

	UNIVERSIDAD SURCOLOMBIANA						
	GESTIÓN DE TALENTO HUMANO						
	DIRECTRICES PARA EL CONTROL DE PERSONAS						
CÓDIGO	AP-THU-DR-01	VERSIÓN	1	VIGENCIA	2026	PÁGINA	1 DE 11

1. OBJETIVO

Definir las directrices para:

- garantizar que todos los aspirantes a convertirse en funcionarios administrativos, docentes y/o contratistas, sean elegibles y adecuados para las funciones y las obligaciones contractuales que se consideren aplicables.
- garantizar que los funcionarios administrativos, docentes y/o contratistas vinculados comprendan sus responsabilidades de seguridad y privacidad de la información para las funciones y obligaciones contractuales que se consideren pertinentes.
- garantizar que los funcionarios administrativos, docentes y/o contratistas conozcan y cumplan con sus responsabilidades en materia de seguridad y privacidad de la información.
- garantizar que los funcionarios administrativos, docentes, contratistas y/u otras partes interesadas comprendan las consecuencias de la violación de la política y directrices de seguridad y privacidad de la información, para disuadir y tratar adecuadamente al personal y otras partes interesadas pertinentes que hayan cometido la violación.
- proteger los intereses de la Universidad, como parte del proceso de cambio o terminación de empleo o contrato.
- mantener la confidencialidad de la información accesible por los funcionarios administrativos, docentes, estudiantes, contratistas y/o terceros
- garantizar la seguridad y privacidad de la información cuando los funcionarios administrativos, docentes, estudiantes, contratistas y/o terceros trabajan de forma remota (trabajo en casa.)
- apoyar la notificación oportuna, coherente y eficaz de los eventos de seguridad y privacidad de la información que pueden ser identificados por los funcionarios administrativos, docentes, contratistas y/u otras partes interesadas

2. ALCANCE

Las presentes directrices aplican a todos los aspirantes y/o funcionarios administrativos, docentes, pasantes, judicantes, contratistas, y/o terceros de la Universidad.

Vigilada Mineducación

La versión vigente y controlada de este documento, solo podrá ser consultada a través del sitio web Institucional www.usco.edu.co, link Sistema Gestión de Calidad. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la Universidad Surcolombiana.

	UNIVERSIDAD SURCOLOMBIANA GESTIÓN DE TALENTO HUMANO					   	
	DIRECTRICES PARA EL CONTROL DE PERSONAS						
CÓDIGO	AP-THU-DR-01	VERSIÓN	1	VIGENCIA	2026	PÁGINA	2 DE 11

3. DEFINICIONES

Incidente seguridad: la ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad.

Grupo de interés: son grupos que no forman parte de la empresa, pero están relacionados por la actividad de la misma.

Personal: Personas que trabajan bajo la dirección de la organización.

Seguridad de la información: es el conjunto de medidas y técnicas utilizadas para asegurar la confidencialidad, integridad y disponibilidad de la información.

Usuario: titular de la comunidad Universitaria que cumple con los criterios para hacer uso de los recursos y servicios informáticos.

4. MARCO DE REFERENCIA

La gestión de riesgos y oportunidades en la Universidad Surcolombiana considera para su labor, los lineamientos definidos en las directrices y políticas institucionales, además de las consideraciones definidas en:

