

|                                                                                   |                                                                                                     |                |          |                 |             |                                                                                     |                |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------|----------|-----------------|-------------|-------------------------------------------------------------------------------------|----------------|
|  | <b>UNIVERSIDAD SURCOLOMBIANA</b><br><b>GESTIÓN DE INFORMACIÓN, TECNOLOGÍAS Y CONTROL DOCUMENTAL</b> |                |          |                 |             |  |                |
|                                                                                   | <b>DIRECTRICES PARA PROTECCION FISICA DE ACTIVOS DE INFORMACION</b>                                 |                |          |                 |             |                                                                                     |                |
| <b>CÓDIGO</b>                                                                     | <b>AP-TIC-DR-08</b>                                                                                 | <b>VERSIÓN</b> | <b>1</b> | <b>VIGENCIA</b> | <b>2026</b> | <b>Página</b>                                                                       | <b>1 de 14</b> |

## 1. OBJETIVOS

- a) Garantizar únicamente la divulgación, modificación, eliminación o destrucción autorizada de la información en los medios de almacenamiento.
- b) Evitar fugas de información del equipo que se va a desechar o reutilizar.
- c) Evitar la pérdida, daño o compromiso de información y otros activos asociados o la interrupción de las operaciones de la Universidad Surcolombiana debido a:
  - fracaso y la interrupción de los servicios públicos de respaldo.
  - cableado de alimentación y comunicaciones.

## 2. ALCANCE

Aplica a funcionarios administrativos, docentes, estudiantes, pasantes, judicantes, contratistas y terceros que utilicen, custodien, administren o tengan acceso a activos de información de la Universidad Surcolombiana.

## 3. DEFINICIONES

**Activo tecnológico:** Activo tecnológico: Equipo, dispositivo, infraestructura o recurso tecnológico utilizado para procesar, almacenar, transmitir o soportar información institucional.

**Control físico:** Medida de seguridad implementada para proteger físicamente las instalaciones, equipos, dispositivos, medios e información frente a accesos no autorizados, daños, pérdida o interrupciones.

**Medio de almacenamiento:** Elemento utilizado para almacenar información, de manera temporal o permanente, como discos duros, memorias USB, discos externos, cintas, tarjetas de memoria y otros medios.

|                                                                                   |                                                                                                     |                |          |                 |             |                                                                                     |                |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------|----------|-----------------|-------------|-------------------------------------------------------------------------------------|----------------|
|  | <b>UNIVERSIDAD SURCOLOMBIANA</b><br><b>GESTIÓN DE INFORMACIÓN, TECNOLOGÍAS Y CONTROL DOCUMENTAL</b> |                |          |                 |             |  |                |
|                                                                                   | <b>DIRECTRICES PARA PROTECCION FISICA DE ACTIVOS DE INFORMACION</b>                                 |                |          |                 |             |                                                                                     |                |
| <b>CÓDIGO</b>                                                                     | <b>AP-TIC-DR-08</b>                                                                                 | <b>VERSIÓN</b> | <b>1</b> | <b>VIGENCIA</b> | <b>2026</b> | <b>Página</b>                                                                       | <b>2 de 14</b> |

**Protección física:** Conjunto de medidas destinadas a proteger los activos de información frente a pérdida, daño, robo, destrucción, acceso físico no autorizado o afectaciones ambientales.

**Seguridad física:** Conjunto de políticas, procedimientos, controles y medidas destinadas a proteger personas, instalaciones, equipos, medios e información frente a amenazas físicas y ambientales.

#### 4. MARCO 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.

|                                                                                   |                                                                                                     |                |          |                 |             |                                                                                                                                                                                                                                                                                                                                                 |                |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------|----------|-----------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
|  | <b>UNIVERSIDAD SURCOLOMBIANA</b><br><b>GESTIÓN DE INFORMACIÓN, TECNOLOGÍAS Y CONTROL DOCUMENTAL</b> |                |          |                 |             |     |                |
|                                                                                   | <b>DIRECTRICES PARA PROTECCION FISICA DE ACTIVOS DE INFORMACION</b>                                 |                |          |                 |             |                                                                                                                                                                                                                                                                                                                                                 |                |
| <b>CÓDIGO</b>                                                                     | <b>AP-TIC-DR-08</b>                                                                                 | <b>VERSIÓN</b> | <b>1</b> | <b>VIGENCIA</b> | <b>2026</b> | <b>Página</b>                                                                                                                                                                                                                                                                                                                                   | <b>3 de 14</b> |

