1. OBJETIVO

Establecer los lineamientos técnicos, administrativos y metodológicos que deben observarse en la elaboración de Estudio de Conveniencia y Oportunidad para proyectos tecnológicos en la Dirección de Tecnologías de la Información y las Comunicaciones (DTIC), con el fin de garantizar decisiones informadas, eficientes y alineadas con los principios de la contratación estatal.

2. ALCANCE

Esta guía aplica a todos los funcionarios, contratistas y equipos técnicos que participen en la formulación, planeación y estructuración de proyectos tecnológicos que requieran contratación, adquisición o desarrollo de soluciones informáticas, infraestructura tecnológica o servicios asociados. Cubre desde la identificación de la necesidad hasta la definición de criterios técnicos, financieros, jurídicos y de seguridad de la información. Este documento es un anexo complementario de la Guía de Proyectos GTI-GU-016 del Sistema de Gestión Integrado.

3. RESPONSABLES

De acuerdo con el documento GIN-PO-001 Políticas del SGI, todos los funcionarios, contratistas, terceros y proveedores que estén involucrados en proyectos que se ejecuten dentro de la Superintendencia de Sociedades tienen la responsabilidad y el deber de realizar como mínimo las actividades acá descritas para la gestión de proyectos.

4. DEFINICIONES

- **Estudio de Conveniencia y Oportunidad (ECO):** Documento técnico que soporta la necesidad de contratación y permite tomar decisiones informadas sobre la viabilidad, conveniencia y oportunidad de un proyecto.
- **Análisis Costo-Beneficio:** Evaluación comparativa entre los costos estimados y los beneficios esperados de una alternativa tecnológica.
- **Riesgo:** Evento potencial que puede afectar negativamente el cumplimiento de los objetivos del proyecto.
- **Matriz de Riesgos:** Herramienta que permite registrar, clasificar y analizar los riesgos identificados en un proyecto, incluyendo su probabilidad de ocurrencia, impacto, controles existentes y responsables de seguimiento.
- **SAST/DAST:** Pruebas de seguridad de aplicaciones estáticas (Static Application Security Testing) y dinámicas (Dynamic Application Security Testing).
- **SLA** (Service Level Agreement): Acuerdo de nivel de servicio (ANS) que define métricas de disponibilidad, tiempos de respuesta y compromisos del proveedor.

Verifique que este documento corresponda a la versión vigente antes de su uso

- **Gestión de riesgos:** Consiste en identificar, evaluar y tratar los riesgos e incertidumbres a los que se enfrentan todos los proyectos. Estos riesgos también pueden convertirse en oportunidades.

5. CONTENIDO

1. Roles Clave en la Construcción y Revisión de Estudios de Conveniencia y Oportunidad

Los siguientes actores institucionales son responsables de participar en la construcción, revisión y validación de los estudios de conveniencia y oportunidad para proyectos tecnológicos:

- **Grupo de Proyectos de Tecnología**: Coordinación de la elaboración del Estudio de Conveniencia y Oportunidad, articulación con áreas técnicas y validación documental.
- **Supervisores designados**: Acompañamiento técnico y funcional desde la planeación.
- **Oficina Asesora de Planeación**: Revisión metodológica y alineación con el Sistema de Gestión Integrado.
- **Oficina de Seguridad Informática y Forense**: Validación de requisitos de seguridad de la información y gestión de riesgos tecnológicos.

2. Marco Normativo

La elaboración de estudios de conveniencia y oportunidad debe observar los siguientes referentes normativos y técnicos:

- **Ley 80 de 1993**: Artículos 25 y 29, que establecen los principios de planeación, economía y responsabilidad en la contratación pública.
- **Decreto 1082 de 2015**: Artículo 2.2.1.1.2.1.1, que define los elementos mínimos que deben contener los estudios previos.
- **Norma ISO/IEC 27001:2022**: En especial el control A.8.30 sobre desarrollo subcontratado, aplicable a proyectos que involucren software o servicios tecnológicos.
- **Guía GTI-GU-016**: Documento institucional que establece las buenas prácticas para la gestión de proyectos en la Superintendencia de Sociedades. Este documento puede ser consultado en el Sistema de Gestión Integrado.

3. Elementos Mínimos del Estudio Previo

3.1. Justificación del Proyecto

- Identificación clara del problema o necesidad que se busca resolver.
- Contexto institucional que respalde la iniciativa.

Verifique que este documento corresponda a la versión vigente antes de su uso

- Alineación con los objetivos estratégicos de la entidad.
- Impacto esperado en términos de eficiencia operativa, mejora del servicio, cumplimiento normativo o fortalecimiento institucional.

3.2. Objetivos

- Definición precisa de los objetivos del proyecto.
- Establecimiento de metas medibles, alcanzables y verificables.
- Relación directa entre los objetivos y los beneficios esperados.

3.3. Análisis de Alternativas

- Evaluación de diferentes opciones técnicas, funcionales y operativas.
- Comparación entre soluciones existentes, modernización de sistemas o adquisición de nuevas tecnologías.
- Justificación de la alternativa seleccionada con base en criterios de eficiencia, sostenibilidad, escalabilidad y alineación estratégica.

3.4. Análisis Costo-Beneficio

- Estimación de costos directos (adquisición, implementación, mantenimiento) e indirectos (capacitación, soporte, gestión del cambio).
- Identificación de beneficios tangibles (reducción de tiempos, ahorro de recursos) e intangibles (mejora en la experiencia del usuario, fortalecimiento institucional).
- Evaluación del retorno de inversión (ROI), impacto presupuestal y sostenibilidad financiera.

3.5. Procedimiento en caso de cambio de una herramienta tecnológica licenciada a perpetuidad.

Objetivo: Definir el proceso para evaluar y ejecutar el reemplazo de una herramienta tecnológica con licencia perpetua, garantizando la continuidad del servicio, la optimización de costos y la alineación con los objetivos estratégicos.

3.5.1. Verificación del estado de la herramienta:

- **Revisión de obsolescencia:**
  - Consultar la hoja de ruta del fabricante (roadmap) y fechas de fin de soporte (EoL/EoS).
  - Validar compatibilidad con sistemas operativos, bases de datos y arquitecturas actuales.
  - Confirmar cumplimiento de estándares de seguridad vigentes (ISO/IEC 27001, SOC 2).
- **Evaluación funcional:**

Verifique que este documento corresponda a la versión vigente antes de su uso

- Determinar si la herramienta sigue cubriendo los requerimientos del negocio.
- Identificar limitaciones frente a nuevas necesidades (escalabilidad, integración, automatización).

3.5.2. Análisis comparativo

Elaborar un cuadro comparativo entre la herramienta actual y las alternativas disponibles, incluyendo:

Criterio	Herramienta Actual	Alternativa A	Alternativa B
Costo Total (TCO)	$XX.XXX (mantenimiento, soporte)	$XX.XXX (suscripción anual)	$XX.XXX
Modelo de Licenciamiento	Perpetuo	SaaS	On-Premise
Ventajas	Sin pagos recurrentes	Actualizaciones automáticas	Control total
Desventajas	Riesgo de obsolescencia	Dependencia del proveedor	Costos iniciales altos
Cumplimiento Normativo	Parcial	Total	Total
Escalabilidad	Limitada	Alta	Media

3.5.3. Evaluación de costos y beneficios

- **Costos directos**: Migración, capacitación, licencias nuevas.
- **Costos indirectos**: Impacto en procesos, gestión del cambio.
- **Beneficios esperados**:
  - ✓ Mejora en seguridad, reducción de riesgos, optimización operativa.
  - ✓ Calcular **ROI** y **costo total de propiedad (TCO)** para cada alternativa.

4. Plan de transición

- Definir cronograma de migración.
- Establecer mecanismos de reversibilidad (exportación de datos, formatos abiertos).
- Garantizar continuidad del servicio durante el cambio.
- Validar pruebas funcionales y de seguridad antes de la puesta en producción.

5. Documentación y aprobación

- Incluir análisis en el Estudio de Conveniencia y Oportunidad.
- Adjuntar cuadro comparativo, matriz de riesgos y plan de transición.
- Obtener aprobación del Comité Técnico y del área jurídica.

Verifique que este documento corresponda a la versión vigente antes de su uso

5.1. Identificación de Riesgos

- Elaboración de una matriz de riesgos desde la etapa de planeación.
- Identificación de riesgos técnicos, operativos, jurídicos, financieros, contractuales y de seguridad de la información.
- Propuesta de controles, medidas de mitigación y responsables de seguimiento.
- Consideración de riesgos asociados a la subcontratación, interoperabilidad, continuidad del servicio y protección de datos.

5.2. Entregables y Criterios de Aceptación

- Identificación clara de los productos, servicios o resultados que se esperan obtener con el proyecto.
- Definición de criterios técnicos, funcionales y de calidad que deben cumplirse para considerar un entregable como aceptado.
- Relación directa entre los entregables y el plan de pagos, asegurando que cada desembolso esté condicionado a la verificación de cumplimiento.
- Inclusión de mecanismos de validación técnica, funcional y de seguridad antes de la puesta en producción.

5.3. Supervisión Técnica y Funcional

- Designación propuesta de supervisores desde la etapa de planeación del proyecto.
- Definición de funciones específicas para la supervisión técnica (infraestructura, sistemas, arquitectura, seguridad, integraciones, etc.) y funcional (cumplimiento de requerimientos, experiencia de usuario, integración con procesos, pruebas, etc.).
- Establecimiento de mecanismos de seguimiento, control y reporte periódico.
- Coordinación entre supervisores, contratistas y áreas usuarias para garantizar la trazabilidad de decisiones y entregables.

5.4. Requisitos de Seguridad de la Información

- Aplicación de los principios de confidencialidad, integridad y disponibilidad en todo el ciclo de vida del proyecto.
- Inclusión de controles mínimos como autenticación segura, cifrado, gestión de accesos, respaldo y recuperación ante desastres.
- Ejecución de pruebas de seguridad SAST y DAST antes de la aceptación final.
- Validación de cumplimiento de la política de seguridad de la información institucional y de la norma ISO/IEC 27001:2022.

Verifique que este documento corresponda a la versión vigente antes de su uso

- Gestión de cuentas temporales y eliminación segura de accesos al finalizar el contrato.

5.5. Requisitos Contractuales

- Inclusión de cláusulas que garanticen la cesión de derechos patrimoniales de autor sobre el software desarrollado.
- Prohibición de subcontratación sin autorización previa, escrita y justificada.
- Definición de acuerdos de nivel de servicio (SLA) que incluyan métricas de disponibilidad, tiempos de respuesta, mantenimiento, compensaciones y penalidades.
- Establecimiento de un plan de reversibilidad de la información en caso de terminación del contrato.
- Requisitos de certificación en seguridad (ISO 27001, SOC 2) para proveedores de servicios SaaS.

