

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 1 de 32

TABLA DE CONTENIDO

1. OBJETIVO	3
2. ALCANCE	3
3. DEFINICIONES.....	3
4. NORMATIVIDAD ASOCIADA.....	4
5. DESARROLLO	5
5.1. Políticas organizacionales	5
<i>Política de estructura organizacional de seguridad de la información</i>	5
<i>Política de gestión de activos de Información</i>	5
<i>Política de uso de los activos</i>	6
<i>Política de uso de los recursos tecnológicos</i>	6
<i>Política de uso del correo electrónico</i>	7
<i>Política de uso de internet</i>	8
<i>Política para uso de dispositivos móviles</i>	9
<i>Política de uso de mensajería instantánea y redes sociales</i>	9
<i>Política para la transferencia de información</i>	10
<i>Política de control y gestión de acceso</i>	11
<i>Política de establecimiento, uso y protección de claves de acceso</i>	14
<i>Manejo de contraseñas para administradores de TI</i>	14
<i>Política en la relación con proveedores</i>	15
<i>Política para el uso de servicios en la nube</i>	15
<i>Política de gestión de los incidentes de la seguridad de la información</i>	16
<i>Política de seguridad de la información durante la interrupción</i>	16
<i>Política de cumplimiento de requisitos legales, estatutarios, reglamentarios y contractuales</i>	17
<i>Política de tratamiento de datos personales</i>	18
<i>Política de revisión independiente de la seguridad de la información</i>	18
<i>Política de cumplimiento</i>	19

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 2 de 32

5.2.	Política de seguridad del recurso humano.....	19
	<i>Política de trabajo a distancia.....</i>	20
	<i>Política de reporte de eventos de seguridad de la información.....</i>	20
5.3.	Política de seguridad física.....	21
	<i>Política de perímetros y entrada física.....</i>	21
	<i>Política de escritorio despejado y pantalla limpia.....</i>	21
	<i>Política de protección contra amenazas físicas y ambientales.....</i>	22
	<i>Política de medios de almacenamiento.....</i>	23
	<i>Política de seguridad del cableado.....</i>	23
	<i>Política de mantenimiento de equipos.....</i>	23
	<i>Política de eliminación segura o reutilización de equipos.....</i>	24
5.4.	Política de las operaciones TIC.....	24
	<i>Política de dispositivos tecnológicos y redundancias.....</i>	24
	<i>Política de accesos con privilegios.....</i>	25
	<i>Política de acceso a sistemas y aplicaciones.....</i>	26
	<i>Política de gestión de vulnerabilidades.....</i>	26
	<i>Política de controles criptográficos.....</i>	27
	<i>Política de respaldo y restauración de información.....</i>	27
	<i>Política de seguridad de las comunicaciones.....</i>	28
	<i>Política de registro y seguimiento de eventos de sistemas de información y comunicaciones.....</i>	28
	<i>Política de adquisición, desarrollo y mantenimiento de sistemas de información.....</i>	29
	<i>Política de protección de la información durante auditorias.....</i>	30
5.5.	Declaración de Aplicabilidad.....	31
6.	ANEXOS.....	31
7.	DOCUMENTOS DE REFERENCIA.....	31
8.	RELACIÓN DE FORMATOS.....	31
9.	CONTROL DE CAMBIOS.....	31

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 3 de 32

1. OBJETIVO

Establecer las políticas específicas que regulan y definen el marco de aplicabilidad de la seguridad de la información, ciberseguridad y protección de la privacidad en La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea", a través de elementos, catalogados como lineamientos descriptivos que reflejan la intención y que se deben conocer, aplicar y cumplir bajo el liderazgo de la Subgerencia de Tecnologías de la Información y las Comunicaciones.

2. ALCANCE

Tiene como alcance principal la orientación y regulación de las prácticas relacionadas con la seguridad de la información en la Agencia ATENEA, con el fin de lograr una gobernanza digital coherente con el nivel de riesgo y exposición a este. Estas políticas son aplicables a todos los funcionarios, contratistas, proveedores y terceros que interactúan con los activos de información físico, electrónicos/digitales de la entidad.

