



Política de Uso Aceptable de la tecnología de la información y la comunicación.

COLOMBIA

Julio de 2026

1. Objetivo

- 1.1 Esta política establece los lineamientos para el uso aceptable o adecuado de las tecnologías de la información y la comunicación en el entorno escolar, incluyendo dispositivos como computadores, tabletas, teléfonos móviles (celulares), y relojes inteligentes, tanto por parte del personal docente y administrativo como de las y los estudiantes. Su propósito principal es definir los estándares de conducta que deben observar los empleados y estudiantes al utilizar los sistemas informáticos del colegio, reducir el riesgo de interacciones inapropiadas entre empleados y estudiantes mediante el uso de tecnología, proteger al personal y a las instituciones educativas frente a posibles demandas legales, y minimizar los riesgos de seguridad que puedan afectar la integridad de los sistemas informáticos del colegio. Asimismo, busca garantizar la seguridad de las y los estudiantes en el entorno digital y prevenir su exposición a contenidos inapropiados o interacciones que representen riesgos para su bienestar físico, emocional o psicológico.

2. Aplicación

- 2.1 Esta política regula el uso de los equipos informáticos y demás tecnologías de los colegios pertenecientes al grupo Cognita, y es aplicable a todos los empleados y estudiantes, así como a otros usuarios autorizados como proveedores, voluntarios y cualquier persona que tenga acceso a dichos sistemas. Su cumplimiento es esencial para garantizar un entorno digital seguro, proteger la integridad de los sistemas informáticos y salvaguardar el bienestar de las y los estudiantes, evitando la exposición a contenidos inapropiados o interacciones que puedan representar riesgos. La aplicación de esta política será diferencial en el caso de estudiantes con necesidades educativas especiales, quienes podrán requerir apoyos tecnológicos específicos para garantizar su participación plena y equitativa en el entorno escolar, conforme a lo establecido en la Política de Acceso e Inclusión Escolar (SEND).
- 2.2 Esta política no forma parte del contrato laboral de ningún empleado, sin embargo, es de obligatorio cumplimiento para todos los trabajadores de Redcol. Cognita – Redcol se reserva el derecho de modificarla en cualquier momento. El incumplimiento de los lineamientos aquí establecidos podrá considerarse una violación de las obligaciones contractuales asumidas por la persona involucrada, con las consecuencias legales y laborales que correspondan en cada caso. En el caso de las y los estudiantes, el incumplimiento de esta política podrá implicar medidas disciplinarias conforme al Manual de Convivencia del Colegio, especialmente en situaciones que comprometan la seguridad digital propia o la de otros miembros de la comunidad educativa, o que impliquen exposición a contenidos o interacciones inapropiadas. Para estudiantes con necesidades educativas especiales, toda medida disciplinaria deberá considerar las adaptaciones, recursos y apoyos definidos en la Política SEND, con enfoque en el respeto, la protección y la equidad.

3. Responsabilidades de Cognita - Redcol y el Colegio

- 3.1 Cognita – Redcol, como órgano de gobernanza del colegio, tiene la responsabilidad de garantizar que sus empleados actúen conforme a la legalidad y hagan un uso apropiado de la tecnología únicamente para fines autorizados. Igualmente, debe promover entre las y los estudiantes el uso responsable de los recursos tecnológicos, asegurándose de que comprendan los límites de su uso y las implicaciones de un uso inapropiado.
- 3.2 Cognita – Redcol es responsable de establecer las políticas relevantes en esta materia, y el rector/a del colegio debe velar por que estas sean implementadas adecuadamente y que tanto el personal como las y los estudiantes estén informados de su contenido y alcances.
- 3.3 El rector/a tiene la responsabilidad de mantener un inventario actualizado de los equipos tecnológicos (hardware y software), incluyendo aquellos asignados al personal para uso personal, como portátiles y teléfonos, y aquellos que sean utilizados por estudiantes dentro del entorno escolar.