- La norma ISO 31000:2018– Gestión del riesgo. Principios y directrices.
- La norma ISO IEC 27005:2022 – Gestión de riesgos para la seguridad de la información.
- Los lineamientos definidos en los documentos del Sistema de Gestión de Seguridad y Privacidad de la Información.
- Los requisitos aplicables a la gestión del riesgo, detallados en el estándar ISO IEC 27001:2022 y la ISO IEC 27701:2025
- Código de Práctica para Controles de Seguridad de la Información - GTC ISO IEC 27002:2022 Tecnología de la Información. Técnicas de Seguridad.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
- Guía de Administración de riesgos y el diseño de controles en entidades públicas
- CONPES de Seguridad Digital (CONPES 3854 de 2016 y actualizaciones)
- Modelo de Seguridad y Privacidad de la Información – MSPI (MinTIC)
- Política de Gobierno Digital (Decreto 1078 de 2015 y actualizaciones)
- Modelo Integrado de Planeación y Gestión – MIPG (DAFP)
- FURAG (Formulario Único de Reporte de Avance de la Gestión)
- Ley 1581 de 2012 y Decreto 1377 de 2013
- Lineamientos y guías de la Superintendencia de Industria y Comercio.

Vigilada Mineducación

La versión vigente y controlada de este documento, solo podrá ser consultada a través del sitio web Institucional www.usco.edu.co, link Sistema Gestión de Calidad. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la Universidad Surcolombiana.

	UNIVERSIDAD SURCOLOMBIANA GESTIÓN DE TALENTO HUMANO						
	DIRECTRICES PARA EL CONTROL DE PERSONAS						
	CÓDIGO	AP-THU-DR-01	VERSIÓN	1	VIGENCIA	2026	PÁGINA

5. GENERALIDADES

Estas directrices son la declaración general que representa la posición de la Universidad, con respecto a la gestión de personal en proceso, durante y después de su vinculación contractual, con base en los siguientes controles de acuerdo a las normas:

ISO/IEC 27001:2022

- A.6.1 Selección
- A.6.2 Términos y condiciones de empleo
- A.6.3 Conciencia de seguridad de la información, educación y formación
- A.6.4 Proceso disciplinario
- A.6.5 Responsabilidades después de la terminación o cambio de empleo
- A.6.6 Acuerdos de confidencialidad o no divulgación
- A.6.7 Trabajo remoto
- A.6.8 Informes de eventos de seguridad de la información

ISO/IEC 27701:2025

- A.3.17 Concienciación, educación y formación en seguridad
- A.3.18 Acuerdos de confidencialidad o no divulgación

6. DIRECTRICES

6.1. SELECCIÓN

A continuación, se establecen las directrices definidas por la Universidad para el proceso de selección de todos los servidores públicos y contratistas.

La verificación de antecedentes de todos los aspirantes aptos debe llevarse a cabo antes de vincularse a la Universidad y de forma continua, tomando en consideración la normatividad interna y externa vigente, la clasificación de la información a la que se va a acceder y los riesgos percibidos. Ver

- ✓ AP-THU-PR-01 VINCULACIÓN Y RETIRO EMPLEADOS PÚBLICOS Y TRABAJADORES OFICIALES
- ✓ AP-THU-FO-12 REQUISITOS PARA LA VINCULACIÓN DEL PERSONAL POR PRESTACIÓN DE SERVICIOS
- ✓ AP-THU-PR-13 VINCULACIÓN Y DESVINCULACIÓN DE CONTRATOS DE PRESTACIÓN DE SERVICIOS

Vigilada Mineducación

La versión vigente y controlada de este documento, solo podrá ser consultada a través del sitio web Institucional www.usco.edu.co, link Sistema Gestión de Calidad. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la Universidad Surcolombiana.



La verificación debe tener en cuenta toda la legislación pertinente en materia de privacidad, protección de los datos personales y basada en el empleo y cuando la circunstancia lo permita, debe incluir lo siguiente:

- a) disponibilidad de referencias personales y/o laborales;
- b) una verificación (para la integridad y exactitud) de la hoja de vida del solicitante;
- c) confirmación de las calificaciones académicas y profesionales declaradas.

Cuando se contrata a una persona para una función específica de seguridad de la información en la Universidad, debe asegurarse que el candidato:

- a) tenga la competencia necesaria para desempeñar el cargo de seguridad;
- b) se pueda confiar en él para asumir el rol, especialmente si el rol es crítico para la Universidad.

