581 de 2012 y normas reglamentarias y en virtud del principio de confidencialidad consagrado en el artículo 4º de la ley 1581 de 2012. El proveedor/contratista que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos está obligado a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma;
3. Si realiza la recolección o captura de datos personales deberá obtener, la autorización previa, expresa e informada del titular, conservar y entregar dichas autorizaciones, a la SIC;
4. Verificar que el tratamiento que va a realizar se encuentre dentro del alcance y finalidades definidos en la respectiva autorización y en la Política de Tratamiento de Datos Personales;
5. Cumplir con las finalidades, los tratamientos autorizados por el titular o por ley, los principios y en general con la normatividad que aplique en materia de protección de datos, en especial deberá dar cumplimiento a la Política de Tratamiento de Datos personales de la SIC y demás normativas internas, tales como manuales, procedimientos, entre otros;
6. El proveedor/contratista deberá tratar la información de forma diligente y asegurar que se conserve en condiciones de seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
7. Deberá verificar la calidad y veracidad de los datos objeto de tratamiento;
8. El proveedor/contratista en calidad de encargado deberá asegurar al titular que en todo momento pueda ejercer sus derechos a consultar, rectificar, actualizar o suprimir sus datos personales o a revocar la autorización conforme a los procedimientos establecidos en la Política de Tratamiento de Datos Personales de la SIC;
9. Responder directamente sobre todos los datos personales que se trate en los equipos o dispositivos que sean de propiedad de la SIC;
10. Dar uso a los datos personales exclusivamente para los fines del presente contrato;
11. Atender las indicaciones de la SIC para realizar los respectivos trámites ante el Registro Nacional de Bases de Datos;
12. Colaborar con la SIC en la debida comunicación y gestión de toda violación a códigos de seguridad y/o incidentes de los datos personales, conforme a los procedimientos internos de la SIC;
13. Dar cumplimiento con las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio;
14. Cumplir con todas las normas internas de la SIC sobre seguridad de la información, gestión documental, y en general sobre el Programa Integral de Gestión de Datos Personales;
15. Devolver a la SIC todo dato personal y toda base de datos que éste le haya entregado, tanto en medios físicos como electrónicos, y eliminar completamente cualquier registro, físicos y/o electrónicos, que contengan datos personales y/o bases de datos obtenidos en el desarrollo del presente contrato. Para tal efecto dentro de los 7 días hábiles siguientes a la terminación del contrato, el proveedor/contratista deberá remitir certificado indicando la devolución y eliminación de los datos personales objeto de tratamiento en virtud del contrato suscrito entre las partes; Queda expresamente prohibido la cesión, transferencia y/o transmisión de la información proporcionada por la SIC a el proveedor/contratista a cualquier tercero sin la debida autorización escrita por parte de la Entidad.