- 3.4 Si el rector/a considera que algún equipo ha sido maltratado o utilizado para fines distintos a los autorizados, debe comunicarlo sin demora a la Gerencia Nacional de Tecnología e Informática, a la Coordinación Nacional de Salvaguarda y Bienestar y a la Vicepresidencia de Educación. Junto con el rector/a, estas personas establecerán una estrategia de investigación conforme a los procedimientos internos. En caso de que se vean involucradas/os estudiantes, el proceso deberá garantizar su bienestar, protección y respeto de sus derechos educativos.
- 3.5 Los rectores/as deben asegurar que ningún miembro del personal, ni estudiante, lleve a cabo investigaciones de este tipo por cuenta propia, a menos que cuenten con autorización expresa para hacerlo, conforme a los protocolos institucionales. Esta autorización podrá otorgarse únicamente a personal capacitado y debidamente facultado para ello; bajo ninguna circunstancia se permitirá que estudiantes realicen investigaciones de carácter institucional o relacionadas con el uso de los equipos tecnológicos del colegio.
- 3.6 Con el fin de fortalecer las acciones de protección y promover entornos tecnológicos seguros para las y los estudiantes, los/las rectores/as podrán coordinar con la Gerencia Nacional de Tecnología e Informática y la Coordinación de Tecnologías la generación de reportes de filtrado web, cuando se considere necesario. Estos reportes podrán ser solicitados de manera puntual por la rectoría o por la/el Líder Delegada/o de Salvaguarda de cada colegio, con el objetivo de facilitar la identificación temprana de posibles alertas por accesos a contenidos inapropiados y la evaluación de riesgos asociados al bienestar estudiantil. Esta práctica contribuirá, cuando sea pertinente, a la detección oportuna de posibles casos de salvaguarda, en coherencia con los protocolos institucionales. Asimismo, los hallazgos derivados de estos reportes podrán servir como base para la elaboración de estrategias preventivas, procesos de sensibilización y acciones pedagógicas dirigidas a atender y prevenir riesgos relacionados con el uso inapropiado de los recursos tecnológicos dentro de la comunidad educativa.
- 3.7 Es responsabilidad del/de la rector/a, en coordinación con las áreas académicas correspondientes, garantizar que tanto estudiantes como personal educativo y administrativo reciban formación continua sobre el uso aceptable de la tecnología institucional, entendido como el uso responsable, seguro y con fines educativos alineados con los valores de la comunidad escolar. Esta formación debe incluir, con énfasis especial, contenidos sobre seguridad digital y en línea, abordando riesgos como el acceso a contenidos inapropiados, el ciberacoso, la protección de datos personales y la interacción segura en entornos virtuales. Dicha formación contribuye directamente a la prevención de usos indebidos y a la creación de una cultura de responsabilidad tecnológica. Estos contenidos deberán estar articulados con los proyectos curriculares transversales de cada colegio, fomentando una comprensión integrada de la ciudadanía digital y sus implicaciones para el bienestar de toda la comunidad educativa.

4. Responsabilidades del usuario

- 4.1 Los colegios del grupo Cognita – Redcol reconocen el derecho de todas/os las/los estudiantes y empleados a un acceso seguro, equitativo y ético a las tecnologías de la información, incluyendo la protección de su identidad digital y privacidad en línea, bajo los límites determinados en el Manual de Convivencia Institucional de cada Colegio. Esta política promueve el uso responsable de dichos recursos y la defensa activa de los derechos digitales en el entorno escolar, con especial énfasis en la seguridad y bienestar de las y los estudiantes. Dado lo cual se dictan las siguientes disposiciones en materia de responsabilidad:
- 4.2 El empleado que incumpla esta política podrá estar sujeto a un procedimiento disciplinario. En algunas circunstancias, dicho incumplimiento podría ser considerado una falta muy grave, dando lugar a la terminación del contrato laboral. En el caso de estudiantes, las infracciones serán evaluadas conforme al Manual de Convivencia del colegio y podrían implicar medidas disciplinarias que protejan la seguridad digital de toda la comunidad educativa. Todo usuario debe informar al/a la rector/a sobre cualquier sospecha de incumplimiento de esta política.
- 4.3 Los usuarios y sus superiores directos son responsables de garantizar que se ofrezca el apoyo y la formación adecuados para implementar esta política de forma eficaz y consciente. En el caso de estudiantes, este apoyo

será proporcionado mediante espacios pedagógicos, acompañamiento y orientación permanente acorde a lo definido dentro de cada colegio.