Cuando un cargo implique que la persona tenga acceso a instalaciones de procesamiento de información y, en especial, si éstas implican el manejo de información confidencial, la Universidad debe considerar la posibilidad de realizar verificaciones adicionales más detalladas.

En situaciones en las que la verificación no se puede completar de forma oportuna, se deberán implementar controles adicionales hasta que se haya terminado la revisión, por ejemplo:

- a) retraso en la vinculación;
- b) retraso en el despliegue de activos de la institución;
- c) vinculación con acceso reducido;
- d) terminación de la vinculación y/o relación contractual.

Los controles de verificación deben repetirse periódicamente por solicitud de las directivas o por la autoridad competente, para confirmar la idoneidad continua del personal, dependiendo de la criticidad de la función de una persona.

Cuando estas personas se contraten a través de proveedores de servicios, los requisitos de selección se deben incluir en los acuerdos contractuales entre la Universidad y los proveedores.

	UNIVERSIDAD SURCOLOMBIANA						
	GESTIÓN DE TALENTO HUMANO						
	DIRECTRICES PARA EL CONTROL DE PERSONAS						
CÓDIGO	AP-THU-DR-01	VERSIÓN	1	VIGENCIA	2026	PÁGINA	5 DE 11

6.2. CONDICIONES DE LA VINCULACIÓN A LA UNIVERSIDAD

Se deben tomar en consideración las siguientes directrices:

En el proceso de vinculación de los funcionarios administrativos, docentes, pasantes, judicantes, contratistas, y/o terceros de la Universidad, se debe tener en cuenta la política y directrices de seguridad y privacidad de la información de la Universidad y las demás directrices específicas relacionadas con seguridad y privacidad de la información, precisando además los siguientes puntos:

- antes de dar acceso a la información y otros activos asociados, se debe firmar los acuerdos de confidencialidad o no divulgación;
- responsabilidades y derechos legales con respecto a las leyes de derechos de autor o la legislación sobre protección de datos, el Estatuto de Propiedad Intelectual Acuerdo 014 de 2018 y Política de Privacidad de Datos Personales, publicada en el Portal Institucional <https://www.usco.edu.co/es/transparencia/>;
- responsabilidades para el manejo de la información recibida de las partes interesadas;
- acciones a tomar si el personal ignora los requisitos de seguridad y privacidad de la información en la Universidad. (cláusulas de confidencialidad, proceso disciplinario)

La Universidad se asegura que los servidores públicos y contratistas acepten los términos y condiciones relativos a la seguridad y privacidad de la información.

Estos términos y condiciones deben ser apropiados a la naturaleza y el grado de acceso que tengan a los activos de la Universidad asociados con los sistemas y servicios de información. Los términos y condiciones relativos a la seguridad y privacidad de la información deben revisarse cuando cambie la normatividad interna y externa.

6.3. SENSIBILIZACIÓN, EDUCACIÓN Y FORMACIÓN EN MATERIA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.3.1 Sensibilización

La Universidad tiene establecido el ES-SGPI-PG-01 PROGRAMA DE TOMA DE CONCIENCIA en materia de seguridad y privacidad de la información en concordancia con la política y objetivos del Sistema de Gestión de Seguridad y Privacidad de la Información, directrices específicas de cada tema, procedimientos pertinentes y de las lecciones aprendidas de los incidentes de seguridad y privacidad de la información, al igual que el Plan de Capacitación

Vigilada Mineducación

La versión vigente y controlada de este documento, solo podrá ser consultada a través del sitio web Institucional www.usco.edu.co, link Sistema Gestión de Calidad. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la Universidad Surcolombiana.

	UNIVERSIDAD SURCOLOMBIANA						
	GESTIÓN DE TALENTO HUMANO						
	DIRECTRICES PARA EL CONTROL DE PERSONAS						
CÓDIGO	AP-THU-DR-01	VERSIÓN	1	VIGENCIA	2026	PÁGINA	6 DE 11

Institucional el cual incluye temas en materia de seguridad y privacidad de la información <https://www.usco.edu.co/es/transparencia/>.

