
	<b>MACROPROCESO ESTRATÉGICO</b>	<b>CÓDIGO: ESG-SSI-M013</b>
	<b>PROCESO GESTIÓN SISTEMAS INTEGRADOS – SEGURIDAD DE LA INFORMACIÓN</b>	<b>VERSIÓN: 4</b>
	<b>MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS</b>	<b>VIGENCIA: 2025-12-05</b>
		<b>PAGINA: 1 de 15</b>

**UNIVERSIDAD DE CUNDINAMARCA**

**MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON  
RELACIÓN A LOS PROVEEDORES Y/O TERCEROS**

**FUSAGASUGÁ  
2025**


	<b>MACROPROCESO ESTRATÉGICO</b>	<b>CÓDIGO: ESG-SSI-M013</b>
	<b>PROCESO GESTIÓN SISTEMAS INTEGRADOS – SEGURIDAD DE LA INFORMACIÓN</b>	<b>VERSIÓN: 4</b>
	<b>MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS</b>	<b>VIGENCIA: 2025-12-05</b>
		<b>PAGINA: 2 de 15</b>

## **UNIVERSIDAD DE CUNDINAMARCA**

**Elaborado por: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN  
ESG-SSII**


### **MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS**

**FUSAGASUGÁ  
2025**

	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-M013
	PROCESO GESTIÓN SISTEMAS INTEGRADOS – SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 4
	MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS	VIGENCIA: 2025-12-05
		PAGINA: 3 de 15

## TABLA DE CONTENIDO


1. INTRODUCCIÓN.....	4
2. OBJETIVO GENERAL .....	5
2.1 OBJETIVOS ESPECÍFICOS .....	5
3. ALCANCE.....	6
4. DEFINICIONES .....	7
5. LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS .....	8
6. LINEAMIENTOS GENERALES.....	8
7. CONDICIONES DE SEGURIDAD DE LA INFORMACIÓN A IMPLEMENTAR	10
7.1 CONTROL DE ACCESO .....	10
8. REQUISITOS DE SEGURIDAD PARA EXIGIR A LOS PROVEEDORES DURANTE LA VIGENCIA DEL CONTRATO .....	10
9. FLUJO DE COMUNICACIÓN PARA PROVEEDORES Y/O TERCEROS.....	11
10. FINALIZACIÓN DEL SERVICIO .....	12
11. BIBLIOGRAFÍA Y WEBGRAFÍA .....	13

	<b>MACROPROCESO ESTRATÉGICO</b>	<b>CÓDIGO: ESG-SSI-M013</b>
	<b>PROCESO GESTIÓN SISTEMAS INTEGRADOS – SEGURIDAD DE LA INFORMACIÓN</b>	<b>VERSIÓN: 4</b>
	<b>MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS</b>	<b>VIGENCIA: 2025-12-05</b>
		<b>PAGINA: 4 de 15</b>

## 1. INTRODUCCIÓN

Los proveedores, contratistas y partes interesadas hacen parte esencial del desempeño de las instituciones, incidiendo en el cumplimiento de la promesa de valor y en la competitividad, siendo indispensable el desarrollo de prácticas responsables que generen confianza y contribuyan a salvaguardar la confidencialidad, integridad, disponibilidad de la información y la protección de los datos personales que se compartirán.

El presente lineamiento tiene como referente los Controles Organizacionales expuestos en el Anexo a de la ISO/IEC 27001:2022 en especial los Controles Organizacionales A.5.19. Seguridad de la información en relación con proveedores, A.5.20 Abordar la seguridad de la Información dentro de los acuerdos con proveedores, A.5.21 Gestión de Seguridad en la cadena de suministro de la tecnología de la información y telecomunicaciones (TIC) y A.5.22 Seguimiento, revisión y gestión del cambio de los servicios de los proveedores.


