UNIVERSIDAD DE CUNDINAMARCA

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

FUSAGASUGÁ
2023

UNIVERSIDAD DE CUNDINAMARCA

Elaborado por: SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI

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

FUSAGASUGÁ
2023

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Los proveedores, contratistas y partes interesadas hacen parte esencial del desempeño de las instituciones, inciden 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 y disponibilidad de la información que se compartirá.

El presente lineamiento tiene como propósito establecer el marco de gestión y relación entre la Universidad de Cundinamarca con sus proveedores y/o terceros, la cual busca establecer requisitos que deben cumplir, para garantizar la protección de los datos y la seguridad de la información compartida. Este lineamiento tiene como referencia lo expuesto en el control A.15 Relación con Proveedores del Anexo A de la norma ISO /IEC 27001:2013.

2. OBJETIVO GENERAL

Establecer los lineamientos que permitan la relación con los proponentes; proveedores, contratistas, partes interesadas, de acuerdo con los objetivos estratégicos de la institución. El presente lineamiento establece las directrices y controles a implementar para proteger los activos de Información de la institución, a los cuales tendrán acceso los proveedores, respecto a interceptaciones, copia, modificación, divulgación y/o destrucción no autorizada, para garantizar la Confidencialidad, Integridad y Disponibilidad de la Información, durante las etapas precontractual, contractual y poscontractual del servicio contratado.

2.1 OBJETIVOS ESPECÍFICOS

- Establecer protocolos de respuesta claros y efectivos en caso de que se produzcan violaciones de seguridad de la información por parte de los proveedores-contratistas.

- Definir las condiciones que se deben tener en cuenta en la etapa precontractual, contractual y poscontractual con el proveedor-contratista.

- Evaluar y seleccionar proveedores-contratistas en función de su capacidad para cumplir con los requisitos de seguridad de la información establecidos en la política.

3. ALCANCE

Este lineamiento es aplicable a todos los proveedores-contratistas (persona natural o jurídica) que tengan acceso a los sistemas de información o a los recursos que manejan activos de información, en todos los procesos de la organización incluyendo sede, seccionales, extensiones, oficina de Bogotá, unidades agroambientales y el Centro Académico Deportivo – CAD de la Universidad de Cundinamarca.

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**.**[1]

CONFIDENCIALIDAD: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados según sea requerida.[2]

DISPONIBILIDAD: Propiedad que determina que la información sea accesible y utilizable por solicitud de una persona o entidad autorizada, cuando ésta así lo Requiera.[3]

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.[4]

INTEGRIDAD: La propiedad de salvaguardar la exactitud y complejidad de la Información.[5]

---

[1] 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

[2] 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.

[3] 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

[4] 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

[5] NSTITUTO 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.

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.[6]

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.

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. [7]

SGSI: Sistema de Gestión de Seguridad de la Información.[8]

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

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

[6] https://economipedia.com/definiciones/proveedor.html
[7] https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en
[8] ídem

ámbito del objeto u orden contractual, para que, de esta manera, se preserve la Confidencialidad, Integridad y Disponibilidad de la información.

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, que involucre el acceso a los activos de información de la Universidad de Cundinamarca, deberán firmar el respectivo acuerdo de confidencialidad.
3. Es responsabilidad de los 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 POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.
4. Todo proveedor; contratista 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 sí 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. Los proveedores; contratista sólo podrán desarrollar para a la Universidad de Cundinamarca aquellas actividades cubiertas bajo el correspondiente contrato u orden contractual de desempeño 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. CONDICIONES DE SEGURIDAD QUE SE DEBEN DEFINIR ANTES DE LA FIRMA DE CONTRATOS

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 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.

7.2 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:

a) La devolución de los activos de información se debe realizar mediante el ESG-SSI-F010 - CHECKLIST PARA ENTREGA Y DEVOLUCIÓN DE ACTIVOS DE LA INFORMACIÓN.
b) 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 documente en el contrato.
c) La entrega de la información generada por el proveedor deberá quedar documentada en el contrato de acuerdo al objeto del mismo. (si aplica)
d) 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”.

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 de acuerdo con el procedimiento ESG-SSI-P09 - GESTIÓN DE 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 POLÍTICAS 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.

9. FLUJO DE COMUNICACIÓN PARA PROVEEDORES Y/O TERCEROS

La Universidad de Cundinamarca en concertación con el proveedor, 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.
- 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.

10. 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_Clasificacion.pdf

CONTROL DE CAMBIOS				
VERSIÓN	FECHA DE APROBACIÓN			DESCRIPCIÓN DEL CAMBIO
	AAAA	MM	DD	
1	2023	12	11	Emisión del documento.

ELABORÓ	
NOMBRES Y APELLIDOS	CARGO
Gustavo Adolfo Domínguez Sierra	Técnico
Juan Diego Burrell Tovar	Técnico

REVISÓ	
NOMBRES Y APELLIDOS	CARGO
María del Pilar Delgado Rodríguez	Coordinadora del SGSI

APROBÓ (GESTOR RESPONSABLE DEL PROCESO)				
NOMBRES Y APELLIDOS	CARGO	FECHA		
		AAAA	MM	DD
María del Pilar Delgado Rodríguez	Coordinadora del SGSI	2023	12	11