La sensibilización, la educación y la formación en materia de seguridad y privacidad de la información tiene por objeto sensibilizar a las partes interesadas internas y externas acerca de sus responsabilidades en materia de seguridad y privacidad de la información y de los medios por los que se han cumplido dichas responsabilidades.

El programa de apropiación incluye una serie de actividades de sensibilización a través de canales físicos o virtuales apropiados, como campañas, folletos, carteles, boletines, sitios web, sesiones de información, sesiones informativas y correos electrónicos.

El conocimiento de la seguridad y privacidad de la información abarca aspectos generales como:

- a) el compromiso de la administración con la seguridad y privacidad de la información en toda la Universidad;
- b) familiaridad y necesidades de cumplimiento con respecto a las normas y obligaciones de seguridad y privacidad de la información aplicables, tomando en consideración la Política de Seguridad y Privacidad de la Información y demás directrices, normativa interna y externa vigente;
- c) responsabilidad personal por las propias acciones e inacciones y responsabilidades generales para asegurar o proteger la información que pertenece a la Universidad y a las partes interesadas;
- d) procedimientos básicos de seguridad y privacidad de la información y controles de referencia;
- e) puntos de contacto y recursos para obtener información adicional y asesoramiento sobre cuestiones de seguridad y privacidad de la información, incluidos otros materiales de sensibilización sobre seguridad y privacidad de la información. ES-GSPI-DA-02 GUÍA DE CONTACTO CON GRUPOS DE INTERÉS ESPECIALES.

La comprensión del personal, debe evaluarse al final de una actividad de sensibilización, educación o capacitación para poner a prueba la transferencia de conocimientos y la eficacia del programa de sensibilización, educación y capacitación. Ver

- ✓ EV-CAL-FO-03 REGISTRO Y CONTROL ASISTENCIA DE ACTIVIDAD YO EVENTO
- ✓ AP-THU-FO-05 EVALUACIÓN DE LA EFICACIA EFICIENCIA O EFECTIVIDAD DE LA CAPACITACIÓN

	UNIVERSIDAD SURCOLOMBIANA GESTIÓN DE TALENTO HUMANO						
	DIRECTRICES PARA EL CONTROL DE PERSONAS						
	CÓDIGO	AP-THU-DR-01	VERSIÓN	1	VIGENCIA	2026	PÁGINA

6.3.2 Educación y formación

La Universidad define el Plan de Capacitación Institucional a partir de la detección de necesidades por dependencias, jefes de área, funciones y necesidades de capacitación individual incluyendo temas de seguridad y privacidad de la información que permiten mejorar las habilidades necesarias para configurar y mantener el nivel de seguridad y privacidad de la información y otros activos asociados de información a nivel institucional. Ver

- ✓ AP-THU-FO-24 SOLICITUD INDIVIDUAL DE AVAL PARA CAPACITACIÓN.
- ✓ AP-THU-FO-30 DETECCIÓN DE NECESIDADES A PARTIR DE FUNCIONES
- ✓ AP-THU-FO-31 DETECCIÓN DE NECESIDADES POR DEPENDENCIAS.
- ✓ AP-THU-FO-32 DETECCIÓN DE NECESIDADES JEFES DE ÁREA.

6.4. PROCESO DISCIPLINARIO

La Universidad ejercerá como mecanismos de prevención para evitar la violación y/o incumplimiento de la Política del Sistema de Gestión de Seguridad y Privacidad de la Información y directrices específicas de seguridad y privacidad de la información, la función de advertencia y la preservación del orden interno y en caso de que se presente incumplimiento y/o violación a la política y directrices de manera reiterativa, se iniciará el respectivo proceso disciplinario según corresponda. Ver

- ✓ EV-CDI-PR-03 PROCEDIMIENTO ORDINARIO – LEY 1952 DE 2019,
- ✓ EV-CDI-PR-04 PROCEDIMIENTO ESPECIAL VERBAL – LEY 1952 DE 2019.