## 5. GENERALIDADES

Estas directrices son la declaración general que representa la posición de la Universidad, con respecto a los controles físicos de acceso a la información y otros activos asociados de la información, con base en los siguientes controles de acuerdo a las normas:

ISO/IEC 27001:2022

- A.7.7 Escritorio y pantalla limpios
- A.7.8 Ubicación y protección de equipos
- A.7.9 Seguridad de los activos fuera de las instalaciones
- A.7.10 Medios de almacenamiento
- A.7.11 Servicios públicos de apoyo
- A.7.12 Seguridad del cableado
- A.7.13 Mantenimiento del equipo
- A.7.14 Disposición o reutilización segura de los equipos

ISO/IEC 27701:2025

- A.3.19 Escritorio limpio y pantalla limpia

## 6. DIRECTRICES

### 6.1. ESCRITORIO LIMPIO Y PANTALLA LIMPIA

Los funcionarios administrativos, docentes, estudiantes, contratistas, judicantes, pasantes y/o terceros de la Universidad Surcolombiana deben:

- a) al levantarse del puesto de trabajo y al finalizar la jornada laboral, los escritorios deben permanecer despejados y libres de documentos físicos y/o medios extraíbles que contengan información clasificada confidencial o de uso reservado que haya sido utilizada, sin importar el medio en que se encuentre (papel, discos, medios magnéticos) éstos deben guardarse en un lugar seguro y bajo llave. Los documentos y/o medios extraíbles con información pública también deben guardarse para evitar la pérdida de esta información. (Ver ES-GSPI-MR-04 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN DOCUMENTAL, ES-GSPI-MR-05 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN)

|                                                                                   |                                                                                                                                                                                  |              |         |   |          |                                                                                                                                                                                                                                                                                                                                                                                                                                                |        |
|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|---------|---|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------|
|  | <div>UNIVERSIDAD SURCOLOMBIANA</div> <div>GESTIÓN DE INFORMACIÓN, TECNOLOGÍAS Y CONTROL DOCUMENTAL</div> <div>DIRECTRICES PARA PROTECCION FISICA DE ACTIVOS DE INFORMACION</div> |              |         |   |          | <div><br/>ISO 9001</div> <div><br/>SA-CERES 807526</div> <div><br/>CS-CER 807555</div> <div></div> |        |
|                                                                                   | CÓDIGO                                                                                                                                                                           | AP-TIC-DR-08 | VERSIÓN | 1 | VIGENCIA | 2026                                                                                                                                                                                                                                                                                                                                                                                                                                           | Página |

- b) guardar la información sensible o crítica de la Universidad en papel o en medio de almacenamiento electrónico en una caja fuerte o en un gabinete u otro mueble de seguridad cuando no se requiera, especialmente cuando en la oficina no se encuentren funcionarios. (Ver ES-GSPI-MR-04 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN DOCUMENTAL, ES-GSPI-MR-05 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN)
- c) no escribir contraseñas y otros datos sensibles en papeles o documentos que queden a la vista.
- d) no dejar documentos con información de uso interno o confidencial sobre impresoras, copiadoras, multifuncionales y puestos de trabajo.
- e) no utilizar como reciclable el papel que contenga información que sea clasificada confidencial o de uso reservado,
- f) mantener la pantalla del computador limpia y libre de documentación para evitar el espionaje de información sensible. La información clasificada confidencial o de uso reservado debe estar almacenada en directorios diferentes al de escritorio,
- g) mantener los equipos y estaciones de trabajo en buenas condiciones, limpios, ordenados, libres de líquidos y/o comestibles que se puedan derramar y afecten (dañen) la integridad de los equipos y/o documentos.
- h) si la persona autorizada no se encuentra en su puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos, etiquetados como clasificados o de uso reservado, deben ser retirados del escritorio o de otros lugares para evitar el acceso no autorizado a los mismos. Este tipo de documentos y soportes deben ser archivados de forma segura. (Ver ES-GSPI-MR-04 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN DOCUMENTAL, ES-GSPI-MR-05 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN)
- i) los documentos que se impriman en la Universidad Surcolombiana, deben ser de carácter institucional.
- j) mantener control de la impresora en el momento de realizar impresiones de documentos con clasificación confidencial o de uso reservado, preservando la