El Manual de Políticas de Seguridad de la Información se estructura conforme a los lineamientos establecidos en la norma ISO/IEC 27001:2022, así como a lo definido en el Anexo 1 de la Resolución 500 de 2021. En particular, se da cumplimiento a lo requerido en la Fase 1: Planificación, la cual contempla la elaboración de los documentos fundamentales para la implementación y gestión del Sistema de Seguridad de la Información

3. DEFINICIONES

- **Activo:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización, los activos pueden ser físicos, lógicos o digitales.
- **Ataque:** intento no autorizado exitoso o fallido de destruir, alterar, deshabilitar, obtener acceso a un activo o cualquier intento de exponer, robar o hacer uso no autorizado de un activo.
- **Autenticación:** Provisión de seguridad de que una característica declarada de una entidad es correcta.
- **Autenticidad:** propiedad de que una entidad es lo que dice ser
- **Evaluación de impacto de la privacidad:** proceso general de identificación, análisis, evaluación, consulta, comunicación y planificación del tratamiento de posibles impactos en la privacidad con respecto al procesamiento de información de identificación personal, enmarcado dentro de la gestión de riesgos.
- **Gestión de incidentes de seguridad de la información:** ejercicio de un enfoque coherente y eficaz para el manejo de incidentes de seguridad de la información.
- **Gobernanza digital:** La gobernanza digital se refiere al marco de políticas, regulaciones y procesos que establecen cómo una organización gestiona y supervisa el uso de tecnologías digitales para alcanzar sus objetivos estratégicos. Involucra la toma de decisiones sobre infraestructura, datos, servicios digitales y la ciberseguridad. (OCDE (2014). *Digital Government Strategies: Good Practices by Countries.*)

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 4 de 32

- **Gobernanza de seguridad digital:** La gobernanza de la seguridad digital es el conjunto de principios, políticas y procesos que garantizan la protección de la información y los sistemas digitales en una organización. Se basa en la gestión de riesgos, la responsabilidad de los actores clave y el cumplimiento de normativas de seguridad. (ISO/IEC 27014:2020. *Information security, cybersecurity and privacy protection — Governance of information security.*)
- **Inteligencia Artificial (IA):** es una rama de la informática que se centra en la creación y el uso de sistemas capaces de realizar tareas que normalmente requieren la inteligencia humana. Estas tareas pueden incluir el aprendizaje, el razonamiento, la resolución de problemas, la percepción y el uso del lenguaje. La IA puede ser utilizada en una variedad de aplicaciones.
- **Información confidencial:** información que no está destinada a estar disponible o divulgarse a personas, entidades o procesos.
- **Objetivo de punto de recuperación-RPO:** tiempo en el que se recuperarán los datos después de que se haya producido una interrupción.
- **Objetivo de tiempo de recuperación-RTO:** Período de tiempo dentro del cual se recuperarán los niveles mínimos de servicios y/o productos y los sistemas, aplicaciones o funciones de soporte después de que haya ocurrido una interrupción
- **Sistema de información:** conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes.
- **Vulnerabilidad:** debilidad de un activo o control que puede ser explotado por una o más amenazas

4. NORMATIVIDAD ASOCIADA

- Documento CONPES No 4144, del 14 de febrero del 2025. Política nacional de inteligencia artificial.
- Decreto distrital No 472 del 2024, por el cual se adopta el modelo de gobernanza de seguridad digital para Bogotá D.C.
- Acuerdo No 002 del 2023, proferido por la comisión distrital de transformación digital, por el cual se adopta el lineamiento para el desarrollo de evaluaciones de impacto a la privacidad.
- Decreto 767 de 2022: Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Resolución 746 de 2022: Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021
- Directiva Presidencial No. 02 de 2022: Reiteración de la Política pública en materia de seguridad digital
- Resolución 500 del 10 de marzo de 2021 del Ministerio de Tecnologías de la Información y Comunicaciones.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 5 de 32