6.5. DIRECTRICES SOBRE RESPONSABILIDADES DESPUÉS DE LA TERMINACIÓN O CAMBIO DE EMPLEO

Las disposiciones legales, responsabilidades y deberes de seguridad y privacidad de la información (confidencialidad de la información, la propiedad intelectual y otros conocimientos obtenidos o relacionados, así como las responsabilidades contenidas en cualquier otro acuerdo de confidencialidad), seguirán siendo válidos aun después de la desvinculación y/o terminación contractual.

Al momento de cambio de funciones y/u obligaciones contractuales, desvinculación o terminación del contrato, la Oficina de Talento Humano debe:

- a) informar a las dependencias involucradas sobre novedades de traslados de dependencia, licencias por períodos prolongados, licencias no remuneradas desvinculación de funcionarios administrativos, docentes y/o terminación de contratos de prestación de servicios, con el propósito de que se actualicen los permisos asignados a los recursos de red, sistemas de información de la Universidad y/o inactivar cuentas de correo electrónico.

	UNIVERSIDAD SURCOLOMBIANA GESTIÓN DE TALENTO HUMANO					 ISO 9001		 ISO 14001	 ISO 45001	 IONET
	DIRECTRICES PARA EL CONTROL DE PERSONAS									
	CÓDIGO	AP-THU-DR-01	VERSIÓN	1	VIGENCIA	2026	PÁGINA	8 DE 11		

- b) solicitar a través del Jefe inmediato y/o supervisor del contrato a funcionarios administrativos, docentes y contratistas copia de respaldo de la información a su cargo durante la vinculación con la Universidad, como requisito para la firma del paz y salvo y/o acta de liquidación del contrato.

6.6. DIRECTRICES SOBRE ACUERDOS DE CONFIDENCIALIDAD O NO DIVULGACIÓN

Los acuerdos de confidencialidad o no divulgación, tienen como objetivo proteger la información confidencial y activos asociados, utilizando términos legalmente exigibles tanto para personas naturales y jurídicas. Estos acuerdos son aplicables además de las anteriores, a las partes interesadas y al personal de la Universidad, al punto de los requisitos de seguridad y privacidad de la información. Los términos de los acuerdos deben determinarse tomando en consideración el tipo de información que se trate, su nivel de clasificación, su uso y el acceso permitido por la otra parte.

Para identificar los requisitos de los acuerdos de confidencialidad o no divulgación, deben considerarse las siguientes directrices:

- a) una definición de la información que se va a proteger;
- b) la duración prevista de un acuerdo, incluidos los casos en que puede ser necesario mantener la confidencialidad indefinidamente o hasta que la información esté disponible públicamente;
- c) las responsabilidades y acciones de los servidores públicos y contratistas para evitar la divulgación de información no autorizada;
- d) la propiedad de la información, los secretos comerciales y la propiedad intelectual y cómo se relaciona con la protección de la información confidencial;
- e) el uso permitido de información confidencial y los derechos del signatario a utilizar la información;
- f) el derecho a auditar y supervisar actividades que impliquen información confidencial en circunstancias muy sensibles;
- g) el proceso para la notificación no autorizada o fuga de información confidencial;
- h) los términos de la información que se devolverá o destruirá en el momento de la terminación del acuerdo;
- i) las medidas previstas en caso de incumplimiento del acuerdo.

	UNIVERSIDAD SURCOLOMBIANA						
	GESTIÓN DE TALENTO HUMANO						
	DIRECTRICES PARA EL CONTROL DE PERSONAS						
CÓDIGO	AP-THU-DR-01	VERSIÓN	1	VIGENCIA	2026	PÁGINA	9 DE 11

j) La Universidad tiene en cuenta el cumplimiento de los acuerdos de confidencialidad y no divulgación.

k) Los requisitos para los acuerdos de confidencialidad y no divulgación deben revisarse periódicamente y cuando se produzcan cambios que influyan en estos requisitos.