6. Documentos de Referencia para Contratación

Con el fin de garantizar la seguridad de la información y el cumplimiento normativo en los procesos de contratación relacionados con desarrollo de software y servicios tecnológicos, se deberán observar los siguientes lineamientos:

- **Cumplimiento Normativo y Protección de Datos:**
  Incluir cláusulas que aseguren el cumplimiento de la Ley 1581 de 2012, Decreto 1377 de 2013 y demás normas aplicables en materia de protección de datos personales. *(Ver Anexo 1 y 2)*
- **Confidencialidad y Derechos de Autor:**
  Establecer acuerdos de confidencialidad para todo el personal involucrado y la cesión expresa de derechos patrimoniales de autor sobre el software desarrollado, conforme a la Ley 23 de 1982. *(Ver Anexo 1 y 2)*
- **Restricción de Subcontratación:**
  Prohibir la subcontratación sin autorización previa, escrita y justificada. *(Ver Anexo 1 y 2)*
- **Seguridad de la Información:**
  Exigir la implementación de controles mínimos (autenticación segura, cifrado, control de accesos, respaldo) y la ejecución de pruebas de seguridad SAST y DAST antes de la aceptación final.
- **Certificación y Auditoría:**
  Para proveedores SaaS, solicitar certificación ISO/IEC 27001 vigente o informe SOC 2 Tipo II. Incluir derecho a auditoría técnica y revisiones periódicas. *(Ver Anexo 3)*

- **Acuerdos de Nivel de Servicio (SLA):**
  Definir métricas de disponibilidad, tiempos de respuesta, procedimientos de mantenimiento y compensaciones por incumplimiento. *(Ver Anexo 3)*
- **Plan de Reversibilidad de Datos:**
  Garantizar la entrega completa de datos en formatos interoperables y la eliminación segura al finalizar el contrato. *(Ver Anexo 3)*

7. Buenas Prácticas para la Elaboración

- Utilizar los formatos institucionales vigentes para garantizar la estandarización y trazabilidad.
- Documentar todas las decisiones técnicas, funcionales y administrativas tomadas durante la formulación del estudio previo.
- Incluir evidencia de análisis, validaciones, consultas y revisiones realizadas.
- Asegurar la trazabilidad de los entregables, compromisos y responsables.
- Promover la participación activa de los interesados desde la etapa de formulación, incluyendo usuarios finales, supervisores y áreas técnicas.
- Validar el cumplimiento normativo y técnico antes de la publicación del estudio previo.

8. Formatos y Anexos Sugeridos

- Matriz de riesgos: Documento que identifica, clasifica y propone controles para los riesgos del proyecto.
- Análisis costo-beneficio: Plantilla que permite comparar alternativas y justificar la decisión tomada.
- Criterios de aceptación técnica: Documento que define los parámetros mínimos para validar entregables.
- Modelos de cláusulas contractuales: Textos sugeridos para incluir en contratos con personas naturales, jurídicas o proveedores SaaS.
- Repositorio documental: Ruta en SharePoint o sistema institucional donde se debe almacenar toda la documentación del proyecto, organizada por etapas.

9. Línea Base de Requisitos de Seguridad de la Información para la Gestión de Proyectos (NTC ISO/IEC 27001:2022)

En el marco del Sistema de Gestión de Seguridad de la Información (SGSI) y en cumplimiento de la Norma NTC ISO/IEC 27001:2022, **esta sección contempla los controles aplicables a la gestión de proyectos para garantizar la seguridad de la información y el cumplimiento normativo**. Se da cumplimiento al control **5.8 Seguridad de la Información en la Gestión de Proyectos** *(Ver Anexo 4 y 5)*, integrando obligaciones, criterios y mecanismos que aseguren la protección de los activos de información desde la concepción, planeación, ejecución y cierre de cada iniciativa.

Verifique que este documento corresponda a la versión vigente antes de su uso

Adicionalmente, se incorporan los requisitos derivados de otros controles del Anexo A de la norma, especialmente aquellos relacionados con terceros, servicios tecnológicos y entornos técnicos:

- 5.19 – Seguridad de la información en las relaciones con proveedores, que establece las obligaciones de evaluación, selección y gestión de proveedores que participan en los proyectos. *(Ver Anexo 6)*
- 5.20 – Seguridad de la información en acuerdos con proveedores, que exige incluir cláusulas contractuales específicas de seguridad de la información en los contratos y acuerdos suscritos para el desarrollo del proyecto. *(Ver Anexo 7)*
- 5.21 – Seguridad de la información en la cadena de suministro, orientado a gestionar los riesgos derivados de la participación de subcontratistas, aliados o terceros vinculados a los servicios o productos del proyecto. *(Ver Anexo 8)*
- 5.22 – Seguimiento, revisión y gestión del cambio de los servicios de los proveedores, que exige evaluar de manera continua el desempeño, cambios y niveles de cumplimiento de seguridad de los proveedores vinculados al proyecto. *(Ver Anexo 9)*
- 5.23 – Seguridad de la información para el uso de servicios en la nube, aplicable cuando los proyectos utilicen ambientes cloud (IaaS, PaaS, SaaS), involucren plataformas externas o requieran la interacción con infraestructura tecnológica provista por terceros. *(Ver Anexo 10)*

Asimismo, se integran controles del Dominio 8 (Controles Tecnológicos) indispensables para la correcta gestión técnica en los proyectos:

- 8.21 – Seguridad de los servicios de red, que establece la necesidad de asegurar los mecanismos, configuraciones y niveles de servicio de la red involucrada en el proyecto. *(Ver Anexo 11)*
- 8.26 – Requisitos de seguridad de las aplicaciones, necesario para proyectos que desarrollen, adquieran o modifiquen aplicaciones, plataformas o servicios tecnológicos. *(Ver Anexo 12)*

De esta manera, esta sección se consolida como un instrumento transversal que unifica los requisitos mínimos de seguridad que deben considerarse en la formulación, contratación, ejecución y supervisión de proyectos institucionales, asegurando confidencialidad, integridad y disponibilidad, así como el cumplimiento de políticas internas y normatividad vigente sobre gestión de riesgos, protección de datos personales, continuidad del negocio y seguridad digital.

Finalidad:

- Integrar la seguridad de la información en todo el ciclo de vida de los proyectos (planificación, ejecución, seguimiento y cierre).
- Asegurar la alineación con las Políticas de Seguridad y Privacidad del SGSI (GIN-PO-003), el Documento de Políticas del SGI (GIN-PO-001) y la Política de Tratamiento de Datos Personales (GIN-PO-002).

- Articular la gestión de proyectos con los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI, definidos por la Resolución 500 de 2021 y actualizados por la Resolución 2277 de 2025.

10. Anexos

- Anexo 1: Cláusulas contractuales para la contratación de persona jurídica para desarrollo de software.
- Anexo 2: Cláusulas contractuales para la contratación de persona natural para desarrollo de software.
- Anexo 3: Contrato de prestación de servicios de Software como Servicio (SaaS).
- Anexo 4: Implementación del Control 5.8 "Seguridad de la Información en la Gestión de Proyectos" – NTC ISO/IEC 27001:2022"
- Anexo 5: Línea Base de Requisitos de Seguridad de la Información para la Gestión de Proyectos (Control 5.8)
- Anexo 6: Implementación del Control 5.19 - Seguridad de la información en las relaciones con proveedores ISO/IEC 27001:2022 – Control 5.19
- Anexo 7: Abordar la seguridad de la información dentro de los acuerdos con proveedores - ISO/IEC 27001:2022 – Control 5.20
- Anexo 8: Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC). - ISO/IEC 27001:2022, Control 5.20
- Anexo 9 Seguimiento, revisión y gestión del cambio de los servicios de los proveedores - ISO/IEC 27001:2022 – Control 5.22
- Anexo 10: Seguridad de la información para el uso de servicios en la nube - ISO/IEC 27001:2022 – Control 5.23
- Anexo 11: Seguridad de los servicios de red - ISO/IEC 27001:2022 – Control 8.21
- Anexo 12: Requisitos de seguridad de las aplicaciones - ISO/IEC 27001:2022 – Control 8.26

1. CONTROL DE CAMBIOS

Versión	Fecha	Descripción del Cambio
001	23/12/2025	Guía Complementaria para la Construcción de Estudio de Conveniencia y Oportunidad para la DTIC

Verifique que este documento corresponda a la versión vigente antes de su uso

Elaboró	Revisó	Aprobó
Nombre: Cristian Camilo Navarro Ballestas Cargo: Profesional universitario – Grupo de Proyectos de Tecnología. Fecha: 11 de noviembre de 2025	Nombre: María José Rosales López Cargo: Coordinadora Grupo de Proyectos de Tecnología Fecha: 12 de noviembre de 2025	Nombre: Ricardo Ríos Rosales Cargo: Director de Tecnología de la Información y las Comunicaciones Fecha: 23 de diciembre de 2025

Verifique que este documento corresponda a la versión vigente antes de su uso

10.1. Anexo 1

Cláusulas Contractuales para la Contratación de Persona Jurídica para Desarrollo de Software

Cláusula 1: Cumplimiento de Requisitos Legales y Protección de Datos Personales

a) De conformidad con la Ley 1581 de 2012 y el Decreto 1377 de 2013, el CONTRATISTA garantizará que todo tratamiento de datos personales realizado en el marco del presente contrato cumpla con los principios de confidencialidad, máxima reserva y protección establecidos por LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES.

b) El CONTRATISTA adoptará e implementará medidas técnicas, humanas y administrativas que garanticen la seguridad de los datos tratados, incluyendo autenticación segura, cifrado y control de accesos.

c) El CONTRATISTA, identificado como encargado del tratamiento de datos en el contrato o su anexo, se compromete a:

d) Usar los datos exclusivamente para los fines definidos por LA SUPERINTENDENCIA DE SOCIEDADES.

e) Abstenerse de divulgar, transferir o usar los datos para fines distintos a los establecidos.

f) Devolver o eliminar los datos tratados al finalizar el contrato, conforme al principio de finalidad.

g) Permitir auditorías y verificaciones por parte del Oficial de Protección de Datos o del Oficial de Seguridad de la Información de LA SUPERINTENDENCIA DE SOCIEDADES cuando se considere conveniente.

h) El incumplimiento de esta cláusula será considerado causal de terminación del contrato y dará lugar a las sanciones previstas en la normativa aplicable.

Cláusula 2: Acuerdos de Confidencialidad

a) Todo el personal del CONTRATISTA que participe en el desarrollo del software firmará un acuerdo de confidencialidad individual, cubriendo información institucional, técnica, operativa, jurídica, financiera y cualquier dato reservado, protegido o clasificado.

Verifique que este documento corresponda a la versión vigente antes de su uso

b) La obligación de confidencialidad será de carácter residual y permanecerá vigente incluso después de la terminación del contrato.

c) El CONTRATISTA será responsable de cualquier violación de confidencialidad por parte de su personal o subcontratistas autorizados.

Cláusula 3: Derechos de Autor y Propiedad Intelectual

a) De acuerdo con la Ley 23 de 1982, el CONTRATISTA cede de manera expresa, por escrito y a título gratuito u oneroso, según lo acordado, los derechos patrimoniales de autor sobre el software desarrollado, incluyendo código fuente, documentación técnica, APIs, modelos de datos, librerías y en general todos los productos desarrollados relacionados con el objeto contractual.

b) La cesión de derechos aplicará durante todo el tiempo de protección legal del software.

c) El CONTRATISTA no podrá registrar, reutilizar ni sublicenciar el software o sus componentes sin autorización previa y escrita de LA SUPERINTENDENCIA DE SOCIEDADES.

d) El CONTRATISTA entregará el código fuente completo en un repositorio institucional o medio seguro acordado, validado por el equipo técnico de LA SUPERINTENDENCIA DE SOCIEDADES antes de la liberación del pago final.