	<b>MACROPROCESO ESTRATÉGICO</b>	<b>CÓDIGO: ESG-SSI-M013</b>
	<b>PROCESO GESTIÓN SISTEMAS INTEGRADOS – SEGURIDAD DE LA INFORMACIÓN</b>	<b>VERSIÓN: 4</b>
	<b>MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS</b>	<b>VIGENCIA: 2025-12-05</b>
		<b>PAGINA: 5 de 15</b>

## 2. OBJETIVO GENERAL

Establecer los lineamientos de Sistemas de Gestión de Seguridad de la Información – SGSI que deben cumplir los proveedores, contratistas, proponentes y terceros en su relación comercial con la Universidad de Cundinamarca. Esto con el fin de garantizar la confidencialidad, integridad y disponibilidad de los activos de información a los cuales tendrán acceso durante las fases precontractual, contractual y poscontractual.

### 2.1 OBJETIVOS ESPECÍFICOS


- Definir requisitos de seguridad que deben cumplir los proveedores y contratistas para garantizar la protección de los datos personales y la confidencialidad, integridad y disponibilidad de la información con la Universidad de Cundinamarca.
- Establecer controles y medidas de seguridad para mitigar o minimizar los riesgos de seguridad de la Información relacionados con el acceso, almacenamiento, uso y circulación, transmisión, transferencia y de la disposición final de la información.
- Evaluar la efectividad de los controles implementados a los proveedores-contratistas en función de su capacidad para cumplir con los requisitos de seguridad de la información establecidos en la política.

	<b>MACROPROCESO ESTRATÉGICO</b>	<b>CÓDIGO: ESG-SSI-M013</b>
	<b>PROCESO GESTIÓN SISTEMAS INTEGRADOS – SEGURIDAD DE LA INFORMACIÓN</b>	<b>VERSIÓN: 4</b>
	<b>MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS</b>	<b>VIGENCIA: 2025-12-05</b>
		<b>PAGINA: 6 de 15</b>

### **3. ALCANCE**

Este lineamiento aplica a todos los proveedores, contratistas y terceros (personas naturales o jurídicas) que, en el desarrollo de sus actividades con la Universidad de Cundinamarca, requieran acceso a sistemas de información, recursos tecnológicos o datos sensibles de la institución. Su aplicación es en sede, seccionales, extensiones, Oficina de Bogotá, Unidades Agroambientales y el Centro Académico Deportivo – CAD de la Universidad de Cundinamarca.

Las disposiciones de este manual son de cumplimiento obligatorio en las etapas precontractual, contractual y poscontractual.

	<b>MACROPROCESO ESTRATÉGICO</b>	<b>CÓDIGO: ESG-SSI-M013</b>
	<b>PROCESO GESTIÓN SISTEMAS INTEGRADOS – SEGURIDAD DE LA INFORMACIÓN</b>	<b>VERSIÓN: 4</b>
	<b>MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS</b>	<b>VIGENCIA: 2025-12-05</b>
		<b>PAGINA: 7 de 15</b>

#### 4. DEFINICIONES

**ACTIVO DE INFORMACIÓN:** Se refiere a cualquier información o elemento en físico y/o digital para el procesamiento, almacenamiento, comunicaciones, procesos, procedimientos y recursos humanos asociados con el manejo y uso de los datos para llevar a cabo las actividades estratégicas, misionales, de apoyo y seguimiento de la institución.<sup>1</sup>

**CONFIDENCIALIDAD:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados según sea requerida.<sup>2</sup>

**DATO:** Es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

**DISPONIBILIDAD:** Propiedad que determina que la información sea accesible y utilizable por solicitud de una persona o entidad autorizada, cuando ésta así lo Requiere.<sup>3</sup>

**INFORMACIÓN:** Datos relacionados que tiene valor para una entidad. Así mismo, la información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la institución y, en consecuencia, necesita una protección adecuada.<sup>4</sup>

**INTEGRIDAD:** La propiedad de salvaguardar la exactitud y complejidad de la Información.<sup>5</sup>

<sup>1</sup> DEPARTAMENTO NACIONAL DE PLANEACIÓN, Consejo Nacional De Política Económica y Social República De Colombia, CONPES 3854 de 2016 [sitio web]. Bogotá D.C. [Consultado: 4 de agosto de 2022]. Disponible en:

<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

<sup>2</sup> INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la Información, Requisitos. ISO/IEC 27001. Bogotá D.C.: El Instituto, 2014. 30 p.