- 4.4 Al acceder a los sistemas informáticos del colegio, los usuarios (incluyendo estudiantes y empleados) aceptan cumplir esta Política de Uso Aceptable y las demás políticas institucionales relacionadas con el uso de tecnología.
- 4.5 Se espera que todas y todos las/los usuarias/os actúen de forma responsable, ética y legal. Es obligatorio el cumplimiento de las leyes vigentes en materia de protección de datos personales, propiedad intelectual y derechos de autor, incluyendo pero sin limitarse a las siguientes: Constitución Política de Colombia artículo 15 (autodeterminación informática y protección al buen nombre), la Ley 1581 de 2012 y sus decretos reglamentarios, la Decisión 351 de la Comunidad Andina de Naciones en materia de propiedad intelectual y derechos de autor, además de las políticas internas de Cognita - Redcol sobre protección de datos personales. La protección de la privacidad y confidencialidad de todos los miembros de la comunidad educativa, en especial de las y los estudiantes, debe ser prioritaria. Se debe evitar cualquier incumplimiento relacionado con derechos de autor, marcas registradas o diseños, y abstenerse de publicar contenido difamatorio o inapropiado.
- 4.6 En coherencia con lo establecido en la Política de Seguridad y controles tecnológicos para los activos de información, las y los empleados deberán firmar el recibo correspondiente por los equipos tecnológicos asignados, como portátiles o teléfonos, y utilizar dichos equipos exclusivamente para labores profesionales autorizadas. De igual manera, las/los estudiantes que hagan uso de equipos proporcionados por el colegio deberán seguir los lineamientos de uso definidos por la institución, garantizando el adecuado manejo y protección de dichos activos.
- 4.7 Las y los empleados deberán seguir los procedimientos autorizados al trasladar dispositivos móviles de propiedad institucional fuera de las instalaciones del colegio. En el caso de estudiantes, el uso de dispositivos escolares fuera del recinto requerirá aprobación previa y estará sujeto a control institucional.
- 4.8 Ningún/a usuario/a está autorizado/a a utilizar los recursos informáticos en violación de acuerdos de licencia, leyes de derechos de autor, contratos o normas legales nacionales. Esto aplica igualmente al uso personal o académico por parte de las y los estudiantes.
- 4.9 En cumplimiento del Procedimiento de administración de accesos, el personal del colegio debe proteger los dispositivos portátiles mediante el uso de contraseñas seguras que cumplan con las siguientes características: longitud mínima de 12 caracteres, combinación alfanumérica, inclusión de al menos un carácter especial y cambio obligatorio cada 90 días. Aunque las/los estudiantes no estén obligadas/os al uso de dispositivos personales, se les promoverá el uso de contraseñas seguras en las plataformas institucionales, fomentando buenas prácticas de seguridad digital dentro de la comunidad educativa.
- 4.10 En concordancia con el proceso de administración de accesos, se recomienda activar la autenticación de dos factores (2FA) para proteger las cuentas institucionales. Ante cualquier intento de suplantación, actividad sospechosa o posible phishing, los usuarios deberán reportarlo de inmediato al equipo técnico del colegio. Aunque no se realizan simulacros de ciberseguridad, se cuenta con cursos obligatorios de formación en ciberseguridad para todo el personal administrativo, los cuales se imparten a través de una plataforma institucional. Estas acciones buscan fortalecer la cultura de prevención digital dentro de la comunidad educativa.
- 4.11 En concordancia con el proceso de administración de accesos, se requiere que todos los usuarios del sistema informático del colegio (incluidos empleados y estudiantes) protejan sus credenciales de acceso, evitando compartir contraseñas, acceder a cuentas ajenas o falsear su identidad digital. En ningún caso se permitirá que un usuario revele su contraseña a otra persona, ni siquiera temporalmente, como medida de seguridad y preservación de la integridad de los datos institucionales.
- 4.12 Ningún usuario, bajo ninguna circunstancia, podrá acceder (leer, modificar, eliminar, copiar o mover)

documentos personales de otro miembro de la comunidad educativa sin autorización explícita, salvo que lo estipule esta política o la legislación vigente. Esta restricción incluye el acceso no autorizado al correo electrónico, archivos personales, plataformas institucionales y demás medios de comunicación interna.