|                                                                                   |                                                                                                     |                |          |                 |             |                                                                                     |                |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------|----------|-----------------|-------------|-------------------------------------------------------------------------------------|----------------|
|  | <b>UNIVERSIDAD SURCOLOMBIANA</b><br><b>GESTIÓN DE INFORMACIÓN, TECNOLOGÍAS Y CONTROL DOCUMENTAL</b> |                |          |                 |             |  |                |
|                                                                                   | <b>DIRECTRICES PARA PROTECCION FISICA DE ACTIVOS DE INFORMACION</b>                                 |                |          |                 |             |                                                                                     |                |
| <b>CÓDIGO</b>                                                                     | <b>AP-TIC-DR-08</b>                                                                                 | <b>VERSIÓN</b> | <b>1</b> | <b>VIGENCIA</b> | <b>2026</b> | <b>Página</b>                                                                       | <b>5 de 14</b> |

confidencialidad de la información y se deben retirar de la impresora de manera inmediata. (Ver ES-GSPI-MR-04 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN DOCUMENTAL, ES-GSPI-MR-05 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN)

k) las estaciones de trabajo deben apagarse completamente al final de la jornada de trabajo, excepto los equipos del Centro de Información, Tecnologías y Control Documental - CITCD, que se requieran para temas de conexión a los servidores.

l) al levantarse del puesto de trabajo, se debe bloquear la sesión de los equipos de cómputo para proteger el acceso a las aplicaciones y servicios de la Universidad Surcolombiana.

m) los gabinetes, cajones y archivadores que contengan documentos y/o medios extraíbles con información clasificada confidencial o de uso reservado deben quedar cerrados durante la hora de almuerzo y al finalizar la jornada laboral.

n) la información confidencial que haya sido consignada en los tableros de las salas de juntas o de las oficinas durante el desarrollo de reuniones, deberá ser borrada al término de las mismas.

o) los dispositivos de almacenamiento, con información clasificada confidencial o de uso reservado deben quedar desconectados y se deben guardar en lugar seguro. (Ver ES-GSPI-MR-04 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN DOCUMENTAL, ES-GSPI-MR-05 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN)

p) los documentos electrónicos que producen los funcionarios administrativos, docentes, estudiantes, contratistas y/o terceros en el ejercicio de sus funciones deben guardarse en la carpeta de almacenamiento en la red dispuesta por la Universidad Surcolombiana.

## 6.2. UBICACIÓN Y PROTECCIÓN DE EQUIPOS

Se debe tomar en consideración las siguientes directrices para proteger los equipos:

Vigilada Mineducación

La versión vigente y controlada de este documento, solo podrá ser consultada a través del sitio web Institucional [www.usco.edu.co](http://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.

|                                                                                   |                                                                                                     |                |          |                 |                                                                                     |  |  |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------|----------|-----------------|-------------------------------------------------------------------------------------|--|--|
|  | <b>UNIVERSIDAD SURCOLOMBIANA</b><br><b>GESTIÓN DE INFORMACIÓN, TECNOLOGÍAS Y CONTROL DOCUMENTAL</b> |                |          |                 |  |  |  |
|                                                                                   | <b>DIRECTRICES PARA PROTECCION FISICA DE ACTIVOS DE INFORMACION</b>                                 |                |          |                 | <b>Página 6 de 14</b>                                                               |  |  |
| <b>CÓDIGO</b>                                                                     | <b>AP-TIC-DR-08</b>                                                                                 | <b>VERSIÓN</b> | <b>1</b> | <b>VIGENCIA</b> | <b>2026</b>                                                                         |  |  |