<sup>3</sup> MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN. Guía para la Gestión y Clasificación de Activos de Información. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 11 julio 2021] Disponible en:

[https://www.mintic.gov.co/gestionti/615/articles482\\_G5\\_Gestion\\_Clasificacion.pdf](https://www.mintic.gov.co/gestionti/615/articles482_G5_Gestion_Clasificacion.pdf)

<sup>4</sup> MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN. Guía para la Gestión y Clasificación de Activos de Información. [Sitio web] Bogotá D.C: MINTIC. [Consultado: 11 julio 2021] Disponible en:

[https://www.mintic.gov.co/gestionti/615/articles482\\_G5\\_Gestion\\_Clasificacion.p](https://www.mintic.gov.co/gestionti/615/articles482_G5_Gestion_Clasificacion.p)

<sup>5</sup> INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la Información, Requisitos. ISO/IEC 27001. Bogotá D.C.: El Instituto, 2014. 30 p.

	<b>MACROPROCESO ESTRATÉGICO</b>	<b>CÓDIGO: ESG-SSI-M013</b>
	<b>PROCESO GESTIÓN SISTEMAS INTEGRADOS – SEGURIDAD DE LA INFORMACIÓN</b>	<b>VERSIÓN: 4</b>
	<b>MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS</b>	<b>VIGENCIA: 2025-12-05</b>
		<b>PAGINA: 8 de 15</b>

**PROVEEDOR:** Persona física o jurídica que provee o suministra profesionalmente de un determinado bien o servicio a otros individuos o sociedades, como forma de actividad económica y a cambio de una contra prestación.<sup>6</sup>

**RIESGO:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

**SGSI:** Sistema de Gestión de Seguridad de la Información.<sup>7</sup>

**VULNERABILIDAD:** Es una debilidad de un activo informático, o sistema de información que puede ser explotada por una o más amenazas para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.<sup>8</sup>

## 5. LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS

La Universidad de Cundinamarca establecerá contratos u ordenes contractuales de bienes, servicios u obras con proveedores; contratistas o terceros, los cuales por sus obligaciones requieren acceso a información confidencial, datos personales de titulares e infraestructura TI de la institución. Los proveedores, contratistas deberán diligenciar los acuerdos de confidencialidad y definir de manera consensuada con la UNIVERSIDAD DE CUNDINAMARCA la implementación, mantenimiento y revisión a intervalos planificados de los controles de seguridad que permitan mitigar los riesgos derivados de la interacción entre las partes. Los proveedores; contratistas deberán cumplir en todos los aspectos del lineamiento de Seguridad de la Información y del tratamiento de datos personales vigente en la UNIVERSIDAD DE CUNDINAMARCA.


## 6. LINEAMIENTOS GENERALES

1. Se debe garantizar que la relación entre la UNIVERSIDAD DE CUNDINAMARCA y los proveedores, contratistas o terceros, se efectúen mediante el cumplimiento de lineamientos de seguridad de la información y la protección de datos personales definidos por la institución y por la normatividad legal vigente en el ámbito del objeto u orden contractual, para que, de esta manera, se preserve la Confidencialidad, Integridad y Disponibilidad de la información.