- 4.13 En coherencia con lo establecido en la Política de Seguridad y controles tecnológicos para los activos de información los usuarios no deben instalar ni descargar software sin la autorización previa del/de la rector/a. Para garantizar la seguridad digital del entorno escolar, se realizarán auditorías periódicas de los equipos informáticos utilizados por empleados y estudiantes.
- 4.14 No se contempla el uso de dispositivos personales para fines laborales o académicos, dado que no es posible ejercer control sobre equipos externos a la compañía. El deber ser es que cada colaborador cuente con recursos tecnológicos provistos por RedCol, los cuales deben ser utilizados conforme a los lineamientos institucionales de seguridad. En el caso de los/las estudiantes, no deberán conectar equipos personales a las plataformas o redes institucionales sin la autorización expresa del colegio. En todo caso, cuando un dispositivo personal sea utilizado en las instalaciones de RedCol o para fines laborales o académicos con la compañía; el usuario o propietario está obligado al cumplimiento de la presente política.
- 4.15 Queda prohibido trasladar datos personales (especialmente los relacionados con estudiantes) fuera de las instalaciones del colegio o la transmisión a terceros sin autorización previa del/de la rector/a. Si excepcionalmente se autoriza dicho traslado, los datos electrónicos deberán ser protegidos mediante contraseñas seguras y sistemas de encriptación. Esto incluye información almacenada en portátiles, dispositivos USB y plataformas de sincronización como Dropbox, Google Drive o One Drive. El uso de tecnología fuera del recinto escolar exige precauciones adicionales para evitar comprometer la seguridad del sistema o la privacidad de la comunidad educativa. Estos datos están sujetos a leyes de protección de datos personales, y deben tratarse con máxima confidencialidad conforme a la política de Protección de Datos de Cognita – Redcol.
- 4.16 En cumplimiento de la Política de Seguridad y controles tecnológicos para los activos de información todo dispositivo conectado a la red institucional debe tener instalado y activo un software antivirus autorizado. Ningún usuario puede desactivar dicha protección. Tanto empleados como estudiantes deben contribuir a la prevención de la propagación de virus informáticos, absteniéndose de crear, instalar, ejecutar o compartir cualquier tipo de código malicioso (como virus, troyanos o software destructivo) de manera deliberada.
- 4.17 Queda estrictamente prohibido interferir conscientemente con los mecanismos de seguridad o la integridad de los sistemas informáticos del colegio. Ningún usuario puede utilizar los recursos tecnológicos para acceder a sistemas de forma no autorizada ni afectar el uso legítimo que otros miembros hacen de los equipos y redes, internas o externas. Todas las actividades de acceso a la red serán objeto de monitoreo en cumplimiento de los protocolos institucionales y las normas aplicables.
- 4.18 De conformidad con la legislación vigente en materia de protección de datos, Cognita – Redcol o el colegio podrá grabar, monitorear o inspeccionar sin aviso previo cualquier información que sea transmitida a través de o contenida en sus equipos tecnológicos, incluidas comunicaciones por correo electrónico, sesiones de inicio de sesión y actividades en línea. Esta facultad será ejercida únicamente en circunstancias justificadas, tales como:
- Cuando exista duda razonable de incumplimiento de esta política;
 - Se detecte actividad inusual o excesiva en una cuenta;
 - Se requiera proteger la integridad, seguridad o funcionamiento de los sistemas informáticos o evitar responsabilidad legal institucional;
 - Se investigue un uso indebido de los equipos;
 - Se necesite recuperar información perdida por fallos técnicos; se busque prevenir o detectar un delito;
 - Se evalúe la relevancia de comunicaciones ante ausencias o situaciones laborales particulares;
 - Cuando así lo permita o exija la ley.