6.7. TRABAJO REMOTO

El trabajo remoto, se presenta cuando el personal de la Universidad trabaja desde un lugar fuera de las instalaciones de la Institución y accede a información ya sea en papel o electrónicamente a través de equipos de TIC.

La Universidad tiene establecida la AP-THU-DR-02 DIRECTRICES PARA EL TRABAJO REMOTO que define las condiciones y restricciones pertinentes.

6.8. DIRECTRICES SOBRE INFORMES DE EVENTOS DE SEGURIDAD DE LA INFORMACIÓN

La Universidad cuenta con:

- ✓ ES-GSPI-DR-01 DIRECTRICES PARA LA GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- ✓ ES-GSPI-PR-01 GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, para informar sobre los eventos de seguridad de la información.

funcionarios administrativos, docentes, pasantes, judicantes, contratistas, y/o terceros deben ser conscientes de la responsabilidad de informar sobre los eventos y/o incidentes de seguridad y privacidad de la información de manera oportuna a través del correo institucional incidentesseguridadinformación@usco.edu.co adjuntando el formato ES-GSPI-FO-03 REPORTE DE EVENTOS E INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, para evitar o minimizar el efecto de los incidentes de seguridad y privacidad de la información.

Entre las situaciones que se deberían tener en cuenta para los reportes de eventos y/o incidentes de seguridad y privacidad de la información se incluyen:

- a) controles de seguridad y privacidad de la información ineficaces;
- b) incumplimiento de las expectativas de confidencialidad, integridad o disponibilidad de la información;

Vigilada Mineducación

La versión vigente y controlada de este documento, solo podrá ser consultada a través del sitio web Institucional www.usco.edu.co, link Sistema Gestión de Calidad. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la Universidad Surcolombiana.

	UNIVERSIDAD SURCOLOMBIANA					 ISO 9001		 ISO 14001	 ISO 45001	 IONET
	GESTIÓN DE TALENTO HUMANO									
	DIRECTRICES PARA EL CONTROL DE PERSONAS									
CÓDIGO	AP-THU-DR-01	VERSIÓN	1	VIGENCIA	2026	PÁGINA	10 DE 11			

- c) errores humanos;
- d) incumplimiento de la política y directrices de seguridad y privacidad de la información, y demás normas aplicables;
- e) infracciones de las medidas de seguridad física;
- f) cambios del sistema que no han pasado por el proceso de gestión de cambios;
- g) fallas de funcionamiento u otro comportamiento anómalo del software o hardware en el sistema;
- h) infracciones de acceso;
- i) vulnerabilidades;
- j) sospecha de infección de malware.

A los funcionarios administrativos, docentes, pasantes, judicantes, contratistas, y/o terceros les está totalmente prohibido intentar probar posibles vulnerabilidades de seguridad y privacidad de la información. Tales intentos, se interpretarán como un posible mal uso del sistema, como quiera que, su intento puede causar daños a estos u ocultar las pruebas digitales. En última instancia, esto puede resultar, en responsabilidad legal de todo orden, para la persona que realice el intento.

7. RESPONSABILIDADES Y AUTORIDADES

Los funcionarios administrativos, docentes, estudiantes, pasantes, judicantes, contratistas y/o terceros deben cumplir con la política y directrices de seguridad y privacidad de la información definidas por la Universidad Surcolombiana; así mismo, deben reportar a los propietarios de la información y otros activos asociados las violaciones a la política, directrices y/o cualquier inconsistencia o irregularidad que pueda ser generada por los usuarios.

Los líderes de procesos y propietarios de la información y otros activos de la información deben revisar periódicamente los riesgos que se identifiquen sobre el uso inadecuado de los activos.