<sup>6</sup> <https://economipedia.com/definiciones/proveedor.html>

<sup>7</sup> ídem

<sup>8</sup> <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

	<b>MACROPROCESO ESTRATÉGICO</b>	<b>CÓDIGO: ESG-SSI-M013</b>
	<b>PROCESO GESTIÓN SISTEMAS INTEGRADOS – SEGURIDAD DE LA INFORMACIÓN</b>	<b>VERSIÓN: 4</b>
	<b>MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS</b>	<b>VIGENCIA: 2025-12-05</b>
		<b>PAGINA: 9 de 15</b>

2. Todos los proveedores que formalicen y/o legalicen la contratación de un servicio, obra, suministro, compraventa y consultoría de conformidad a lo establecido en el Manual de Contratación de la institución **ESG-SST-M011** - MANUAL DE CONTRATISTAS y la Resolución No. 206 del 27 de noviembre del 2012 y la Resolución No.170 por medio de la cual se modifica y ajusta la resolución 206 del 27 de noviembre del 2012, que involucre el acceso a los activos de información de la Universidad de Cundinamarca, deberán firmar el **ESG-SSI-F020** - ACUERDO DE CONFIDENCIALIDAD PARA PROVEEDORES Y TERCEROS .
3. Es responsabilidad de los supervisores, proveedores, contratistas y partes interesadas que ejecutan un contrato con la Universidad de Cundinamarca conocer y cumplir con los lineamientos de Seguridad de la Información y de protección de datos personales el **ESG-SSI-M001** - MANUAL DE LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.
4. Todo proveedor, supervisor, contratista o área técnica, que por motivo del objeto contractual requiera acceso a los activos de información de la Universidad de Cundinamarca debe ser evaluado por parte del Sistema de Gestión de Seguridad de la información durante el proceso de postulación, con el fin de establecer si se debe exigir una política, norma y/o estándar de Seguridad de la Información y de Protección de Datos Personales al interior de su organización; las cuales deben desarrollarse y mantenerse actualizadas.
5. El contratista sólo podrá desarrollar para a la Universidad de Cundinamarca aquellas actividades cubiertas bajo el correspondiente contrato u orden contractual de actividades u otro equivalente, o una modificación formalizada por medio de Otro Si.
6. Todo proveedor, contratista que preste el servicio de desarrollo de software, actualización de aplicativos existentes y/o adquisición de licencias para la gestión de procesos administrativos, con la Universidad de Cundinamarca deberá atender lo dispuesto en el **ASIP16** DESARROLLO DE SISTEMAS DE INFORMACIÓN.
7. El proveedor en cumplimiento de los controles establecidos deberá actuar conforme a los lineamientos institucionales en los procesos **ABSP01** - Adquisición de Bienes, Servicios u Obras Contratación Directa y **ABSP15** - Adquisición de Bienes, Servicios u Obras Invitación Privada e Invitación Pública, asegurando el cumplimiento de las directrices institucionales.
8. El proveedor deberá conocer y firmar el formato **ESG-SSI-F044** – CONTRATO DE ENCARGO DE PROTECCIÓN, TRANSMISIÓN Y TRATAMIENTO DE DATOS PERSONALES, conforme a la ley 1581 y demás normatividad vigente.

	<b>MACROPROCESO ESTRATÉGICO</b>	<b>CÓDIGO: ESG-SSI-M013</b>
	<b>PROCESO GESTIÓN SISTEMAS INTEGRADOS – SEGURIDAD DE LA INFORMACIÓN</b>	<b>VERSIÓN: 4</b>
	<b>MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS</b>	<b>VIGENCIA: 2025-12-05</b>
		<b>PAGINA: 10 de 15</b>

## **7. CONDICIONES DE SEGURIDAD DE LA INFORMACIÓN A IMPLEMENTAR**

### **7.1 CONTROL DE ACCESO**


1. Los supervisores y/o interventores de los contratos deben realizar una descripción de la información que se va a suministrar o a la que va a tener acceso el proveedor como parte del servicio contratado.
2. Los supervisores y/o interventores deberán solicitar al proveedor la lista del personal autorizado con sus correos corporativos, para tener acceso a la información de la institución.
3. Los supervisores y/o interventores con accesos otorgados a los terceros o proveedores deben estar alineados con las necesidades de la ejecución del contrato, evitando en todo momento el acceso innecesario a la información y cumpliendo el criterio de acceder a la información mínima necesaria para el desarrollo de las actividades planeadas. Lo anterior se puede aplicar tanto al ámbito físico como lógico.