Esta medida también aplica a las cuentas y accesos utilizados por estudiantes bajo los mismos principios de salvaguarda y protección institucional.

- 4.19 El Equipo de Apoyo Técnico Central, con la aprobación del/de la rector/a, podrá inspeccionar correos electrónicos y datos de usuarios por los motivos previamente establecidos. Otras comunicaciones basadas en internet serán monitorizadas mediante software automatizado. Estas medidas serán aplicadas con especial cuidado cuando involucren a estudiantes, garantizando en todo momento el respeto a su integridad personal y derechos educativos.
- 4.20 Un sistema de videovigilancia (CCTV) monitorea las áreas exteriores del colegio durante las 24 horas del día como parte de las estrategias institucionales de seguridad y prevención del delito. Las imágenes registradas se almacenan conforme a la normativa de protección de datos y con fines estrictamente institucionales.
- 4.21 En caso de que se autorice el uso de dispositivos personales para fines laborales o académicos, estos deberán contar con medidas de seguridad adecuadas, como software antivirus actualizado y controles de acceso. El equipo técnico podrá implementar soluciones de gestión de dispositivos móviles (MDM) en equipos particulares que se utilicen para acceder a plataformas institucionales. Esta medida no aplica para estudiantes, salvo autorización específica del colegio para actividades pedagógicas controladas.
- 4.22 Ningún usuario podrá crear páginas web o contenidos digitales en los equipos del colegio sin la autorización escrita del/de la rector/a. Esto incluye tanto al personal como a estudiantes que hagan uso de plataformas institucionales.
- 4.23 Está estrictamente prohibido utilizar los recursos informáticos para transmitir contenido abusivo, amenazante, acosador, mensajes en cadena, correos electrónicos masivos no autorizados (spam), o cualquier tipo de comunicación prohibida por la ley o que pueda afectar negativamente la imagen del colegio o del grupo Cognita – Redcol. Ningún usuario, incluyendo estudiantes, podrá participar en foros, grupos o listas de correo en nombre del colegio sin cumplir las políticas correspondientes.
- 4.24 Todos los usuarios deberán seguir las recomendaciones de comunicación segura y responsable contenidas en la Política de Seguridad Digital. Esto incluye el uso adecuado del lenguaje, la cortesía digital y el respeto a los demás en ambientes virtuales escolares.
- 4.25 En coherencia con lo establecido en la Política de Seguridad y controles tecnológicos para los activos de información, en ningún caso está permitido que los usuarios (incluyendo estudiantes) descarguen, generen o accedan a contenido considerado inadecuado, tales como:
- Material pornográfico en cualquier formato;
 - Imágenes o videos que representen violencia, heridas o muerte;
 - Contenido que genere humillación o vergüenza;
 - Correos no deseados o spam;
 - Material que promueva la discriminación o intolerancia por razones de raza, género, discapacidad, orientación sexual, religión, edad u otras condiciones protegidas por ley.

El acceso a este tipo de contenido será considerado una infracción grave y estará sujeto a medidas disciplinarias conforme a los reglamentos institucionales:

- 4.26 Queda prohibido el uso de lenguaje ofensivo, sexista o discriminatorio por motivos de género, identidad de género, orientación sexual, raza, discapacidad, religión u cualquier otra condición personal. Todos los miembros de la comunidad educativa (empleados y estudiantes) deben comunicarse de manera respetuosa e inclusiva, conforme a los valores institucionales de diversidad, equidad y convivencia. Asimismo, se prohíbe la creación, descarga, distribución o acceso a material vinculado con actividades criminales, música, videos o contenido que infrinja los derechos de autor, así como cualquier material que genere riesgos de seguridad

o fomenta el uso inapropiado de los recursos informáticos.