Cláusula 4: Restricción a la Subcontratación

a) El CONTRATISTA no podrá subcontratar total o parcialmente las actividades objeto del contrato sin autorización previa, escrita y justificada de LA SUPERINTENDENCIA DE SOCIEDADES.

b) En caso de autorización, los subcontratistas cumplirán con los mismos requisitos legales, técnicos y de seguridad exigidos al CONTRATISTA, incluyendo la firma de acuerdos de confidencialidad y el cumplimiento de la normativa de protección de datos y de seguridad de la información.

c) El CONTRATISTA será responsable solidario por cualquier incumplimiento de los subcontratistas

Cláusula 5: Seguridad de la Información

a) El CONTRATISTA cumplirá con la Política de Seguridad de la Información de LA SUPERINTENDENCIA DE SOCIEDADES, garantizando los principios de confidencialidad, integridad y disponibilidad en el manejo de la información institucional.

b) El CONTRATISTA implementará controles mínimos de seguridad, incluyendo autenticación segura, cifrado, control de accesos y respaldo de información.

c) El CONTRATISTA reportará de inmediato a la Mesa de Ayuda y al Oficial de Seguridad de la Información cualquier incidente de seguridad, incluyendo análisis de causa raíz y acciones correctivas.

d) El CONTRATISTA entregará evidencias de pruebas de seguridad realizadas al software de tipo SAST (Pruebas de Seguridad de Aplicaciones Estáticas) y DAST (Pruebas de Seguridad de Aplicaciones Dinámicas) las cuales pueden se desarrolladas por medio de herramientas libres o licenciadas, incluyendo informes firmados con resultados de pruebas y re-tests.

Cláusula 6: Requisitos Técnicos del Desarrollo

a) El CONTRATISTA garantizará la separación de ambientes de desarrollo, pruebas y producción, prohibiendo realizar pruebas en ambientes productivos y ajustándose al procedimiento de control de cambios institucional.

b) El desarrollo del software seguirá buenas prácticas de desarrollo seguro, incluyendo el cumplimiento de los principios de OWASP Top 10 y la Resolución 1519 de 2020.

c) El CONTRATISTA entregará documentación completa, incluyendo:

   i. Manual técnico (arquitectura, librerías, dependencias, APIs).

   ii. Manual de usuario (flujos, pantallas, accesos, roles).

   iii. Arquitectura de solución.

   iv. Resultados de pruebas realizadas.

d) LA SUPERINTENDENCIA DE SOCIEDADES podrá realizar auditorías técnicas al software y al proceso de desarrollo, sin

Cláusula 7: Gestión de Accesos y Cuentas Temporales

a) El CONTRATISTA gestionará cuentas con roles mínimos necesarios y vigencia definida para el acceso a información institucional.

b) Los accesos serán registrados y monitoreados por la Oficina de Seguridad de Seguridad Informática y Forense y el Grupo de Sistemas y Arquitectura de Tecnología de LA SUPERINTENDENCIA DE SOCIEDADES

c) Al finalizar el contrato, el CONTRATISTA garantizará la eliminación inmediata de todas las cuentas y accesos, preferiblemente mediante procesos automatizados y deberá ser validado por medio de la Oficina de Seguridad Informática y forense y el Grupo de Sistemas y Arquitectura de Tecnología

Cláusula 8: Pruebas y Aceptación

a) El CONTRATISTA diseñará, en conjunto con LA SUPERINTENDENCIA DE SOCIEDADES, un plan de pruebas funcionales, de seguridad y de aceptación, asegurando trazabilidad entre requisitos y resultados.

b) La aceptación del software estará sujeta a la firma de un acta de aceptación técnica y de seguridad por parte de LA SUPERINTENDENCIA DE SOCIEDADES.

c) Los entregables serán revisados como condición para la liberación de pagos.

Cláusula 9: Cumplimiento y Supervisión

a) LA SUPERINTENDENCIA DE SOCIEDADES realizará supervisión contractual permanente para verificar el cumplimiento de los requisitos normativos y técnicos.

b) La Oficina de Seguridad de Seguridad Informática y Forense revisará los entregables y registrará hallazgos o desviaciones en el marco del Sistema de la Seguridad de la Información.

c) En caso de incumplimiento, el CONTRATISTA aplicará medidas correctivas inmediatas, sujetas a la aprobación de LA SUPERINTENDENCIA DE SOCIEDADES.

Cláusula 10: Auditoría Técnica

a) La SUPERINTENDENCIA DE SOCIEDADES podrá realizar auditorías técnicas sin previo aviso al CONTRATISTA, incluyendo revisiones de código, pruebas e infraestructura utilizada para el desarrollo.

b) El CONTRATISTA facilitará el acceso a toda la información y recursos necesarios para dichas auditorías, garantizando el cumplimiento de los controles establecidos.

Verifique que este documento corresponda a la versión vigente antes de su uso

10.2. Anexo 2

CLÁUSULAS CONTRACTUALES PARA LA CONTRATACIÓN DE PERSONA NATURAL PARA EL DESARROLLO DE SOFTWARE

PRIMERA – Cumplimiento Normativo y Protección de Datos Personales
El CONTRATISTA, en calidad de persona natural, se obliga a dar estricto cumplimiento a lo dispuesto en la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás normas aplicables en materia de protección de datos personales. En caso de acceder a datos personales de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES, actuará como Encargado del Tratamiento, debiendo:

a) Utilizar dichos datos exclusivamente para el desarrollo de las actividades contratadas.
b) Abstenerse de divulgarlos, transferirlos o utilizarlos para fines distintos a los previstos en este contrato.
c) Adoptar las medidas normativas, técnicas y administrativas para su protección, incluyendo autenticación segura, cifrado y control de accesos y lo relacionado en las políticas y documentos vigentes que hagan parte del Sistema de Gestión Integrado (SGI).
d) Proceder a la eliminación de los datos o devolución de los datos según corresponda, una vez finalizada la relación contractual.
e) El incumplimiento de lo aquí pactado será causal de terminación inmediata del contrato, sin perjuicio de las acciones legales pertinentes.

SEGUNDA – Confidencialidad
El CONTRATISTA suscribirá un Acuerdo de Confidencialidad que cubrirá toda la información institucional, técnica, operativa, jurídica, financiera o clasificada a la que tenga acceso en virtud del presente contrato. La obligación de confidencialidad tendrá vigencia indefinida, incluso después de la terminación del vínculo contractual. El CONTRATISTA será responsable por cualquier vulneración a esta obligación derivada de su conducta dolosa o culposa.

TERCERA – Derechos de Autor y Propiedad Intelectual
En cumplimiento de la Ley 23 de 1982 y demás normas aplicables, el CONTRATISTA cede de manera total, exclusiva, expresa e irrevocable a favor de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES todos los derechos patrimoniales sobre el software, código fuente, librerías, documentación técnica, APIs, modelos de datos y demás componentes desarrollados en ejecución del presente contrato, por todo el tiempo de protección legal.
El CONTRATISTA no podrá registrar, reutilizar ni sublicenciar el software o cualquiera de sus partes sin autorización previa y escrita de la Entidad. La entrega del código fuente completo en el repositorio institucional será requisito indispensable para el pago final.

CUARTA – Prohibición de Subcontratación

Verifique que este documento corresponda a la versión vigente antes de su uso

El CONTRATISTA no podrá delegar, transferir o subcontratar total o parcialmente las obligaciones contractuales, salvo autorización previa, escrita y motivada de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES. En caso de ser autorizada, el subcontratista deberá cumplir las mismas obligaciones legales, técnicas y de seguridad aquí pactadas.

QUINTA – Seguridad de la Información

El CONTRATISTA deberá dar estricto cumplimiento a la Política de Seguridad de la Información de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES, garantizando la **confidencialidad, integridad y disponibilidad** de la información que procese, almacene o transmita. Deberá:

a) Implementar controles mínimos como autenticación segura, cifrado, control de accesos y respaldo de información.
b) Reportar de forma inmediata cualquier incidente de seguridad a la Mesa de Ayuda y al Oficial de Seguridad de la Información.
c) El CONTRATISTA se compromete a adoptar y cumplir rigurosamente los requerimientos de seguridad establecidos en la metodología de desarrollo de software definida por LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES, incluyendo, pero no limitándose a, las mejores prácticas de desarrollo seguro como OWASP Top 10, directrices de la Resolución 1519 de 2020 y estándares internacionales aplicables (ISO/IEC 27001).
d) El CONTRATISTA acatará los lineamientos, directrices y políticas emitidos por el Equipo de Seguridad Informática y Forense o el Oficial de Seguridad de la Información de LA SUPERINTENDENCIA DE SOCIEDADES, incluyendo aquellos que surjan por actualizaciones, modificaciones o necesidades identificadas en respuesta a riesgos específicos, boletines de seguridad emitidos por el COLCERT, el CSIRT Nacional, o cualquier otra entidad reconocida nacional o internacionalmente.
e) En caso de alertas de seguridad, vulnerabilidades críticas o boletines emitidos por dichas entidades, el CONTRATISTA deberá implementar de manera inmediata las medidas correctivas o preventivas indicadas por el Oficial de Seguridad de la Información, incluyendo parches, actualizaciones o ajustes al software desarrollado.
f) El incumplimiento de los lineamientos de seguridad o la falta de respuesta oportuna a los requerimientos del Equipo de Seguridad Informática y Forense será considerada causal de terminación del contrato y podrá derivar en sanciones conforme a la normativa aplicable.

SEXTA – Requisitos Técnicos del Desarrollo

El CONTRATISTA desarrollará el software observando buenas prácticas de programación segura y conforme a los lineamientos del OWASP Top 10 y la Resolución 1519 de 2020. Mantendrá ambientes de desarrollo, pruebas y producción separados, y no realizará pruebas sobre ambientes productivos. Deberá entregar:

a. Manual técnico de arquitectura, librerías y dependencias.
b. Manual de usuario con flujos, accesos y roles.
c. Documentación de pruebas funcionales y de seguridad realizadas.

SÉPTIMA – Gestión de Accesos
El CONTRATISTA utilizará exclusivamente credenciales temporales con privilegios mínimos, asignadas por la Dirección de Tecnologías de la Información y las Comunicaciones de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES, para acceder a los sistemas y recursos institucionales necesarios para la ejecución del contrato. Estas credenciales estarán sujetas a monitoreo continuo y tendrán una vigencia limitada al período estrictamente necesario para el cumplimiento de las actividades contratadas. Al finalizar el contrato, la Dirección de Tecnologías de la Información y las Comunicaciones garantizará la eliminación inmediata y segura de todas las cuentas, accesos y permisos otorgados al CONTRATISTA, implementando, preferiblemente, procesos automatizados para asegurar la revocación completa y prevenir accesos no autorizados posteriores.

OCTAVA – Pruebas y Aceptación
La entrega y aceptación del software estará condicionada a la aprobación de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES, mediante la firma del Acta de Aceptación Técnica y de Seguridad, previa validación de todos los requisitos contractuales y técnicos.

NOVENA – Supervisión y Cumplimiento
LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES realizará seguimiento permanente a la ejecución del contrato. El incumplimiento de cualquiera de las obligaciones aquí pactadas facultará a la Entidad para aplicar las sanciones previstas en la normatividad vigente y en este contrato.