## **8. REQUISITOS DE SEGURIDAD PARA EXIGIR A LOS PROVEEDORES DURANTE LA VIGENCIA DEL CONTRATO**

Se deben establecer y acordar todos los requisitos de ejecución de contrato u orden contractual de seguridad de la información pertinentes, con cada proveedor, contratista que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura tecnológica para la información de la institución.

Los siguientes términos, sin limitarse a ellos, se deben incluir en los acuerdos del contrato, con el fin de satisfacer los requisitos de seguridad de la información durante la vigencia del contrato o prestación del servicio:

1. Responsable de seguridad: Requerir al proveedor contratista la designación de un responsable de seguridad quien servirá de interlocutor para cualquier tema de seguridad y el responsable de que se cumplan los controles pactados entre las partes.
2. Control del personal: Requerir al proveedor, contratista que mantenga informado de cualquier cambio de personal dedicado a la prestación de servicios dentro del acuerdo firmado.
3. Gestión de incidentes: se debe documentar la obligación del proveedor, contratista de reportar y demostrar la gestión oportuna sobre incidentes de seguridad de la información relacionados con el objeto del servicio contratado

	<b>MACROPROCESO ESTRATÉGICO</b>	<b>CÓDIGO: ESG-SSI-M013</b>
	<b>PROCESO GESTIÓN SISTEMAS INTEGRADOS – SEGURIDAD DE LA INFORMACIÓN</b>	<b>VERSIÓN: 4</b>
	<b>MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS</b>	<b>VIGENCIA: 2025-12-05</b>
		<b>PAGINA: 11 de 15</b>

de acuerdo con el procedimiento **ESG-SSI-P09** - GESTIÓN DE EVENTOS Y/O INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.

4. Obligaciones del personal: dentro de los acuerdos contractuales se pueden incluir las siguientes obligaciones, pero sin limitar a:
  - a) Conocer y cumplir con los lineamientos definidos en el **ESG-SSI-M001** MANUAL DE LINEAMIENTOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
  - b) Firmar el acuerdo de confidencialidad y mantener el acuerdo aun después de terminar la relación contractual.
  - c) Los demás requisitos que se consideren necesarios para la prestación del servicio.
5. Control del supervisor(a): Realizar el diligenciamiento del formulario **ABSF146** - EVALUACIÓN DE PROVEEDORES.

## 9. FLUJO DE COMUNICACIÓN PARA PROVEEDORES Y/O TERCEROS


La Universidad de Cundinamarca en concertación con el proveedor, área técnica, supervisor, contratista o tercero, deben determinar los roles y responsabilidades de ambas partes en el proceso contractual.

### Responsabilidades de la Universidad de Cundinamarca:

- Designar un representante o encargado de contratos para actuar como punto de contacto principal con los proveedores/terceros/área técnica/supervisor.
- Proporcionar información precisa y completa sobre los requisitos del contrato.
- Cumplir con los plazos y compromisos establecidos en el contrato.
- Revisar y responder de manera oportuna a las comunicaciones y consultas de los proveedores/terceros.

### Responsabilidades de los Proveedores/Contratistas/Terceros:

- Designar un representante principal para el contacto con la Universidad.
- Comunicar de manera clara cualquier desviación o problema en la ejecución del contrato.
- Cumplir con las obligaciones contractuales y los plazos acordados.
- Mantener la confidencialidad de la información proporcionada por la Universidad.


	MACROPROCESO ESTRATÉGICO	CÓDIGO: ESG-SSI-M013
	PROCESO GESTIÓN SISTEMAS INTEGRADOS – SEGURIDAD DE LA INFORMACIÓN	VERSIÓN: 4
	MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS	VIGENCIA: 2025-12-05
		PAGINA: 12 de 15

## 10. FINALIZACIÓN DEL SERVICIO

Dentro de los acuerdos o anexos contractuales, debe quedar documentado la finalización de los acuerdos de servicio, trabajos o relación contractual, esta no supone la finalización de las obligaciones en materia de confidencialidad de la información. Por esta razón, se define a través del Acuerdo de Confidencialidad para Proveedores y Terceros, CLAUSULA SÉPTIMA. DURACIÓN DEL ACUERDO, tres (3) años, como el tiempo mínimo de confidencialidad posterior a la terminación del contrato.