- 4.27 Es posible que un usuario (empleado o estudiante) acceda por error o sea redirigido a sitios web inaceptables. Ante la dificultad que puede representar salir de estas páginas, se recomienda que, si se ha accedido o recibido material inapropiado por correo electrónico u otros medios, se informe inmediatamente al/a la rector/a y/o al/a la Líder Delegado/a de Salvaguarda (DSL). Esta acción permitirá activar los mecanismos de seguimiento y evitar complicaciones posteriores.
- 4.28 El acceso remoto a los sistemas institucionales del colegio deberá ser previamente autorizado por el/la rector/a y configurado exclusivamente por el equipo de informática. Ejemplos de acceso remoto incluyen: correo electrónico a través de webmail o plataformas como Blackberry o Windows Mobile, reenvío de correos a cuentas personales, conexiones mediante VPN, LogMeln, portales web y herramientas de sincronización como Dropbox, Google Drive o One Drive. Quienes reciban autorización (únicamente podrán serlo empleados) deberán cumplir estrictamente con las condiciones de uso establecidas. Este tipo de acceso no será permitido para estudiantes bajo ninguna circunstancia.
- 4.29 Ningún usuario podrá conectar equipos personales a la red del colegio sin autorización expresa del/de la rector/a. En el caso de estudiantes, esta autorización no será otorgada salvo en contextos controlados de enseñanza y con fines pedagógicos previamente validados por el colegio.
- 4.30 Todos los equipos portátiles deben ser guardados de manera segura cuando no estén en uso. Los empleados autorizados a llevarse estos dispositivos fuera del colegio, ya sea a sus hogares o en modalidad roaming, deberán adoptar las medidas necesarias para garantizar su protección, evitando su pérdida, robo o uso indebido. Las/Los estudiantes no podrán trasladar equipos institucionales sin acompañamiento y supervisión del personal autorizado.
- 4.31 Por razones de seguridad, los usuarios deben cerrar sesión o bloquear sus dispositivos si se ausentan de su puesto por un tiempo prolongado. Al finalizar la jornada escolar o laboral, es obligatorio apagar los equipos correctamente para preservar la seguridad digital.
- 4.32 Los empleados no podrán copiar ni instalar software propiedad del colegio en sus dispositivos personales sin la debida autorización del/de la rector/a. Esta práctica está estrictamente prohibida para estudiantes.
- 4.33 El personal docente podrá hacer uso de equipos de grabación digital en el marco de sus actividades pedagógicas. Como parte del currículo, se deberá educar a las y los estudiantes sobre el uso seguro, ético y apropiado de estos dispositivos. Cada vez que se realice una grabación deberá explicarse claramente su propósito y uso previsto, garantizando el consentimiento, privacidad y protección de quienes participen.
- 4.34 Los empleados no deben utilizar imágenes ni grabaciones obtenidas en el entorno escolar para fines distintos de aquellos expresamente autorizados por el colegio. Está prohibido distribuir dicho contenido en espacios públicos, plataformas no institucionales o para beneficio personal. En el caso de estudiantes, cualquier participación en actividades que impliquen grabaciones deberá estar debidamente acompañada por el personal docente y regida por los protocolos de protección de datos y salvaguarda del colegio.

5. Comunicación por teléfono móvil y mensajería instantánea

- 5.1 Por motivos de protección de datos y salvaguarda, los empleados no deben compartir su número personal (de casa o móvil) con estudiantes. El uso de teléfonos móviles personales está prohibido en presencia de niñas, niños y adolescentes durante el ejercicio de funciones laborales. El colegio deberá proveer dispositivos institucionales para actividades o visitas educativas que requieran comunicación.
- 5.2 Está prohibido tomar fotografías o realizar grabaciones mediante dispositivos móviles personales, incluidos relojes inteligentes. Toda captura de imagen o video deberá hacerse exclusivamente con dispositivos propiedad del colegio, destinados a fines institucionales previamente autorizados por el/la rector/a. En caso

de realizar dicha acción, especialmente en casos sin autorización, deberá hacerse siempre un autorreporte al Equipo de Salvaguarda según lo definido en la Política de Salvaguarda y Protección Infantil.