- a) colocación de equipos para minimizar el acceso innecesario a las zonas de trabajo y evitar el acceso no autorizado;
- b) colocar cuidadosamente las instalaciones de procesamiento de información que manipulan datos sensibles para reducir el riesgo de que personas no autorizadas vean la información durante su uso;
- c) adoptar controles para minimizar el riesgo de posibles amenazas físicas y ambientales, por ejemplo, robo, incendio, explosivos, humo, agua, polvo, vibraciones, efectos químicos, interferencias en el suministro eléctrico, interferencias de comunicaciones, radiación electromagnética y vandalismo;
- d) no se debe comer, beber y fumar en proximidad a las instalaciones de procesamiento de información;
- e) controlar las condiciones ambientales, como la temperatura y la humedad, para condiciones que puedan afectar negativamente al funcionamiento de las instalaciones de procesamiento de información;
- f) aplicar protección contra rayos a todos los edificios e instalar polos a tierra a todas las líneas de alimentación y comunicaciones entrantes;
- h) protección del equipo que procesa información confidencial para minimizar el riesgo de fuga de información debido a emanaciones electromagnéticas;
- i) separar físicamente las instalaciones de procesamiento de información gestionadas por la Universidad Surcolombiana de las no gestionadas por la Universidad Surcolombiana.

### 6.3. SEGURIDAD DE LOS ACTIVOS FUERA DE LAS INSTALACIONES

Se debe tener en cuenta las siguientes directrices para la protección de los dispositivos que almacenan o procesan información fuera de las instalaciones de la Universidad Surcolombiana:

- a) no dejar el equipo y los medios de almacenamiento sin supervisión en lugares públicos y no protegidos;

Vigilada Mineducación

La versión vigente y controlada de este documento, solo podrá ser consultada a través del sitio web Institucional [www.usco.edu.co](http://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.

|                                                                                   |                                                                                                     |                |          |                 |                                                                                     |  |  |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------|----------|-----------------|-------------------------------------------------------------------------------------|--|--|
|  | <b>UNIVERSIDAD SURCOLOMBIANA</b><br><b>GESTIÓN DE INFORMACIÓN, TECNOLOGÍAS Y CONTROL DOCUMENTAL</b> |                |          |                 |  |  |  |
|                                                                                   | <b>DIRECTRICES PARA PROTECCION FISICA DE ACTIVOS DE INFORMACION</b>                                 |                |          |                 | <b>Página 7 de 14</b>                                                               |  |  |
| <b>CÓDIGO</b>                                                                     | <b>AP-TIC-DR-08</b>                                                                                 | <b>VERSIÓN</b> | <b>1</b> | <b>VIGENCIA</b> | <b>2026</b>                                                                         |  |  |

- b) observar las instrucciones del fabricante para proteger los equipos;
- c) cuando el equipo fuera de las instalaciones se transfiere entre diferentes personas o partes interesadas, manteniendo un registro que defina la cadena de custodia del equipo, incluidos al menos los nombres y organizaciones de los responsables del equipo. La información que no necesita transferirse con el activo debería eliminarse de forma segura antes de la transferencia;
- d) cuando sea necesario y práctico, que requiera autorización para retirar el equipo y los medios de comunicación de las instalaciones de la Universidad Surcolombiana y que se mantenga un registro de dichas retiradas a fin de mantener un registro de auditoría;
- e) protección contra la visualización de información en un dispositivo en transporte público y los riesgos asociados con el fisgoneo por encima del hombro;
- a) implementación del seguimiento de ubicación y capacidad para el borrado remoto de dispositivos.

La instalación permanente de equipos fuera de las instalaciones de la Universidad Surcolombiana puede estar sujeta a un mayor riesgo de daños, robo o espionaje. Estos riesgos pueden variar considerablemente de un lugar a otro y deberían tenerse en cuenta al determinar las medidas más adecuadas. Al situar este equipo fuera de las instalaciones de la Universidad Surcolombiana, deberían tenerse en cuenta las siguientes directrices:

- a) supervisión de la seguridad física;
- b) protección contra las amenazas físicas y ambientales;
- a) controles de acceso físico y de prueba de manipulación;
- b) control de acceso lógico.