DÉCIMA – Auditoría Técnica
LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES podrá realizar auditorías técnicas en cualquier momento, sin previo aviso, a los desarrollos y procesos del CONTRATISTA, quien deberá facilitar el acceso a la información y medios requeridos para verificar el cumplimiento de las obligaciones contractuales.

Verifique que este documento corresponda a la versión vigente antes de su uso

10.3. Anexo 3

Contrato de Prestación de Servicios de Software como Servicio (SaaS)

Cláusula 1: Cumplimiento Normativo y Certificación ISO 27001

a) EL PROVEEDOR declara y garantiza que sus procesos, infraestructura y operaciones cumplen con la norma ISO/IEC 27001, así como con la Ley 1581 de 2012 y el Decreto 1377 de 2013 de Colombia, en materia de protección de datos personales.
b) EL PROVEEDOR entregará a LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES, como parte de los anexos del contrato, una copia vigente de su certificación ISO/IEC 27001 o un informe SOC 2 Tipo II, emitido por una entidad auditora independiente, legalmente constituida, con una trayectoria mínima de tres (3) años en el mercado al momento de la emisión del informe. Dicho informe estará acompañado de la documentación oficial que acredite la existencia legal y la capacidad técnica de la entidad auditora, así como el cumplimiento efectivo de los controles de seguridad de la información establecidos en la norma correspondiente. EL PROVEEDOR garantizará que la certificación o informe se mantenga vigente durante toda la duración del contrato y notificará a LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES, dentro de las 24 horas siguientes, cualquier cambio, suspensión o revocación de la certificación o informe. Adicionalmente, EL PROVEEDOR proporcionará, a solicitud de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES, evidencia complementaria, como reportes de auditorías internas o evaluaciones de terceros, que demuestren la implementación continua y efectiva de los controles de seguridad.

Cláusula 2: Ubicación Geográfica de los Datos y Tratamiento Transfronterizo

a) EL PROVEEDOR garantiza que los datos de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES serán almacenados y procesados exclusivamente en (ubicación geográfica acordada, ej. servidores ubicados en la Unión Europea o Colombia), salvo autorización previa y escrita de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES para cualquier tratamiento transfronterizo.
b) 2.2. En caso de tratamiento transfronterizo, EL PROVEEDOR cumplirá con las normativas aplicables, incluyendo la Ley de Protección de Datos y documentos internos relacionados con Seguridad de la Información, si los datos se procesan en la Unión Europea, y garantizará la implementación de medidas de seguridad equivalentes a las exigidas por la legislación colombiana.
c) EL PROVEEDOR proporcionará un inventario detallado de las ubicaciones de los centros de datos y subprocesadores involucrados, actualizado al menos semestralmente o ante cualquier cambio.

Cláusula 3: Copias de Seguridad, Recuperación ante Desastres y Retención de Datos

a) EL PROVEEDOR implementará un plan de copias de seguridad automatizadas, con una frecuencia mínima de (especificar, ej: Diaria, Semanal, mensual, etc),

Verifique que este documento corresponda a la versión vigente antes de su uso

asegurando que las copias sean cifradas y almacenadas en ubicaciones seguras y redundantes.

b) EL PROVEEDOR garantizará un plan de recuperación ante desastres (DRP) que permita la restauración del servicio en un tiempo máximo de (especificar, acorde al a criticidad del servicio ej: 4 horas) y un punto de recuperación objetivo (RPO) de (especificar, ej: 15 minutos).

c) Los datos de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES serán retenidos únicamente durante el período necesario para cumplir con los fines del contrato o según lo exija la normativa aplicable, y serán eliminados de forma segura al finalizar el contrato, salvo que se acuerde lo contrario, en caso de que se requiera la eliminación EL PROVEEDOR deberá certificar el borrado total de la información, incluyendo las copias de seguridad existentes.

d) EL PROVEEDOR entregará a LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES un informe sobre la ejecución de copias de seguridad y pruebas de recuperación ante desastres (especificar, la periodicidad ej: mensual, trimestral, semestral, etc).

Cláusula 4: Cifrado de Datos

a) EL PROVEEDOR garantizará que todos los datos de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES, tanto en tránsito como en reposo, estarán protegidos mediante cifrado con algoritmos estándar de la industria (Definir: mínimo AES-256 para datos en reposo y TLS 1.3 para datos en tránsito).

b) Las claves de cifrado serán gestionadas por EL PROVEEDOR bajo estrictos controles de acceso, asegurando que solo personal autorizado pueda acceder a ellas.

c) EL PROVEEDOR proporcionará evidencia documental del cumplimiento de los requisitos de cifrado, incluyendo configuraciones técnicas y auditorías de terceros, cuando sea solicitado por LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES.

Cláusula 5: Gestión de Identidades y Accesos

a) EL PROVEEDOR implementará un sistema de gestión de identidades y accesos basado en el principio de privilegios mínimos, utilizando autenticación multifactor (MFA) para todos los usuarios administrativos y aquellos con acceso a datos de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES.

b) Las credenciales de acceso otorgadas a LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES serán temporales, renovables y monitoreadas, con registros de actividad disponibles para auditoría.

c) EL PROVEEDOR garantizará la desactivación inmediata de cualquier cuenta o acceso al finalizar su necesidad o el contrato, utilizando procesos preferiblemente automatizados.

d) EL PROVEEDOR entregará un informe (especificar, la periodicidad ej: mensual, trimestral, semestral, etc) de gestión de accesos, detallando roles, permisos y actividades realizadas.}

Cláusula 6: Notificación de Incidentes de Seguridad

a) EL PROVEEDOR notificará a LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES, a través del Oficial de Seguridad de la Información, cualquier incidente de seguridad que pueda afectar los datos o el servicio en un plazo no superior a 24 horas desde su detección.
b) La notificación incluirá:
   i. Descripción del incidente, incluyendo fecha, hora y naturaleza.
   ii. Evaluación preliminar del impacto en los datos de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES.
   iii. Acciones correctivas tomadas o planificadas.
iv. Análisis de causa raíz, cuando esté disponible.
c) EL PROVEEDOR colaborará con LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES en la investigación y mitigación del incidente, proporcionando toda la información y registros necesarios

d) EL PROVEEDOR mantendrá un registro de incidentes que estará disponible para auditorías por parte de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES

Cláusula 7: Derecho a Auditoría y Revisión Técnica

a) LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES, a través del equipo de Seguridad Informática y Forense, firma consultora o un auditor externo designado, tendrá derecho a realizar auditorías técnicas y revisiones del servicio SaaS, incluyendo infraestructura, procesos y controles de seguridad, con o sin notificación previa, al menos una vez al año de ser necesario.
b) EL PROVEEDOR facilitará el acceso a la documentación, registros y sistemas necesarios para dichas auditorías, garantizando la confidencialidad de la información de otros clientes.
c) EL PROVEEDOR entregará, como parte de los anexos, un informe de cumplimiento que incluya pruebas y análisis de vulnerabilidades realizados al servicio (SAST, DAST, pentesting), con resultados y remediaciones documentadas.

Cláusula 8: Reversibilidad de la Información

a) En caso de terminación del contrato, por cualquier causa, EL PROVEEDOR garantizará la entrega completa de los datos de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES en un formato estándar, interoperable y acordado (ej. CSV, JSON, XML), dentro de un plazo máximo de (especificar el tiempo en días ej: 10 días calendario o hábiles).
b) EL PROVEEDOR proporcionará asistencia técnica para la migración de los datos a otro proveedor o sistema, si así lo solicita LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES, durante un período de (especificar ej: 30 días) tras la terminación.

Verifique que este documento corresponda a la versión vigente antes de su uso

c) EL PROVEEDOR eliminará de forma segura todos los datos de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES de sus sistemas al completar la entrega, proporcionando un certificado de eliminación segura.
d) EL PROVEEDOR incluirá en los anexos un plan de reversibilidad detallado, especificando formatos, plazos y procedimientos.

Cláusula 9: Acuerdos de Nivel de Servicio (SLA)

a) EL PROVEEDOR garantizará un nivel de disponibilidad del servicio de al menos (especificar, ej. 99.9%) mensual, medido según los términos definidos.
b) EL PROVEEDOR proporcionará un Anexo de Acuerdos de Nivel de Servicio (SLA) que detalle:
    i. Tiempos de respuesta y resolución para incidentes.
    ii. Procedimientos de mantenimiento programado, con notificación previa de al menos [especificar, ej. 7 días].
    iii. Métricas de rendimiento y disponibilidad.
    iv. Compensaciones en caso de incumplimiento (ej. créditos o descuentos).
c) EL PROVEEDOR entregará informes mensuales de cumplimiento de los SLA, incluyendo métricas de disponibilidad, tiempos de respuesta y resultados de pruebas de seguridad.

Cláusula 10: Obligaciones Generales del Proveedor

a) EL PROVEEDOR cumplirá con todas las normativas aplicables, incluyendo la Ley 1581 de 2012, el Decreto 1377 de 2013, y las políticas de seguridad de la información de LA SUPERINTENDENCIA DE SOCIEDADES DE SOCIEDADES.
b) EL PROVEEDOR será responsable de cualquier daño derivado del incumplimiento de las obligaciones establecidas en este contrato, incluyendo sanciones regulatorias o pérdidas de datos.
c) EL PROVEEDOR mantendrá una póliza de responsabilidad civil que cubra posibles incidentes de seguridad o violaciones de datos, con una cobertura mínima de (especificar monto en salarios mínimos legales mensuales vigentes).

Cláusula 12: Anexos

Los siguientes documentos forman parte integral de este contrato:

a) Anexo de Seguridad del Servicio y Acuerdos de Nivel de Servicio (SLA).
b) Informe de cumplimiento (ISO 27001, SOC 2 o equivalente).
c) Resultados de pruebas y análisis de vulnerabilidades.
d) Plan de reversibilidad de datos.

10.4. Anexo 4

Implementación del Control 5.8 "Seguridad de la Información en la Gestión de Proyectos" – NTC ISO/IEC 27001:2022"

1. Integración de requisitos de seguridad de la información en los proyectos

1.1 Se deberán identificar explícitamente los requisitos de seguridad de la información desde la fase de formulación, incluyendo confidencialidad, integridad, disponibilidad y privacidad de los datos.

1.2 Estos requisitos deberán quedar documentados en el Acta de Inicio del proyecto, el Plan del Proyecto o el documento equivalente, y ser trazables a los objetivos del SGSI y del MSPI.

1.3 Los entregables del proyecto deberán contemplar los controles de seguridad definidos (políticas, procedimientos, configuraciones técnicas, evidencias de pruebas, capacitación, etc.).

2. Gestión de riesgos de seguridad de la información en proyectos

1.4 Todo proyecto deberá realizar un análisis de riesgos de seguridad de la información, alineado con la metodología institucional y con el MSPI, identificando activos, amenazas, vulnerabilidades y controles asociados.

1.5 Los riesgos identificados deberán registrarse en la matriz de riesgos del proyecto, con su tratamiento (aceptación, mitigación, transferencia o evitación) y responsables definidos.

1.6 Cuando el proyecto implique servicios de terceros o proveedores, se deberán articular los requisitos del control 5.19 "Seguridad de la información en las relaciones con proveedores" y las cláusulas contractuales definidas por la entidad.