8. DOCUMENTOS RELACIONADOS Y REGISTROS

AP-THU-FO-06 EVALUACIÓN DEL DESEMPEÑO LABORAL NIVEL ASISTENCIAL
AP-THU-PR-08 INDUCCIÓN, ENTRENAMIENTO Y REINDUCCIÓN
AP-THU-PR-09 TRAMITE DE VINCULACIÓN, RETIRO Y NÓMINA DE CATEDRA

Vigilada Mineducación

La versión vigente y controlada de este documento, solo podrá ser consultada a través del sitio web Institucional www.usco.edu.co, link Sistema Gestión de Calidad. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la Universidad Surcolombiana.



UNIVERSIDAD SURCOLOMBIANA GESTIÓN DE TALENTO HUMANO



DIRECTRICES PARA EL CONTROL DE PERSONAS

CÓDIGO

AP-THU-DR-01

VERSIÓN

1

VIGENCIA

2026

PÁGINA

**11 DE
11**

AP-THU-PR-11 CREACIÓN, ADMINISTRACIÓN Y CUSTODIA DE HISTORIAS LABORALES

AP-THU-PR-12 TRAMITE DE VINCULACIÓN, RETIRO Y NÓMINA DE DOCENTES VISITANTES Y DOCENTES OCASIONALES

AP-THU-PR-13 VINCULACIÓN Y DESVINCULACIÓN DE CONTRATOS DE PRESTACIÓN DE SERVICIOS

AP-THU-PR-15 EVALUACIÓN DE DESEMPEÑO LABORAL DEL PERSONAL ADMINISTRATIVO

AP-THU-FO-18 LISTA DE CHEQUEO PARA VINCULACIÓN DE PERSONAL

AP-THU-FO-23 REQUISITOS PARA LA VINCULACIÓN DE DOCENTES OCASIONALES Y VISITANTES TC Y MT

AP-THU-FO-28 EVALUACIÓN DE LA INDUCCIÓN A SERVIDORES PÚBLICOS

ES-GSPI-DA-02 GUÍA DE CONTACTO CON LAS AUTORIDADES Y GRUPOS DE INTERES ESPECIAL

EV-CAL-FO-03 REGISTRO Y CONTROL ASISTENCIA DE ACTIVIDAD YO EVENTO

AP-THU-FO-05 EVALUACIÓN DE LA EFICACIA EFICIENCIA O EFECTIVIDAD DE LA CAPACITACIÓN

ES-GSPI-PR-01 GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ES-GSPI-DR-01 DIRECTRICES PARA LA GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ES-GSPI-FO-03 REPORTE DE EVENTOS Y/O INCIDENTES DE SEGURIDAD Y/O PRIVACIDAD DE LA INFORMACIÓN

AP-THU-DR-02 DIRECTRICES PARA EL TRABAJO REMOTO

CONTROL DE CAMBIO

VERSIÓN	DOCUMENTO Y FECHA DE APROBACIÓN	DESCRIPCION DE CAMBIOS
01	EV-CAL-FO 17 - 24 de agosto de 2026	Creación documento – Requisito NTC ISO IEC 27001 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de la Seguridad de la Información

ELABORÓ	REVISÓ	APROBÓ
MARTHA LILIANA HERMOSA TRUJILLO Gestión Seguridad y Privacidad de la Información Elaboró TANIA BEATRIZ PEÑAFIEL ESPAÑA Líder Oficina Talento Humano Aprobó	ERIKA FERNANDA HERRERA RAMIREZ Profesional de Apoyo SGC	MAYRA ALEJANDRA BERMEO BALAGUERA Asesora en la Coordinador del SGC

Vigilada Mineducación

La versión vigente y controlada de este documento, solo podrá ser consultada a través del sitio web Institucional www.usco.edu.co, link Sistema Gestión de Calidad. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la Universidad Surcolombiana.