- 5.3 El personal no podrá utilizar los números de teléfono móvil de estudiantes para hacer o recibir llamadas, ni enviar o recibir mensajes, salvo en el marco de una actividad oficialmente autorizada por el colegio y bajo condiciones controladas.
- 5.4 La comunicación electrónica entre empleados y estudiantes deberá realizarse únicamente a través de cuentas de correo institucionales provistas por el colegio, y limitada a asuntos académicos pertinentes, como trabajos escolares o deberes.
- 5.5 Los empleados no podrán enviar mensajes ni comunicarse con estudiantes mediante canales no institucionales, incluyendo aplicaciones de mensajería instantánea, redes sociales u otras plataformas personales. Cualquier excepción deberá estar respaldada por autorización oficial del colegio, en el marco de una actividad específica y debidamente registrada. En caso de realizar dicha acción deberá hacerse siempre un autorreporte al Equipo de Salvaguarda según lo definido en la Política de Salvaguarda y Protección Infantil.
- 5.6 Durante el horario laboral, los empleados deben abstenerse de responder llamadas personales o enviar mensajes personales, especialmente en espacios compartidos con estudiantes. Esta medida protege la concentración en las funciones profesionales y evita distracciones que puedan comprometer la supervisión adecuada.
- 5.7 En todas las áreas del colegio, y especialmente en enfermería, está estrictamente prohibido tomar, enviar o compartir fotografías o videos relacionados con posibles lesiones o condiciones físicas de estudiantes, ya sea mediante dispositivos móviles personales, institucionales o directamente desde el dispositivo del estudiante. Esta disposición tiene como objetivo proteger la privacidad, dignidad y bienestar de niñas, niños y adolescentes, conforme a los estándares institucionales de salvaguarda. Toda situación que requiera registro o documentación deberá comunicarse verbalmente o por escrito a las familias, utilizando exclusivamente los canales autorizados. Para ello se deberá emplear el formato de Mapa del Cuerpo incluido en el DSL Toolkit, según lo establecido en la Política de Salvaguarda y Protección Infantil y en las disposiciones del Manual del DSL Toolkit.
- 5.8 En caso de presentarse un incidente de salvaguarda que pudiera comprometer el bienestar, la integridad o la seguridad de una niña, niño o adolescente, ningún miembro del personal (de cualquier área del colegio) deberá documentar la situación mediante fotografías, videos ni grabaciones de audio. Toda situación de posible salvaguarda debe ser reportada inmediatamente al/a la Líder Delegado/a de Salvaguarda, su suplente, o rector/a, conforme a los protocolos definidos en la Política de Salvaguarda y Protección Infantil. La documentación de estos casos se realizará únicamente a través del formato de Registro de Inquietud o Incidente referido a un Estudiante (RIIE). Esta medida busca garantizar una respuesta ética, segura y respetuosa frente a situaciones sensibles, evitando vulneraciones adicionales y fortaleciendo la cultura de protección dentro del colegio. Para comunicar estos incidentes a las familias se deberá hacer siempre solamente desde dispositivos y sistemas institucionales.
- 5.9 En cumplimiento del principio de desconexión digital y del derecho de niñas, niños y adolescentes a disfrutar de su tiempo personal, familiar y de descanso sin obligaciones escolares fuera del horario establecido, ningún miembro del personal del colegio podrá exigir, promover o facilitar comunicaciones académicas o institucionales fuera del horario escolar definido. Esto incluye el envío de tareas, mensajes, correos electrónicos o actividades a través de plataformas virtuales, aplicaciones de mensajería o llamadas. Salvo en circunstancias excepcionales justificadas por actividades autorizadas previamente por el colegio y comunicadas con antelación a las familias, se deberá respetar el tiempo de desconexión de las y los estudiantes, garantizando su bienestar emocional, salud mental y equilibrio entre el ámbito educativo y personal.
- 5.10 En coherencia con la Ley 2170 de 2021, los pronunciamientos de la Corte Constitucional y los principios de