Por otro lado, durante la etapa postcontractual, el supervisor debe garantizar los siguientes controles:

- Realizar el diligenciamiento del formulario **ABSF145** – REEVALUACIÓN DE PROVEEDORES.
- La eliminación o supresión de datos mediante certificación que debe entregar el proveedor al supervisor de acuerdo con la temporalidad del dato y como se documentó en el contrato.
- La entrega de la información generada por el proveedor deberá quedar documentada en el acuerdo final
- El supervisor debe solicitar la cancelación y revocación de los accesos físicos o lógicos de acuerdo al procedimiento **ASIP20** - GESTIÓN DE ACCESO A LOS SISTEMAS DE INFORMACIÓN, RECURSOS Y SERVICIOS TECNOLÓGICOS y el manual **ESG-SSI-M010** “MANUAL POLÍTICA DE CONTROL DE ACCESO FÍSICO A ÁREAS SEGURAS”.


	<b>MACROPROCESO ESTRATÉGICO</b>	<b>CÓDIGO: ESG-SSI-M013</b>
	<b>PROCESO GESTIÓN SISTEMAS INTEGRADOS – SEGURIDAD DE LA INFORMACIÓN</b>	<b>VERSIÓN: 4</b>
	<b>MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS</b>	<b>VIGENCIA: 2025-12-05</b>
		<b>PAGINA: 13 de 15</b>

## 11. BIBLIOGRAFÍA Y WEBGRAFÍA

- DEPARTAMENTO NACIONAL DE PLANEACIÓN, Consejo Nacional De Política Económica y Social República De Colombia, CONPES 3854 de 2016 [sitio web]. Bogotá D.C.  
[Consultado: 4 de agosto de 2022]. Disponible en:  
<https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>
- ESG-SSI-M011 MANUAL POLÍTICA DE USO ACEPTABLE DE ACTIVOS DE INFORMACIÓN – RUTA: MODELO DE OPERACIÓN DIGITAL / MACROPROCESO ESTRATÉGICO / SISTEMAS INTEGRADOS / SEGURIDAD DE LA INFORMACIÓN
- Galán, J. S. (2018, noviembre 5). Proveedor. Economipedia.  
<https://economipedia.com/definiciones/proveedor.html>.
- INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Sistemas de Gestión de Seguridad de la Información, Requisitos. ISO/IEC 27001. Bogotá D.C.: El Instituto, 2014. 30 p.
- MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN. Guía para la Gestión y Clasificación de Activos de Información. [Sitio web] Bogotá D.C: MINTIC.  
[Consultado: 11 julio 2021] Disponible en:  
[https://www.mintic.gov.co/gestionti/615/articles482\\_G5\\_Gestion\\_Clasificacio](https://www.mintic.gov.co/gestionti/615/articles482_G5_Gestion_Clasificacio)  
n.pdf

	<b>MACROPROCESO ESTRATÉGICO</b>		<b>CÓDIGO: ESG-SSI-M013</b>
	<b>PROCESO GESTIÓN SISTEMAS INTEGRADOS – SEGURIDAD DE LA INFORMACIÓN</b>		<b>VERSIÓN: 4</b>
	<b>MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS</b>		<b>VIGENCIA: 2025-12-05</b>
			<b>PAGINA: 14 de 15</b>