|                                                                                   |                                                                                                     |                |          |                 |             |                                                                                     |                |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------|----------|-----------------|-------------|-------------------------------------------------------------------------------------|----------------|
|  | <b>UNIVERSIDAD SURCOLOMBIANA</b><br><b>GESTIÓN DE INFORMACIÓN, TECNOLOGÍAS Y CONTROL DOCUMENTAL</b> |                |          |                 |             |  |                |
|                                                                                   | <b>DIRECTRICES PARA PROTECCION FISICA DE ACTIVOS DE INFORMACION</b>                                 |                |          |                 |             |                                                                                     |                |
| <b>CÓDIGO</b>                                                                     | <b>AP-TIC-DR-08</b>                                                                                 | <b>VERSIÓN</b> | <b>1</b> | <b>VIGENCIA</b> | <b>2026</b> | <b>Página</b>                                                                       | <b>8 de 14</b> |

#### 6.4. MEDIOS DE ALMACENAMIENTO

Se deberían tener en cuenta las siguientes directrices para la gestión de medios de almacenamiento extraíbles:

- a) establecer una directriz específica de un tema sobre la administración de medios de almacenamiento extraíbles y comunicar dicha directriz específica de un tema a cualquier persona que utilice o gestione medios de almacenamiento extraíbles;
- b) cuando resulte necesario y práctico, exigir la autorización para el retiro de los dispositivos de almacenamiento de la Universidad Surcolombiana y mantener un registro con el fin de conservar un registro de auditoría;
- c) almacenar todos los medios de almacenamiento en un entorno seguro según la clasificación de información y protegerlos contra amenazas ambientales (como calor, humedad, campo electrónico o envejecimiento), de conformidad con las especificaciones de los fabricantes;
- d) si la confidencialidad o integridad de la información son consideraciones importantes, utilizar técnicas cifradas para proteger la información en medios de almacenamiento extraíbles;
- e) para mitigar el riesgo de degradación de los medios de almacenamiento mientras aún se necesita información almacenada, transfiera la información a medios de almacenamiento nuevos antes de que sea ilegible;
- f) almacenar varias copias de información valiosa en medios de almacenamiento independientes para reducir aún más el riesgo de daños o pérdidas de información fortuita;
- g) considerar el registro de medios de almacenamiento extraíbles para limitar la posibilidad de pérdida de información;
- h) cuando sea necesario utilizar medios de almacenamiento extraíbles, supervisando la transferencia de información;

|                                                                                   |                                                                                                     |                |          |                 |                                                                                     |  |  |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------|----------|-----------------|-------------------------------------------------------------------------------------|--|--|
|  | <b>UNIVERSIDAD SURCOLOMBIANA</b><br><b>GESTIÓN DE INFORMACIÓN, TECNOLOGÍAS Y CONTROL DOCUMENTAL</b> |                |          |                 |  |  |  |
|                                                                                   | <b>DIRECTRICES PARA PROTECCION FISICA DE ACTIVOS DE INFORMACION</b>                                 |                |          |                 | <b>Página 9 de 14</b>                                                               |  |  |
| <b>CÓDIGO</b>                                                                     | <b>AP-TIC-DR-08</b>                                                                                 | <b>VERSIÓN</b> | <b>1</b> | <b>VIGENCIA</b> | <b>2026</b>                                                                         |  |  |

j) al enviar medios de almacenamiento a través del servicio postal o a través del servicio de mensajería, asegúrese que la información no sea vulnerable al acceso no autorizado, al uso indebido o a la corrupción durante el transporte físico;

#### 6.4.1 Reutilización o eliminación segura

Se deben establecer procedimientos para la reutilización o eliminación segura de los medios de almacenamiento a fin de reducir al mínimo el riesgo de fuga de información confidencial a personas no autorizadas. ver AP-TIC-PR-11 BORRADO DE ACTIVOS DE INFORMACION, AP-GDC-PR-06 ELIMINACIÓN DOCUMENTAL

Se debe tomar en consideración los siguientes factores:

1. si es necesario reutilizar los medios de almacenamiento que contienen información confidencial dentro de la Universidad Surcolombiana, eliminar los datos de forma segura o formatear los medios de almacenamiento antes de volverlos a utilizar;
- b) desechar los medios de almacenamiento que contienen información confidencial de forma segura cuando ya no sea necesario (destruir, triturar o eliminar el contenido de forma segura);
- c) disponer de procedimientos para identificar los elementos que pueden requerir una eliminación segura;
- d) registrar la eliminación de elementos sensibles para mantener un registro de auditoría;
- f) Se debe realizar una evaluación de riesgos en los dispositivos dañados que contengan datos sensibles para determinar si los elementos deberían destruirse físicamente en lugar de enviarse para su reparación o descartarse.