protección y bienestar infantil establecidos por el Ministerio de Educación Nacional, el colegio regulará en su Manual de Convivencia el uso de teléfonos celulares y dispositivos electrónicos por parte de las y los estudiantes durante la jornada escolar. Si bien no está permitida una prohibición absoluta, se establecerán restricciones claras en el Manual de Convivencia que limiten su uso únicamente a actividades pedagógicas autorizadas, bajo supervisión directa del personal docente y con el aval previo del Comité Escolar de Convivencia y del Consejo Directivo. Fuera de estos casos excepcionales, las y los estudiantes no deben portar ni utilizar sus dispositivos móviles, con el fin de promover un entorno libre de distracciones, salvaguardar su integridad emocional y social, y prevenir riesgos relacionados con el uso inapropiado de la tecnología. El personal del colegio deberá velar por el cumplimiento de estas disposiciones como parte de sus responsabilidades institucionales de cuidado y protección.

6. Redes Sociales e Inteligencia Artificial (IA)

- 6.1 El uso de herramientas de inteligencia artificial generativa (IA) en contextos educativos debe estar estrictamente regulado. Está prohibido utilizar IA para interactuar directamente con estudiantes o sus registros fotográficos o de video, compartir información personal, académica o confidencial en plataformas públicas, no autorizadas o que no cumplan con los estándares de protección de datos establecidos por Cognita – Redcol. Toda implementación de IA en el entorno escolar deberá ser previamente evaluada y autorizada por el equipo de tecnología y el/la rector/a del colegio, asegurando el cumplimiento de las políticas institucionales de privacidad de datos y salvaguarda.
- 6.2 Ningún empleado podrá comunicarse, seguir, interactuar o establecer conexiones mediante redes sociales con estudiantes o egresados menores de 18 años sin contar con autorización escrita del/de la rector/a. Esta medida busca proteger la integridad y seguridad digital de niñas, niños y adolescentes, y reforzar los límites profesionales adecuados en entornos virtuales.
- 6.3 Los empleados no deberán crear ni administrar grupos en redes sociales que estén directamente vinculados al colegio o Cognita - Redcol sin contar con la aprobación explícita y por escrito del/de la rector/a. Cualquier presencia institucional en redes sociales deberá estar alineada con los objetivos educativos, comunicativos y estratégicos definidos por la rectoría del colegio y el área de comunicaciones.
- 6.4 El personal del colegio deberá abstenerse de utilizar redes sociales para discutir asuntos laborales, compartir contenido sensible o utilizar su rol en la institución para beneficio personal. Toda expresión pública en redes sociales deberá ser respetuosa, ética y en consonancia con los valores institucionales. La identidad laboral asociada al colegio o Cognita - Redcol no podrá usarse para promocionar intereses ajenos a la labor educativa.
- 6.5 Cualquier publicación de material videográfico que incluya menores de edad, deberá estar precedido de la revisión de autorización de uso de imagen y voz suscrito por los representantes legales del menor de edad.

Titularidad y consultas	
Patrocinador (sponsor) del documento (rol)	Director de Educación
Autor del documento (nombre)	Simon Camby
Asesoría especializada	Equipo Legal Cognita Chile
Consulta	Jayne Pinchbeck, Asesora Legal Cognita Global

Adaptado para aplicación en Colombia	
Aprobado por	Paula Nikotian
Adaptado por	Paola Barrios, Carlos Alberto Corredor, y Juan Pablo Rueda Bonilla
Aprobado en Cognita – Redcol por	José Quijano
Audiencia	
Audiencia	Todo el personal, estudiantes y los voluntarios de los colegios de Cognita - Redcol
Aplicación y publicación de documentos	
Colombia	Sí
Control de versión	
Fecha de implementación	Septiembre 2023 (Fecha original de implementación de la política en su primera versión)
Fecha de revisión	Julio 2026 (Segunda actualización)
Documentación relacionada	Keeping Children Safe in Education Código de Conducta DSL Toolkit Reglamento de cada colegio Legislación colombiana Política de Salvaguarda y Protección Infantil Política de Acceso e Inclusión Escolar (SEND) Política de Cuidados Íntimos