CONTROL DE CAMBIOS				
VERSIÓN	FECHA DE APROBACIÓN			DESCRIPCIÓN DEL CAMBIO
	AAAA	MM	DD	
1	2023	12	11	Emisión del documento.
2	2025	04	24	<p>-Según la resolución rectoral 074 del 22 de julio del 2024, dando cumplimiento a la ley 2345 del 2023 "chao marcas" y dando alcance a la circular 006 "Cambio de identificador visual en los documentos de gestión documental" se realiza el cambio de logo en el documento.</p> <p>- Cambio en la introducción de acuerdo con la norma ISO/IEC 27001:2022</p> <p>-Modificación en el objetivo general y los objetivos específicos</p> <p>-Modificación en el alcance</p> <p>-Modificación en el numeral dos de los "LINEAMIENTOS GENERALES" se agregan las resoluciones 206 del 27 de noviembre y la Resolución 170 que modifica la resolución 206.</p> <p>-Modificación en el numeral tres de los "LINEAMIENTOS GENERALES" donde se menciona el manual ESG-SSI-M001 ya que su nombre se actualizo.</p> <p>-Modificación en el numeral cuatro de los "LINEAMIENTOS GENERALES" que va dirigido nada más a los contratistas, se debe dirigir también a el supervisor o área técnica.</p> <p>-Modificación en el numeral cinco de los "LINEAMIENTOS GENERALES" que va dirigido solo al contratista</p> <p>-Se agrega el numeral siete de los "LINEAMIENTOS GENERALES" que va dirigido al contratista en el cumplimiento de los controles en los procesos.</p> <p>-Se modifiko el título "CONDICIONES DE SEGURIDAD QUE SE DEBEN DEFINIR ANTES DE LA FIRMA DE CONTRATOS" por "CONDICIONES DE SEGURIDAD DE LA INFORMACIÓN A IMPLEMENTAR"</p> <p>- Se agrego el formulario "ABSF146 – EVALUACIÓN DE PROVEEDORES" en los "REQUISITOS DE SEGURIDAD PARA EXIGIR A LOS PROVEEDORES DURANTE LA VIGENCIA DEL CONTRATO"</p> <p>-Se modifica el Párrafo inicial de "FLUJO DE COMUNICACIÓN PARA</p>

	<b>MACROPROCESO ESTRATÉGICO</b>		<b>CÓDIGO: ESG-SSI-M013</b>
	<b>PROCESO GESTIÓN SISTEMAS INTEGRADOS – SEGURIDAD DE LA INFORMACIÓN</b>		<b>VERSIÓN: 4</b>
	<b>MANUAL – LINEAMIENTO DE SEGURIDAD DE LA INFORMACIÓN CON RELACIÓN A LOS PROVEEDORES Y/O TERCEROS</b>		<b>VIGENCIA: 2025-12-05</b>
			<b>PAGINA: 15 de 15</b>

				PROVEEDORES Y/O TERCEROS” al agregar “área técnica, supervisor” -Para la “FINALIZACIÓN DEL SERVICIO” se modificó el lugar donde iba, por su contenido se deja al final del documento y Se agrego el formulario “ABSF145 – REEVALUACIÓN DE PROVEEDORES”.
3	2025	06	18	Se estructuro la redacción en los “LINEAMIENTOS GENERALES” en su numeral 7 y de igual manera se agregó el numeral 8.
4	2025	12	05	-Durante todo el documento se ajustó la nomenclatura correspondiente a la norma, reemplazando la referencia <b>ISO 27001:2022</b> por <b>ISO/IEC 27001:2022</b> , conforme a la denominación técnica oficial. -Asimismo, en el ítem 2 de los lineamientos generales se incorporó la referencia al formato <b>ESG-SSI-F020 – Acuerdo de Confidencialidad para Proveedores y Terceros</b> , con el fin de fortalecer los controles aplicables a las partes externas vinculadas.

ELABORÓ				
NOMBRES Y APELLIDOS		CARGO		
Duván Felipe Castillo Avila		Técnico		
REVISÓ				
NOMBRES Y APELLIDOS		CARGO		
María del Pilar Delgado Rodríguez		Coordinadora del Sistema de Gestión de seguridad de la Información – SGSI		
APROBÓ (GESTOR RESPONSABLE DEL PROCESO)				
NOMBRES Y APELLIDOS	CARGO	FECHA		
		AAAA	MM	DD
María del Pilar Delgado Rodríguez	Coordinadora del Sistema de Gestión de seguridad de la Información – SGSI	2025	12	05