#### 6.5. SERVICIOS PÚBLICOS DE APOYO

La Universidad Surcolombiana debe:

- a) asegurarse de que el equipo que soporta la infraestructura tecnológica está configurado, operado y mantenido de acuerdo con las especificaciones del fabricante correspondiente;

Vigilada Mineducación

La versión vigente y controlada de este documento, solo podrá ser consultada a través del sitio web Institucional [www.usco.edu.co](http://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.

|                                                                                   |                                                                                                     |                |          |                 |                                                                                     |  |  |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------|----------|-----------------|-------------------------------------------------------------------------------------|--|--|
|  | <b>UNIVERSIDAD SURCOLOMBIANA</b><br><b>GESTIÓN DE INFORMACIÓN, TECNOLOGÍAS Y CONTROL DOCUMENTAL</b> |                |          |                 |  |  |  |
|                                                                                   | <b>DIRECTRICES PARA PROTECCION FISICA DE ACTIVOS DE INFORMACION</b>                                 |                |          |                 | <b>Página 10 de 14</b>                                                              |  |  |
| <b>CÓDIGO</b>                                                                     | <b>AP-TIC-DR-08</b>                                                                                 | <b>VERSIÓN</b> | <b>1</b> | <b>VIGENCIA</b> | <b>2026</b>                                                                         |  |  |

- b) garantizar que los servicios públicos sean evaluados periódicamente en cuanto a su capacidad para satisfacer el crecimiento de la institución y las interacciones con otros servicios de respaldo;
- c) garantizar que los equipos de soporte de los servicios públicos se inspeccionen y prueben regularmente para garantizar su correcto funcionamiento;
- d) si es necesario, levantar alarmas para detectar fallas de funcionamiento de los servicios públicos;
- e) si es necesario, asegurarse de que los servicios públicos tienen varias fuentes con enrutamiento físico diverso;
- f) garantizar que los equipos que soportan los servicios públicos estén en una red separada de las instalaciones de procesamiento de la información, si están conectadas a una red;
- g) garantizar que los equipos que soportan los servicios públicos se conecten a Internet solo cuando sea necesario y de forma segura.
- h) Se debe proporcionar iluminación de emergencia y comunicaciones.
- i) Los interruptores y válvulas de emergencia para cortar la alimentación, el agua, el gas u otros servicios públicos deben estar ubicados cerca de las salidas de emergencia o de las salas de equipos.
- j) Los datos de contacto de emergencia deben registrarse y ponerse a disposición del personal en caso de interrupción del servicio.

## 6.6. SEGURIDAD DEL CABLEADO

Se debe tener en cuenta las siguientes directrices para la seguridad del cableado:

- a) líneas de energía y telecomunicaciones en instalaciones de procesamiento de información bajo tierra siempre que sea posible o sometidas a una protección alternativa adecuada, como el protector de cables de suelo y el polo de servicio; si los cables están bajo tierra, deben estar protegidos de cortes accidentales;

Vigilada Mineducación

La versión vigente y controlada de este documento, solo podrá ser consultada a través del sitio web Institucional [www.usco.edu.co](http://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.

|                                                                                   |                                                                                                     |                |          |                 |                                                                                     |  |  |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------|----------|-----------------|-------------------------------------------------------------------------------------|--|--|
|  | <b>UNIVERSIDAD SURCOLOMBIANA</b><br><b>GESTIÓN DE INFORMACIÓN, TECNOLOGÍAS Y CONTROL DOCUMENTAL</b> |                |          |                 |  |  |  |
|                                                                                   | <b>DIRECTRICES PARA PROTECCION FISICA DE ACTIVOS DE INFORMACION</b>                                 |                |          |                 | <b>Página 11 de 14</b>                                                              |  |  |
| <b>CÓDIGO</b>                                                                     | <b>AP-TIC-DR-08</b>                                                                                 | <b>VERSIÓN</b> | <b>1</b> | <b>VIGENCIA</b> | <b>2026</b>                                                                         |  |  |