3. Roles y responsabilidades en seguridad de la información para proyectos

2.1 La Alta Dirección y los Dueños de Proceso garantizarán la integración de la seguridad en los proyectos bajo su responsabilidad, de acuerdo con las políticas del SGSI.

2.2 Cada proyecto deberá designar un responsable de Seguridad de la Información del Proyecto, que actuará como enlace con el Oficial de Seguridad de la Información y el Equipo de Seguridad Informática y Forense.

2.3 En la matriz RACI del proyecto deberán incluirse las responsabilidades específicas en materia de:

- Identificación de requisitos de seguridad.
- Gestión de riesgos.
- Gestión de incidentes.
- Administración de accesos.

Verifique que este documento corresponda a la versión vigente antes de su uso

- Cierre y devolución / eliminación de información.

4. Controles de acceso y uso aceptable de activos en los proyectos

3.1 Los proyectos deberán respetar los lineamientos de uso aceptable de activos de información (GIN-GU-004), incluyendo restricciones sobre USB, nube pública no autorizada, cuentas compartidas y uso de equipos personales.

3.2 Los accesos a sistemas, repositorios de código, bases de datos y ambientes de prueba deberán otorgarse bajo el principio de mínimo privilegio y con vigencia limitada al tiempo del proyecto.

3.3 Al cierre del proyecto se deberá garantizar la revocación de todos los accesos otorgados a contratistas y personal interno para fines del proyecto.

3.4 Se debe informar al contratista todo nuevo control relacionado, ser capacitado y contar con la evidencia correspondiente.

5. Protección de información y datos personales en los proyectos

4.1 Cuando un proyecto implique tratamiento de datos personales, se aplicarán la Política GIN-PO-002 y la normativa de protección de datos (Ley 1581 de 2012 y Decreto 1377 de 2013), asegurando que la finalidad, las bases de datos y los encargados estén formalmente definidos manteniendo el principio de responsabilidad compartida.

4.2 Se deberán implementar mecanismos de minimización, anonimización o seudonimización de datos cuando sea posible, especialmente en ambientes de desarrollo y pruebas.

4.3 En el cierre se deberá asegurar la devolución o eliminación segura de los datos personales tratados en el marco del proyecto.

6. Gestión de incidentes de seguridad de la información en proyectos

5.1 Todos los miembros del proyecto deberán conocer y aplicar el procedimiento institucional de gestión de incidentes de seguridad digital, alineado con el MSPI y la Política de Gestión de Incidentes del SGSI.

5.2 Los incidentes identificados durante el proyecto se reportarán a la Mesa de Ayuda y al Equipo de Seguridad Informática y Forense, documentando causa raíz, impacto, acciones correctivas y lecciones aprendidas.

5.3 Los incidentes significativos deberán ser considerados en los cierres de proyecto y en los planes de mejora del SGSI.

7. Documentación, cierre del proyecto y mejora continua

6.1 Los proyectos deberán conservar evidencias documentales de los requisitos, análisis de riesgos, decisiones de seguridad, incidentes y acciones correctivas, conforme a la Política de Gestión Documental del SGI (GIN-PO-001).

6.2 El acta de cierre de proyecto deberá incluir un apartado específico de seguridad de la información donde se deje constancia de:

- Cumplimiento de los requisitos definidos.
- Resultados de pruebas y revisiones de seguridad.

Verifique que este documento corresponda a la versión vigente antes de su uso

- Revocación de accesos y devolución/eliminación de información.
- Lecciones aprendidas para retroalimentar el SGSI y el MSPI.

Verifique que este documento corresponda a la versión vigente antes de su uso

10.5. Anexo 5

Línea Base de Requisitos de Seguridad de la Información para la Gestión de Proyectos (Control 5.8)

Esta línea base aplica a:

- Proyectos de desarrollo o adquisición de software.
- Proyectos de infraestructura tecnológica.
- Proyectos que involucren tratamiento de datos personales o información clasificada o reservada.
- Proyectos misionales o de apoyo que utilicen activos de información críticos.

1. Gobierno y Alcance

- Declarar en el documento de inicio del proyecto que se encuentra sujeto a las políticas, manuales, procedimientos, guías, formatos y demás documentos relacionados en el Sistema de Gestión de Seguridad de la Información (SGSI) y el Sistema de Gestión Integrado (SGI).
- Identificar si el proyecto es interno, tercerizado o mixto (contratos de servicios o proveedores).
- Asignar responsable de incluir y hacerle seguimiento a los requisitos de seguridad en el proyecto.

2. Requisitos de Seguridad de la Información

- Documentar requisitos de confidencialidad, integridad, disponibilidad y privacidad aplicables al proyecto.
- Incorporar estos requisitos en estudios previos y contratos cuando aplique.
- Definir los controles mínimos tales como autenticación segura, control de accesos, cifrado cuando corresponda, respaldo y trazabilidad.

3. Gestión de Riesgos

- Identificar activos de información del proyecto (datos, sistemas, infraestructura, procesos).
- Realizar análisis de riesgos de seguridad de la información específico del proyecto.
- Definir y documentar el tratamiento de riesgos y los controles seleccionados.
- Integrar los riesgos críticos en el mapa de riesgos institucional.

4. Roles, Responsabilidades y Competencias

- Incluir en la matriz RACI del proyecto las funciones de seguridad (definir requisitos, revisar diseños, aprobar cambios, gestionar incidentes).
- Verificar competencia mínima en seguridad para el personal clave del proyecto o programar capacitación específica.
- Definir el rol del Supervisor contractual cuando el proyecto se ejecute mediante contratistas.

5. Control de Accesos y Uso de Activos

Verifique que este documento corresponda a la versión vigente antes de su uso

- Solicitar y documentar la creación de cuentas y permisos para el proyecto, bajo mínimo privilegio.
- Prohibir cuentas genéricas o compartidas; justificar excepcionalidades.
- Restringir uso de USB, servicios en nube públicos y dispositivos personales no autorizados.
- Establecer fecha y responsable de revocación de accesos al cierre del proyecto.

6. Ambientes y Desarrollo Seguro (si aplica)

- Asegurar separación de ambientes desarrollo/pruebas/producción.
- Evitar uso de datos reales en ambientes no productivos; cuando sea indispensable, aplicar enmascaramiento o anonimización.
- Integrar controles de desarrollo seguro tales como OWASP, revisiones de código y pruebas de seguridad.

7. Protección de Datos Personales

- Determinar si el proyecto involucra datos personales y, de ser así, identificar responsable y encargado del tratamiento.
- Documentar finalidades, bases de datos afectadas, flujos de información y medidas de seguridad asociadas.
- Garantizar la aplicación de los principios de la Ley 1581 de 2012 y la política GIN-PO-002 (legalidad, finalidad, libertad, veracidad, circulación restringida, seguridad y confidencialidad).

8. Gestión de Incidentes

- Incluir en el plan del proyecto el procedimiento de reporte y atención de incidentes de seguridad digital.
- Definir responsables en el proyecto para coordinar con la Mesa de Ayuda y el Equipo de Seguridad Informática y Forense.
- Registrar incidentes, causas raíz y acciones de mejora vinculadas al proyecto.

9. Documentación y Cierre

- Mantener carpeta o repositorio del proyecto con: requisitos, riesgos, decisiones, pruebas de seguridad, incidentes, actas y configuraciones finales.
- Incluir en el acta de cierre la verificación de:
  - Cumplimiento de requisitos de seguridad.
  - Revocación de accesos.
  - Devolución o eliminación de información.
  - Lecciones aprendidas para el SGSI/MSPI.

Verifique que este documento corresponda a la versión vigente antes de su uso

10.6. Anexo 6

Seguridad de la información en las relaciones con proveedores ISO/IEC 27001:2022 – Control 5.19

1. Objetivo de la línea base

Establecer los requisitos y lineamientos que deben aplicarse en la contratación, supervisión y relación con proveedores, para asegurar que:

- Los riesgos asociados al uso de productos o servicios de terceros sean gestionados adecuadamente.
- Se cumplan las políticas internas de seguridad y privacidad de la Superintendencia.
- Se garantice la protección de la información institucional y los datos personales.

2. Normatividad aplicable

- Ley 1581 de 2012 – Protección de datos personales
- Decreto 1377 de 2013 – Reglamentación Ley 1581
- Ley 1712 de 2014 – Transparencia y acceso a la información pública
- Resolución 500 de 2021 – Modelo MSPI
- Resolución 2277 de 2025 – Actualización del MSPI
- Política de Seguridad y Privacidad de la Información – GIN-PO-003 Incluye el apartado A.5.20 – Relaciones con proveedores, que establece obligaciones, controles, requisitos contractuales y responsabilidades.
- Política de Tratamiento de Datos Personales – GIN-PO-002 Obliga a proveedores a cumplir Ley 1581/2012, Decreto 1377/2013 y medidas técnicas, administrativas y jurídicas de protección.
- Guía de Uso Aceptable – GIN-GU-004 Establece restricciones para proveedores respecto al uso de activos, acceso a red, medios removibles, información, equipos y recursos institucionales.
- Políticas del Sistema Integrado – GIN-PO-001 Objeto, alcance y responsabilidades asociadas a la gestión institucional y documental.

3. Alcance

Esta línea base aplica a:

- Contratos de prestación de servicios profesionales
- Contratos de soporte, mantenimiento o tecnología
- Contratos de desarrollo o adquisición de software
- Servicios en la nube
- Procesos de externalización (outsourcing)
- Suministro de infraestructura, hardware o redes
- Servicios que impliquen acceso a datos personales o información clasificada

Proveedores contratistas, subcontratistas, operadores externos, empresas aliadas, integradores y cualquier tercero con acceso a activos de información institucional

4. Línea Base de Requisitos del Control 5.19

Verifique que este documento corresponda a la versión vigente antes de su uso

A continuación, se presentan los requisitos mínimos que deben integrarse en estudios previos, términos de referencia (TDR), contratos, supervisión y auditoría.

4.1. Identificación y evaluación de riesgos del proveedor

- Realizar evaluación de riesgos del proveedor antes de contratar.
- Identificar activos afectados, información, bases de datos, sistemas e infraestructura.
- Determinar riesgos de confidencialidad, integridad, disponibilidad y privacidad.
- Registrar riesgos en la matriz institucional y proyecto.
- Verificar cumplimiento del proveedor con:
  - Ley 1581 y Decreto 1377
  - ISO 27001
  - Políticas internas GIN-PO-003, GIN-PO-002, GIN-GU-004

4.2. Requisitos de seguridad para Términos de Referencia (TDR) y contratos

Los términos de referencia (TDR) deben incluir cláusulas que obliguen al proveedor a:

- Cumplir el SGI y SGSI y demás legislación nacional y políticas institucionales.
- Mantener confidencialidad y secreto profesional incluso después del contrato.
- Implementar controles técnicos de protección:
  - Cifrado
  - Control de accesos
  - Autenticación segura
  - Trazabilidad
  - Backups si aplica

- Reportar incidentes en máximo 1 hora.
- Permitir auditorías de seguridad.
- Evitar subcontratación sin autorización.
- Usar exclusivamente equipos autorizados por la entidad.
- Separar ambientes dev/test/prod si participa en desarrollo.

4.3. Control de Accesos del Proveedor

- Asignar accesos con vigencia limitada al contrato y al mínimo privilegio.
- Prohibir cuentas compartidas.
- Registrar todos los accesos otorgados.
- Monitorear accesos durante la ejecución del contrato.
- Al finalizar, revocar todos los accesos y emitir certificado de revocación.