- b) separar los cables de alimentación eléctrica de los cables de comunicaciones para evitar interferencias;
- c) para sistemas sensibles o críticos otros controles a considerar incluyen:
  - 1) instalación de conductos blindados y salas o cajas bloqueadas y alarmas en los puntos de inspección y terminación;
  - 2) uso de blindaje electromagnético para proteger los cables;
  - 3) barridos técnicos periódicos e inspecciones físicas para detectar dispositivos no autorizados que se conectan a los cables;
  - 4) Acceso controlado a paneles de conexiones y salas de cables;
  - 5) uso de cables de fibra óptica;
- d) etiquetar los cables en cada extremo con suficientes detalles de origen y destino para permitir la identificación física y la inspección del cable.

## 6.7. MANTENIMIENTO DE EQUIPOS

Se debe tener en cuenta las siguientes directrices para el mantenimiento de equipos:

- a) mantener el equipo de acuerdo con la frecuencia de servicio y las especificaciones recomendadas por el proveedor;
- b) ejecución y seguimiento de un programa de mantenimiento por parte de la Universidad Surcolombiana;
- c) solo el personal de soporte técnico del CITCD autorizado puede realizar las reparaciones y el mantenimiento de los equipos;
- d) mantener registros de todas las averías sospechosas o reales, así como de todo mantenimiento preventivo y correctivo;

|                                                                                   |                                                                                                     |                |          |                 |                                                                                     |  |  |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------|----------|-----------------|-------------------------------------------------------------------------------------|--|--|
|  | <b>UNIVERSIDAD SURCOLOMBIANA</b><br><b>GESTIÓN DE INFORMACIÓN, TECNOLOGÍAS Y CONTROL DOCUMENTAL</b> |                |          |                 |  |  |  |
|                                                                                   | <b>DIRECTRICES PARA PROTECCION FISICA DE ACTIVOS DE INFORMACION</b>                                 |                |          |                 | <b>Página 12 de 14</b>                                                              |  |  |
| <b>CÓDIGO</b>                                                                     | <b>AP-TIC-DR-08</b>                                                                                 | <b>VERSIÓN</b> | <b>1</b> | <b>VIGENCIA</b> | <b>2026</b>                                                                         |  |  |

- e) implementar controles adecuados cuando el equipo esté programado para el mantenimiento, tomando en consideración si este mantenimiento lo realiza el personal interno o externo a la Universidad Surcolombiana; someter al personal de mantenimiento a un acuerdo de confidencialidad adecuado;
- f) supervisar al personal de mantenimiento durante el mantenimiento in situ;
- g) autorizar y controlar el acceso para el mantenimiento remoto;
- h) la aplicación de medidas de seguridad para los activos fuera de las instalaciones si el equipo que contiene información se retira de las instalaciones para su mantenimiento;
- i) el cumplimiento de todos los requisitos de mantenimiento impuestos por el seguro;
- j) antes de volver a poner el equipo en funcionamiento después del mantenimiento, se debe inspeccionar para asegurarse de que el equipo no se ha manipulado y funciona correctamente;
- k) aplicar medidas seguras para la eliminación o reutilización del equipo si se determina que el equipo se va a dar de baja.

## 6.8. DISPOSICIÓN O REUTILIZACIÓN SEGURA DE LOS EQUIPOS

Se debe tener en cuenta las siguientes directrices para la disposición o reutilización del equipo: ver AP-TIC-PR-11 BORRADO DE ACTIVOS DE INFORMACION

- a) el equipo se debería verificar para asegurarse de qué medios de almacenamiento están contenidos o no antes de su eliminación o reutilización.
- b) Los medios de almacenamiento que contienen información confidencial o protegida por derechos de autor deberían destruirse físicamente o la información debería destruirse, eliminarse o sobrescribirse al utilizar técnicas para que la información original no pueda recuperarse en lugar de utilizar la función de eliminación convencional.