4.4. Uso aceptable de activos

El proveedor deberá cumplir con GIN-GU-004:

- No usar USB, medios removibles o almacenamiento externo sin autorización.
- No acceder a redes, VPN o servicios de la entidad desde dispositivos no autorizados.
- No almacenar información institucional en equipos personales.
- No utilizar nubes públicas o aplicaciones no autorizadas.

Verifique que este documento corresponda a la versión vigente antes de su uso

- Cumplir reglas de acceso físico y lógico a activos y áreas.

4.5. Protección de datos personales

El proveedor deberá:

- Tratar datos personales solo bajo instrucciones de la entidad.
- Garantizar medidas técnicas, organizativas y jurídicas.
- Aplicar minimización, anonimización o seudonimización cuando aplique.
- Gestionar solicitudes de titulares a través de la entidad.
- Garantizar privacidad por defecto y por diseño.

4.6. Gestión de incidentes asociados a proveedores

- Reportar incidentes a la Mesa de Ayuda en el tiempo establecido.
- Apoyar análisis forense cuando corresponda.
- Implementar medidas correctivas inmediatas.
- Documentar causa raíz y plan de mejora.

4.7. Auditorías, seguimiento y cumplimiento

- Supervisar el cumplimiento de requisitos de seguridad durante el contrato.
- Realizar auditorías técnicas cuando corresponda.
- Evaluar desempeño y madurez del proveedor.
- Documentar hallazgos para mejora del SGSI.

4.8. Cierre del contrato con proveedor

- Revocar accesos.
- Exigir devolución, entrega o eliminación segura de información.
- Solicitar certificación formal del proveedor.
- Recibir manuales, documentación técnica y llaves de cifrado.
- Documentar lecciones aprendidas.

5. Matriz Línea Base Control 5.19 - Seguridad de la información en las relaciones con proveedores

Elemento	Requisito / Descripción según ISO 27001:2022 (5.19)	Responsable(s)	Evidencias esperadas
5.19.1 Evaluación de riesgos del proveedor	Realizar evaluación de riesgos de seguridad de la información asociados al uso de productos o servicios del proveedor, identificando activos,	Dueño del proceso, OSI, Grupo de Seguridad Informática	Matriz de riesgos por proveedor, clasificación del proveedor, acta de evaluación, informe de riesgo residual.

Verifique que este documento corresponda a la versión vigente antes de su uso

Elemento	Requisito / Descripción según ISO 27001:2022 (5.19)	Responsable(s)	Evidencias esperadas
	amenazas y vulnerabilidades.		
5.19.2 Requisitos de seguridad en términos de referencia (TDR) y contratos	Incluir requisitos de seguridad de la información en estudios previos, TDR y contratos: cláusulas de confidencialidad, controles técnicos, obligaciones de cumplimiento normativo y del SGSI.	Supervisor del contrato, Jurídica, OSI	TDR y contratos con cláusulas de seguridad, matrices de requisitos, conceptos de OSI, actas de comité de contratación.
5.19.3 Gestión de accesos del proveedor	Definir, otorgar, monitorear y revocar accesos lógicos y físicos a sistemas e instalaciones para proveedores, bajo el principio de mínimo privilegio y por el tiempo estrictamente necesario.	TI, OSI, Dueño del proceso, Seguridad física	Solicitudes de creación de usuarios, listados de permisos, bitácoras de acceso, evidencias de revocación al cierre del contrato.
5.19.4 Uso aceptable de activos por parte del proveedor	Asegurar que el proveedor cumple las reglas de uso aceptable de activos de información, equipos, redes, medios removibles y servicios en la nube definidos por la entidad.	Proveedor, Supervisor del contrato, OSI	Compromisos firmados, inducción de seguridad a proveedores, registros de cumplimiento, controles sobre USB, nube pública, dispositivos personales.
5.19.5 Protección de datos personales tratados por proveedores	Garantizar que el proveedor cumple la normativa de protección de datos personales y la política institucional, actuando como encargado del tratamiento bajo instrucciones de la entidad.	Oficial de Protección de Datos, OSI, Dueño del proceso, Proveedor	Contratos de encargado del tratamiento, avisos de privacidad, análisis de impacto, registros de bases de datos, certificaciones del proveedor.

Verifique que este documento corresponda a la versión vigente antes de su uso

Elemento	Requisito / Descripción según ISO 27001:2022 (5.19)	Responsable(s)	Evidencias esperadas
5.19.6 Gestión de incidentes de seguridad asociados a proveedores	Definir y aplicar procedimientos para que los proveedores reporten, gestionen y apoyen la atención de incidentes de seguridad de la información.	Proveedor, OSI, Grupo de Seguridad Informática y Forense, Mesa de Ayuda	Registro de incidentes reportados por proveedores, análisis de causa raíz, planes de acción, evidencias de comunicación y atención.
5.19.7 Seguimiento, auditoría y evaluación del proveedor	Realizar seguimiento y, cuando aplique, auditorías a los proveedores para verificar el cumplimiento de los requisitos de seguridad y privacidad acordados.	Supervisor del contrato, OSI, Control Interno	Informes de seguimiento, actas de comité, planes de mejora, resultados de auditorías al proveedor.
5.19.8 Cierre de la relación con el proveedor	Gestionar el cierre del contrato garantizando la revocación de accesos, devolución o eliminación certificada de información y activos, así como la entrega de documentación final.	Supervisor del contrato, TI, OSI, Proveedor	Acta de cierre, certificaciones de eliminación/devolución de información, listado de accesos revocados, inventario actualizado de activos.

Verifique que este documento corresponda a la versión vigente antes de su uso

10.7. Anexo 7

Abordar la seguridad de la información dentro de los acuerdos con proveedores - ISO/IEC 27001:2022 – Control 5.20

1. Objetivo

Definir los requisitos mínimos de seguridad de la información que deben incorporarse en acuerdos, contratos, convenios, términos de referencia (TDR) y relaciones formales con proveedores, asegurando la protección de activos, datos personales, infraestructura y servicios tecnológicos.

2. Normatividad aplicable

- ISO 27001:2022 – Control 5.20.
- Resolución 500 de 2021.
- Resolución 746 de 2022.
- Ley 1581 de 2012.
- Decreto 1377 de 2013.
- Ley 1712 de 2014.
- Políticas de Seguridad y Privacidad de la Información – GIN-PO-003
- Política de Tratamiento de Datos Personales – GIN-PO-002
- Guía de Uso Aceptable – GIN-GU-004
- Política del SGI – GIN-PO-001

3. Alcance

Aplica a todos los acuerdos y relaciones con terceros que:

- Accedan a información institucional
- Traten datos personales
- Operen infraestructura tecnológica
- Suministren servicios en la nube
- Provean seguridad digital, hardware, software, soporte o mantenimiento
- Gestionen operaciones sensibles o críticas
- Incluye proveedores nacionales e internacionales, y subcontratistas.

4. Línea Base de Requisitos – control 5.20

Todos los acuerdos deberán incluir:

- Definición de roles y responsabilidades
- Clasificación y manejo seguro de información compartida
- Controles de acceso, monitoreo y auditoría
- Obligación de cumplir con políticas internas del SGSI
- Los sujetos obligados deben definir e implementar controles mínimos para relaciones con proveedores, incluyendo:
  - Definir claramente los roles y responsabilidades en la gestión de la seguridad de información en la relación con proveedores.

Verifique que este documento corresponda a la versión vigente antes de su uso

- Identificar de manera documentada los activos del proveedor y de la entidad involucrados.
- Determinar los niveles de criticidad del servicio o producto respecto a la información tratada.
- Establecer mecanismos de monitoreo y supervisión sobre los controles durante la ejecución del contrato.

- Inventario de activos involucrados en el servicio.
- Plan de evaluación y tratamiento de riesgos.
- Identificación de normatividad aplicable (protección de datos, propiedad intelectual, laboral).
- Análisis de criticidad del producto/servicio.

4.1. Selección del proveedor

- Cumplimiento aspectos habilitantes acorde con la normatividad nacional en contratación.
- Verificación de antecedentes de proveedor
- Criterios de selección basados en madurez en seguridad digital.
- Obligación de aceptar los requisitos de seguridad definidos en el pliego.
- Preparación y firma de acuerdos de confidencialidad.

4.2. Negociación de acuerdos con proveedores

- Cambios y transiciones evaluados en términos de riesgos.
- Capacitación al personal involucrado.
- Gestión de incidentes y cambios.

4.3. Gestión de la relación durante el contrato

- Gestión del modelo de responsabilidad compartida.
- Revisión periódica de documentos y controles.
- Evaluación continua de riesgos.
- Pruebas periódicas de continuidad, recuperación y respuesta a incidentes.

4.4. Terminación de la relación contractual

- Plan de terminación aprobado y probado.
- Comité técnico de cierre.
- Entrega de documentación técnica completa.
- Eliminación segura certificada de datos.
- Revocación de accesos.

5. Matriz Línea Base Control 5.20 - Abordar la seguridad de la información dentro de los acuerdos con proveedores

Elemento del Control	Requisito	Evidencias	Responsable
Definición de roles y responsabilidades	Establecer roles en la relación contractual	Matriz RACI, actas	Supervisor /GSIF
Identificación de activos	Identificar activos de ambas partes	Inventario, fichas	Proceso /GSIF
Evaluación de criticidad	Clasificación del servicio/producto	Matriz de criticidad	OSI / Supervisor
Inclusión de requisitos de seguridad	Incorporar cláusulas, Acuerdos de Nivel de Servicio	TDR, contrato	Jurídica / DTIC
Gestión de riesgos	Evaluación y tratamiento de riesgos	Matriz de riesgos	OSI
Gestión de incidentes	Notificación, soporte, mitigación	Reportes	Proveedor / OSI
Auditoría y supervisión	Monitoreo continuo de controles	Informes, evidencias	OSI / Control Interno
Cierre contractual	Terminación segura y eliminación de datos	Acta, certificación	Supervisor / TI

Verifique que este documento corresponda a la versión vigente antes de su uso

10.8. Anexo 8

Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC). - ISO/IEC 27001:2022, Control 5.20

1. Identificación y análisis de la cadena de suministro

La entidad deberá:

- Mapear los servicios críticos que dependen de terceros.
- Identificar eslabones de la cadena que puedan impactar la confidencialidad, integridad o disponibilidad.
- Registrar todos los proveedores de segundo y tercer nivel cuando impacten el servicio.
- Analizar riesgos derivados de:
  - externalización,
  - transferencia de datos,
  - integración con sistemas externos,
  - dependencia tecnológica.

2. Requisitos mínimos de seguridad para toda la cadena

Los proveedores deberán cumplir los mismos estándares aplicados internamente, incluyendo:

- Controles de acceso, cifrado, trazabilidad.
- Protección de datos personales conforme a Ley 1581y política de protección de datos en la entidad.
- Controles de continuidad y disponibilidad.
- Controles específicos para servicios en la nube.

3. Acuerdos formales de responsabilidad

Los acuerdos deberán contemplar:

- Modelo de responsabilidad compartida (obligatorio en servicios en la nube).
- Obligaciones claras de subcontratación y notificación de cambios en terceros.
- Transferencia internacional de datos (si aplica).

4. Supervisión y monitoreo continuo

La entidad deberá:

- Verificar periódicamente el cumplimiento de controles de seguridad.
- Realizar evaluaciones sobre proveedores críticos.
- Solicitar evidencias periódicas (logs, reportes, auditorías).
- Monitorear incidentes afectando la cadena.

5. Gestión de incidentes en la cadena de suministro

Los proveedores deben:

- Notificar incidentes de manera inmediata.

Verifique que este documento corresponda a la versión vigente antes de su uso

- Proveer acceso para análisis forense si es requerido.
- Activar planes de continuidad y recuperación del servicio.

6. Terminación segura de la relación con terceros

Debe garantizarse:

- Eliminación o devolución certificada de información.
- Entrega de documentación técnica.
- Retiro de accesos y cuentas.
- Cierre formal mediante comité técnico.

7. Matriz Línea Base Control 5.21 - Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC).

Elemento	Requisito	Evidencias	Responsable
Identificación de cadena de suministro	Mapeo de servicios y terceros	Inventario, análisis	OSI / Proceso
Evaluación de riesgos	Riesgos derivados de terceros	Matriz de riesgos	OSI
Requisitos de seguridad	Controles equivalentes para terceros	Contratos, cláusulas	Jurídica / OSI
Responsabilidad compartida	Detalle de obligaciones en toda la cadena	Acuerdos, ANS	Supervisor / Proveedor
Supervisión continua	Auditoría, verificación y seguimiento	Reportes, actas	OSI / Supervisor
Gestión de incidentes	Notificación y tratamiento de incidentes	Registro de incidentes	Proveedor / OSI
Terminación segura	Procesos para cierre de la relación	Acta de cierre	Supervisor / TI

Verifique que este documento corresponda a la versión vigente antes de su uso

10.9. Anexo 9
Seguimiento, revisión y gestión del cambio de los servicios de los proveedores - ISO/IEC 27001:2022 – Control 5.22

1. Objetivo
Establecer los requisitos para supervisar, revisar, evaluar y gestionar cambios que puedan afectar la seguridad de la información en los servicios suministrados por proveedores, garantizando que:
- Los proveedores mantengan los controles de seguridad acordados.
- Los cambios planificados o no planificados no introduzcan riesgos adicionales.
- Se mantenga la trazabilidad y evidencia de la gestión de la relación.
- La organización conserve la capacidad de operar de manera segura y continua.

2. Normatividad aplicable
- Política de Seguridad y Privacidad de la Información – GIN-PO-003.
- Guía de Uso Aceptable – GIN-GU-004.
- Política de Tratamiento de Datos Personales – GIN-PO-002.
- Sistema Integrado de Gestión – GIN-PO-001.
- ISO/IEC 27001:2022
- ISO 22301:2019
- Ley 1581 de 2012
- Decreto 1377 2013
- Resolución 2277 de 2025
- Resolución 746 de 2022
- Resolución 500 de 2021

3. Alcance
- Todos los proveedores de servicios que procesan, almacenan o transmiten información institucional.
- Proveedores con acceso físico o lógico a activos de información.
- Proveedores que operan plataformas tecnológicas, infraestructura, nube, aplicaciones, redes o bases de datos.
- Subcontratistas y proveedores de segundo o tercer nivel (cadena de suministro).
- Servicios críticos según BIA, análisis de riesgos o ISO 22301.

4. Requisitos de la Línea Base – Control 5.22
4.1. Monitoreo continuo del proveedor
La organización debe:
- Supervisar el cumplimiento de controles de seguridad establecidos.
- Monitorear incidentes, vulnerabilidades, accesos y cambios operativos del proveedor.

Verifique que este documento corresponda a la versión vigente antes de su uso

- Revisar logs y reportes de actividad relevantes para los servicios tercerizados.
- Validar que el proveedor mantenga sus certificaciones y controles (ISO 27001, ISO 22301, etc.).

4.2. Revisión periódica del desempeño

- Mensuales, trimestrales o según criticidad.
- De SLA/OLA asociados a seguridad.
- De desempeño en gestión de incidentes, continuidad, disponibilidad y soporte.
- Debe existir evidencia documentada.

4.3. Gestión del cambio del proveedor

- Identificar cambios en infraestructura, procesos, personal o tecnología del proveedor.
- Evaluar riesgos de dichos cambios.
- Validar si requieren ajustes en configuraciones, contratos o controles.
- Aprobar o rechazar cambios significativos que puedan impactar la seguridad.
- Cambios en subcontratistas.
- Cambios de ubicación geográfica de datos.
- Migraciones de plataforma.
- Nuevas APIs, módulos o integraciones.

4.4. Evaluación del impacto en la cadena de suministro

- Riesgos ampliados por terceros indirectos.
- Cadena de suministro digital (ISO 27036- Resolución 746).
- Dependencias críticas que afecten la disponibilidad (ISO 22301).

4.5. Gestión de incidentes asociados al proveedor

- Canal para recibir notificaciones del proveedor.
- Mecanismos de análisis y gestión conjunta.
- Registros de incidentes y acciones correctivas.
- Validación de tiempos de respuesta y recuperación.

4.6. Revisión contractual y ajustes

Cuando un cambio del proveedor afecte la seguridad, la organización debe:

- Modificar acuerdos de nivel de servicio (SLA/OLA).
- Actualizar cláusulas de seguridad y responsabilidades.
- Exigir nuevas garantías o controles.
- Requerir un plan de transición o mitigación.

4.7. Evidencia documental

Todo proceso debe estar respaldado por:

- Actas de seguimiento.
- Matrices de riesgos actualizadas.
- Reportes del proveedor.
- Informes de auditoría.

Verifique que este documento corresponda a la versión vigente antes de su uso

- Registros de cambios y aprobaciones.

5. Matriz Línea Base Control 5.22 - Seguimiento, revisión y gestión del cambio de los servicios de los proveedores

Elemento	Requisito	Evidencia requerida	Responsable
Monitoreo continuo	Supervisar actividades, cumplimiento y cambios del proveedor	Logs, reportes, dashboards	Seguridad / TI / Supervisor
Revisión periódica del servicio	Evaluaciones programadas del desempeño	Actas de revisión, SLA	Supervisor /GSIF
Gestión del cambio	Identificación, análisis y aprobación de cambios del proveedor	Registro de cambios, evaluación de riesgos	Supervisor / Jurídica
Evaluación de impacto	Impacto en cadena de suministro y continuidad	Matriz de riesgos, análisis BIA	OSI / Continuidad
Gestión de incidentes	Notificación, tratamiento y registro	Reportes de incidentes	Seguridad / Mesa de servicio
Revisión contractual	Ajustes a contratos, SLA y cláusulas de seguridad	Anexos actualizados	Jurídica / Supervisor
Evidencia documental	Demostrar cumplimiento del ciclo de supervisión	Repositorio de evidencias	OSI / Control Interno

Verifique que este documento corresponda a la versión vigente antes de su uso

10.10. Anexo 10
Seguridad de la información para el uso de servicios en la nube - ISO/IEC 27001:2022 – Control 5.23

1. Objetivo del control
Establecer los requisitos mínimos para adquirir, implementar, usar, gestionar y terminar servicios en la nube de manera segura, garantizando:
- La protección de la información procesada en plataformas cloud (IaaS, PaaS, SaaS).
- El cumplimiento de políticas internas, marco legal y estándar internacional.
- La gestión adecuada de riesgos, responsabilidades compartidas y cadena de suministro.
- La continuidad del negocio cuando la operación dependa de servicios cloud.

2. Normatividad aplicable
2.1. Normatividad interna
- GIN-PO-003 Política de Seguridad y Privacidad de la Información.
- GIN-PO-002 Política de Tratamiento y Protección de Datos Personales.
- GIN-GU-004 Guía de Uso Aceptable de Activos de Información.
- Lineamientos del SGI – GIN-PO-001.
- ISO/IEC 27001:2022 – Control 5.23 (uso seguro de servicios cloud).
- ISO 22301:2019 – Requisitos de continuidad en servicios externalizados
- Ley 1581 de 2012 – Protección de datos personales.
- Decreto 1377 de 2013 – Reglamentación.

3. Alcance
Aplica a todos los servicios en la nube utilizados por la entidad, incluyendo:
- Infraestructura como servicio (IaaS).
- Plataforma como servicio (PaaS).
- Software como servicio (SaaS).
- Servicios cloud híbridos, públicos, privados o multicloud.
- Proveedores de nube (CSP) y sus subprocesadores.
- Arquitecturas serverless, contenedores, microservicios, API gateways y servicios administrados.

Incluye ambientes de:
- Producción
- Desarrollo
- QA / pruebas
- Analítica
- Integración con terceros

Verifique que este documento corresponda a la versión vigente antes de su uso

4. Línea Base de Requisitos – Control 5.23

4.1. Evaluación y selección del servicio cloud

Antes de contratar o habilitar un servicio en la nube, la entidad debe:

- Identificar los riesgos inherentes al modelo cloud.
- Determinar el modelo de responsabilidad compartida entre la entidad y el proveedor.
- Establecer ubicación geográfica de datos y jurisdicción aplicable.
- Evaluar certificaciones, auditorías y controles del proveedor de servicios Cloud (CSP).
- Validar subprocesadores del proveedor.
- Verificar requisitos de continuidad del negocio (ISO 22301).

4.2. Requisitos contractuales y de servicio (SLA)

Los acuerdos deben incluir:

- Roles y responsabilidades del cliente (entidad) y del CSP.
- Reglas para transferencia y tratamiento de datos personales.
- Parámetros de seguridad:
  - cifrado,
  - gestión de claves,
  - autenticación,
  - segregación de datos.
- Obligación de notificar incidentes en tiempos establecidos.
- Auditoría, revisiones y acceso a reportes de seguridad.
- Manejo de subprocesadores y cadena de suministro.

4.3. Controles técnicos para el uso seguro de servicios cloud

La entidad debe implementar:

- Gestión de identidades y accesos (IAM) con MFA u otro control para garantizar el acceso y trazabilidad.
- Principio de mínimo privilegio para permisos cloud.
- Configuración segura de servicios cloud (hardening).
- Monitoreo continuo (logs, SIEM, alertas de seguridad).
- Políticas de cifrado en tránsito y en reposo.
- Gestión de claves.
- Segmentación y zonas seguras.

Se debe:

- Monitorear indicadores de cumplimiento de seguridad.
- Revisar periódicamente configuraciones y controles.
- Validar reportes de auditoría del proveedor.
- Registrar actividades relevantes (logs, accesos, cambios).
- Verificar continuidad y disponibilidad del servicio cloud.

4.4. Protección de datos personales

Verifique que este documento corresponda a la versión vigente antes de su uso

En cumplimiento con Ley 1581, Decreto 1377 y GIN-PO-002:

- Garantizar tratamiento bajo instrucciones de la entidad.
- Evaluar riesgos de transferencias internacionales.
- Evitar subprocesamiento no autorizado.
- Aplicar seudonimización, anonimización o cifrado cuando corresponda.
- Obtener garantías contractuales de eliminación segura.

4.5. Planificación de continuidad y recuperación

Según ISO 22301:

- Validar si el servicio cloud soporta los RTO/RPO requeridos.
- Realizar pruebas de recuperación cuando aplique.
- Asegurar redundancia geográfica si es necesaria.