|                                                                                   |                                                                                                     |                |          |                 |             |                                                                                     |                 |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------|----------|-----------------|-------------|-------------------------------------------------------------------------------------|-----------------|
|  | <b>UNIVERSIDAD SURCOLOMBIANA</b><br><b>GESTIÓN DE INFORMACIÓN, TECNOLOGÍAS Y CONTROL DOCUMENTAL</b> |                |          |                 |             |  |                 |
|                                                                                   | <b>DIRECTRICES PARA PROTECCION FISICA DE ACTIVOS DE INFORMACION</b>                                 |                |          |                 |             |                                                                                     |                 |
| <b>CÓDIGO</b>                                                                     | <b>AP-TIC-DR-08</b>                                                                                 | <b>VERSIÓN</b> | <b>1</b> | <b>VIGENCIA</b> | <b>2026</b> | <b>Página</b>                                                                       | <b>13 de 14</b> |

c) Las etiquetas y las marcas que identifiquen a la Universidad Surcolombiana o indiquen la clasificación, propietario, sistema o red, deberían eliminarse antes de su disposición final, esto incluye la reventa o donación a una organización benéfica.

d) la Universidad Surcolombiana debe considerar la eliminación de los controles de seguridad, como los controles de acceso o los equipos de vigilancia, al final del contrato de arrendamiento o cuando se traslade de las instalaciones. Esto depende de factores como:

1. su contrato de arrendamiento para devolver la instalación a su condición original;
2. minimizar el riesgo de dejar sistemas con información confidencial para el siguiente arrendatario;
3. la capacidad de reutilizar los controles en la siguiente instalación.

## 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-INF-FO-06 ORDEN DE SALIDA DE ELEMENTOS DEVOLUTIVOS Y DE CONSUMO  
ES-GSPI-MR-04 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN DOCUMENTAL  
ES-GSPI-MR-05 MATRIZ DE INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN

|                                                                                   |                                                                                                     |                |          |                 |             |                                                                                     |                 |
|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------|----------|-----------------|-------------|-------------------------------------------------------------------------------------|-----------------|
|  | <b>UNIVERSIDAD SURCOLOMBIANA</b><br><b>GESTIÓN DE INFORMACIÓN, TECNOLOGÍAS Y CONTROL DOCUMENTAL</b> |                |          |                 |             |  |                 |
|                                                                                   | <b>DIRECTRICES PARA PROTECCION FISICA DE ACTIVOS DE INFORMACION</b>                                 |                |          |                 |             |                                                                                     |                 |
| <b>CÓDIGO</b>                                                                     | <b>AP-TIC-DR-08</b>                                                                                 | <b>VERSIÓN</b> | <b>1</b> | <b>VIGENCIA</b> | <b>2026</b> | <b>Página</b>                                                                       | <b>14 de 14</b> |

AP-GDC-PR-06 ELIMINACIÓN DOCUMENTAL

AP-GDC-FO-16 ACTA DE ELIMINACIÓN DOCUMENTAL

AP-TIC-PR-11 BORRADO DE ACTIVOS DE INFORMACION

AP TIC PR 05 DISEÑO E IMPLEMENTACIÓN DE NUEVAS REDES DE DATOS

AP TIC PR 04 ADMINISTRACIÓN REDES DE DATOS

AP TIC PR 06 SOPORTE TÉCNICO DE EQUIPOS INFORMATICOS Y PUNTOS DE RED

| CONTROL DE CAMBIO |                                        |                       |
|-------------------|----------------------------------------|-----------------------|
| VERSIÓN           | DOCUMENTO Y FECHA DE APROBACIÓN        | DESCRIPCION DE CAMBIO |
| 01                | EV-CAL-FO-17 14 de septiembre del 2026 | Creación documento    |

| ELABORÓ                                                                                                                                                                                                                                   | REVISÓ                                            | APROBÓ                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|-------------------------------------------|
| MARTHA LILIANA<br>HERMOSA TRUJILLO<br>Gestión Seguridad y<br>Privacidad de la Información<br><b>Elaboró</b><br><br>DIEGO ANDRES<br>CARVAJAL RUIZ<br>Director Centro de<br>Tecnología Información y<br>Control Documental<br><b>Aprobó</b> | ALVARO TORRENTE LÓPEZ<br>Profesional de apoyo SGC | MAYRA ALEJANDRA BERMEO<br>Coordinador 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](http://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.