4.6. Terminación del servicio cloud

Debe garantizarse:

- Eliminación segura certificada por el CSP.
- Migración o exportación íntegra de datos.
- Revocación de accesos y tokens.
- Cierre formal del servicio y documentación final.

5. Matriz Línea Base Control 5.23 - Seguridad de la información para el uso de servicios en la nube

Elemento	Requisito	Evidencia	Responsable
Evaluación inicial del servicio cloud	Análisis de riesgos, responsabilidad compartida, jurisdicción, certificaciones	Matriz de riesgos	Equipo Técnico / GSIF Jurídica / TI
Definición contractual	SLA, cláusulas de seguridad, subprocesadores, seguridad por diseño	Contrato, anexos técnicos	Jurídica /GSIF
Configuración segura	Configuración reforzada, IAM, MFA, cifrado	Evidencias técnicas, reportes	TI / GSIF
Monitoreo continuo	Supervisión de accesos, logs, alertas, cumplimiento	Dashboards, informes	Seguridad / TI
Protección de datos	Cumplimiento Ley 1581, subprocesamiento, ubicaciones	Contratos que evidencie la aceptación de la política de tratamiento de datos personales.	Supervisort / Jurídica
Continuidad y resiliencia	Validación RTO/RPO, pruebas de recuperación	Resultados de pruebas	OSI / TI
Cierre de servicio	Eliminación segura, revocación de accesos, exportación	Acta de cierre, certificación	TI / Supervisor

Verifique que este documento corresponda a la versión vigente antes de su uso

10.11. Anexo 11
Seguridad de los servicios de red - ISO/IEC 27001:2022 – Control 8.21

1. Objetivo
Garantizar que los servicios de red, internos o tercerizados, se diseñen, configuren, operen y monitoreen con medidas de seguridad apropiadas que protejan:
- La confidencialidad, integridad y disponibilidad del tráfico de red.
- La infraestructura que soporta servicios institucionales.
- El acceso seguro entre segmentos, usuarios, equipos, servidores y servicios cloud.
- Los niveles de servicio (SLA/OLA) asociados a la red.

2. Normatividad aplicable
- GIN-PO-003: Política de Seguridad y Privacidad de la Información.
- GIN-GU-004: Guía de Uso Aceptable de Activos de Información.
- GIN-PO-001: Sistema Integrado de Gestión.
- Políticas de administración de red.
- ISO/IEC 27001:2022 — Control 8.21
- ISO/IEC 27002:2022 — Seguridad de los servicios de red (guía de implementación)

3. Alcance
Este control aplica a todos los servicios de red, incluyendo:
- Redes LAN, WLAN, WAN, MAN
- VPN corporativa
- Segmentación y VLAN
- Firewalls y sistemas IDS/IPS
- Proxy, DNS, DHCP
- Servicios de red hacia aplicaciones internas o cloud.
- Integración con redes de proveedores.
- Red de servidores, centros de datos, campus y nube híbrida.
- Incluye redes administradas por terceros o por personal interno.

4. Requisitos de la Línea Base – Control 8.21
4.1. Identificación de servicios de red y requisitos de seguridad
La entidad debe:
- Inventariar todos los servicios de red y sus dependencias.
- Definir requisitos mínimos de seguridad por servicio (cifrado, autenticación, segmentación).
- Identificar tráfico crítico, sensible o confidencial.
- Documentar los niveles de servicio acordados.

4.2. Implementación de mecanismos de seguridad en la red

Verifique que este documento corresponda a la versión vigente antes de su uso

Se deben implementar controles como:

- Firewalls perimetrales e internos con políticas actualizadas.
- IDS/IPS para detección de intrusiones.
- Autenticación fuerte para acceso remoto y administración.
- Segmentación de red (VLAN, DMZ, zonas seguras).
- Protección contra ataques (DoS/DDoS, spoofing, ARP poisoning).
- Protocolos de cifrado en tránsito (TLS, IPsec).
- DNS seguro (DNSSEC/filtrado).
- Registros y trazabilidad del tráfico relevante.

4.3. Monitoreo activo y continuo

La entidad debe:

- Monitorear disponibilidad, tráfico y alertas de seguridad.
- Supervisar latencia, caídas del servicio, congestión y desviaciones.
- Revisar logs de dispositivos de red mediante SIEM u otras herramientas.
- Validar que se cumplan los niveles de servicio (SLA).

4.4. Gestión de cambios en la infraestructura de red

Todo cambio debe:

- Ser aprobado mediante el proceso institucional de gestión de cambios.
- Contar con análisis de impacto y riesgos de seguridad.
- Registrar configuraciones antes y después del cambio.
- Actualizar documentación técnica.

4.5. Validación, pruebas y auditorías

Debe realizarse:

- Pruebas de penetración o escaneo periódico.
- Auditoría de configuración de switches, routers, firewalls.
- Revisión del cumplimiento de políticas de endurecimiento.
- Validación periódica de reglas de firewall y accesos de red.

4.6. Aseguramiento de la continuidad del servicio de red

Debe incluir:

- Redundancia en enlaces críticos.
- Failover automático o manual.
- Monitoreo del estado de enlaces y equipos.
- Pruebas de recuperación ante fallos de red.

4.7. Documentación y evidencia

- Debe mantenerse:
- Diagramas actualizados de red.
- Inventario de dispositivos y servicios de red.
- Historial de cambios y configuraciones.
- Reportes de monitoreo y auditorías.

Verifique que este documento corresponda a la versión vigente antes de su uso

5. Matriz Línea Base Control 8.21 - Seguridad de la información para el uso de servicios en la nube

Elemento	Requisito	Evidencia	Responsable
Identificación de servicios de red	Inventario, criticidad, requisitos de seguridad	Inventarios, mapas de red	TI / Seguridad
Implementación de controles de seguridad	Firewalls, IDS/IPS, segmentación, cifrado	Configuraciones, reportes	TI / Seguridad
Monitoreo de red	Supervisión de tráfico, alertas y SLA	Logs, dashboards, informes	TI / Seguridad
Gestión de cambios	Control de configuraciones y análisis de impacto	Registros, aprobaciones	TI
Auditorías y validaciones	Revisión de reglas, hardening, pruebas	Informes de auditoría	Control Interno / Seguridad
Continuidad del servicio	Redundancia y recuperación de enlaces	Pruebas, evidencias	TI
Documentación	Diagramas, inventarios, configuraciones	Repositorio actualizado	TI

Verifique que este documento corresponda a la versión vigente antes de su uso

10.12. Anexo 12
Requisitos de seguridad de las aplicaciones - ISO/IEC 27001:2022 – Control 8.26

2. Objetivo
Asegurar que toda aplicación desarrollada, adquirida o modificada incluya requisitos de seguridad desde el inicio del ciclo de vida, evitando vulnerabilidades, fallas de diseño y riesgos asociados al tratamiento de datos e integración con otros sistemas.

3. Normatividad aplicable
- GIN-PO-003 – Política de Seguridad y Privacidad de la Información.
- GIN-GU-004 – Guía de Uso Aceptable de Activos.
- Política de Tratamiento de Datos Personales – GIN-PO-002.
- Lineamientos de SGI – GIN-PO-001.
- ISO/IEC 27001:2022 – Control 8.26
- ISO/IEC 27002:2022 – Seguridad de aplicaciones
- Estándares de desarrollo seguro:
  - OWASP Application Security Verification Standard (ASVS)
  - OWASP Top 10
  - NIST SP 800-64 (ciclo de vida del desarrollo seguro)

4. Alcance
Este control aplica a:
- Desarrollo interno de software.
- Adquisición de aplicaciones a proveedores.
- Servicios SaaS, PaaS y componentes de software integrados.
- Aplicaciones móviles, web, de escritorio o APIs.
- Modificaciones, actualizaciones y evolutivos.

Incluye aplicaciones que:
- Procesan información institucional.
- Acceden a datos personales o confidenciales.
- Se integran con otros sistemas.
- Funcionan en ambientes cloud o híbridos.

5. Requisitos de la Línea Base – Control 8.26

5.1. Identificación de requisitos de seguridad
Antes de desarrollar o adquirir una aplicación, se deben identificar y documentar:
- Requisitos de confidencialidad, integridad y disponibilidad.
- Requisitos normativos (protección de datos, continuidad, auditoría).
- Restricciones de acceso, autenticación y autorización.
- Necesidades de cifrado (en tránsito y reposo).

Verifique que este documento corresponda a la versión vigente antes de su uso

- Requisitos de registro, monitoreo, trazabilidad y segregación.
- Requisitos de interoperabilidad y seguridad en APIs.

5.2. Especificación formal de requisitos

Los requisitos deben especificarse en:

- Documento de Especificación de Requisitos (SRS).
- Historias de usuario con criterios de aceptación de seguridad.
- Catálogo de controles mínimos según criticidad.

5.3. Aprobación de requisitos de seguridad

Los requisitos deben ser aprobados por:

- Propietario del proceso.
- Seguridad informática y forense.
- Equipo de arquitectura TI (si aplica).
- Oficial de protección de datos personales (cuando aplique).

5.4. Requisitos para aplicaciones adquiridas o SaaS

Cada solución adquirida debe:

- Cumplir con controles de seguridad mínimos.
- Demostrar certificaciones (ISO 27001, ISO 22301, etc.).
- Proveer documentación de arquitectura y medidas de seguridad.
- Cumplir requisitos de protección de datos personales.
- Pasar evaluación de riesgos de terceros.

5.5. Requisitos de desarrollo seguro

Las aplicaciones desarrolladas deben cumplir con:

- Controles OWASP ASVS según nivel requerido.
- Validación de entradas/salidas.
- Gestión segura de sesiones.
- Mecanismos de autenticación robustos.
- Manejo seguro de errores y excepciones.
- Eliminación de código vulnerable u obsoleto.

5.6. Documentación y trazabilidad

Debe mantenerse evidencia de:

- Requisitos funcionales y no funcionales aprobados.
- Evaluación de riesgos de la aplicación.
- Análisis de impacto en seguridad.
- Cambios aprobados que afecten la seguridad de la aplicación.

Verifique que este documento corresponda a la versión vigente antes de su uso

6. Anexo 8 – Matriz Línea Base Control 8.26 - Requisitos de seguridad de las aplicaciones

Elemento	Requisito	Evidencia	Responsable
Identificación de requisitos	Definir requisitos de seguridad previos al desarrollo o adquisición	Documento de requisitos, historias de usuario	Proceso / TI /GSIF
Especificación técnica	Documentar requisitos de seguridad en el diseño	SRS, arquitectura, diagramas	TI / Arquitectura
Aprobación de requisitos	Validación y aprobación formal	Actas, firmas, registros	Propietario del proceso /GSIF
Evaluación de aplicaciones adquiridas	Verificar cumplimiento de requisitos de seguridad	Checklists, informes del proveedor	OSI / Jurídica / TI
Desarrollo seguro	Aplicar prácticas OWASP, cifrado, sesiones, validación	Evidencias de desarrollo seguro	TI / Equipos Dev
Pruebas de seguridad	Pruebas dinámicas, estáticas y de penetración	Resultados de pruebas	Seguridad / QA
Documentación	Mantener trazabilidad de requisitos y cambios	Repositorio actualizado	TI /GSIF

Verifique que este documento corresponda a la versión vigente antes de su uso