5. DESARROLLO

5.1. Políticas organizacionales

Política de estructura organizacional de seguridad de la información

- La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea", en cumplimiento al compromiso de implementar el Sistema de Gestión de Seguridad de la Información - SGSI, establece un esquema de seguridad de la información definiendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información a través de su Política de seguridad y privacidad de la información.
- Se adopta la estrategia de seguridad digital, identificando el alcance y responsable de su implementación mediante la política y manual de seguridad y privacidad de la información.
- Las políticas que componen el sistema de Gestión de Seguridad de la Información son aprobadas por la Alta Dirección o quien este designe, publicadas, comunicadas y reconocidas por los colaboradores y las partes interesadas, las actualizaciones serán a intervalos planificados o si ocurren cambios significativos.

Política de gestión de activos de Información

La Agencia, en su propósito de salvaguardar la confidencialidad, integridad y disponibilidad de la información, contenida en sus activos físicos, lógicos y digitales, define:

- Documentar un procedimiento formal para la gestión de activos de información.
- Las dependencias de la Agencia deben identificar y mantener actualizados los activos de información que tengan a su cargo.
- Los activos de información serán responsabilidad de los líderes de cada dependencia.
- Es responsabilidad de cada dependencia informar las novedades que puedan afectar la integridad, disponibilidad o confidencialidad de los activos de información.
- Los activos de información son propiedad de la Agencia, por tal motivo, los colaboradores, con asignación directa, al finalizar su contrato o acuerdo deberán devolverlos.
- Se debe identificar y documentar todos los activos a ser devueltos, como, por ejemplo: información física, hardware de autenticación, equipos y dispositivos tecnológicos, que previamente han sido asignados.
- Para la entrega y devolución de los activos tecnológicos asignados, deberá utilizarse el formato "Acta Entrega y Devolución de Equipos", el cual documenta la trazabilidad de los elementos tecnológicos físicos, su estado, seriales y responsables durante el ciclo de vida del activo.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 6 de 32

Política de uso de los activos

La Agencia, en su propósito de asegurar un uso adecuado y racional en sus activos de información, define:

- La Entidad implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo con sus roles y funciones.
- La asignación de los activos de información es para uso exclusivo del desarrollo de las actividades contractuales que le sean asignadas en la Agencia.
- El usuario de los recursos tecnológicos proporcionados por la Agencia se debe comprometer a dar buen uso, de acuerdo con las políticas definidas por el SGSI.
- Todos los colaboradores que hagan uso de los activos de información de la Agencia tienen la responsabilidad de seguir las políticas establecidas para el uso aceptable de los activos de información, entendiendo que el uso no adecuado de los recursos puede poner en riesgo la disponibilidad de los servicios tecnológicos institucionales.
- Los activos de información estarán sujetos a monitoreo y auditoria según sea necesario.
- Cada colaborador será el responsable de salvaguardar la integridad física y lógica del activo asignado, incluso en el caso que este sea retirado de la entidad, con previo VoBo de su supervisor o jefe directo.
- En el caso de presentarse la pérdida o afectación del referido activo, el colaborador será el responsable de interponer las debidas denuncias y de ser el caso, responder económicamente por la reposición del activo a su cargo.

Política de uso de los recursos tecnológicos.

La Agencia, en su propósito de asegurar un uso adecuado y racional en sus recursos tecnológicos, define:

- Todos los colaboradores deben hacer buen uso de los activos de información a los cuales tienen acceso y que son suministrados por la Agencia, de igual forma, son responsables de cualquier uso directo o indirecto, sobre este.
- Solo se permite la manipulación especializada, la cual incluye el destapar, actualizar o intervenir física y lógicamente los equipos de cómputo; al personal autorizado en la Subgerencia de Tecnologías de la Información y las Comunicaciones
- Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red (nube), archivos de vídeo, música, fotos o cualquier tipo de archivo que no sean de carácter institucional.
- No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo la disponibilidad de la información por fallas en el suministro eléctrico a los equipos de cómputo.
- La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, debe ser informada de inmediato a la Subgerencia de Gestión Administrativa, en el caso de bienes incluidos en el inventario de la entidad. Para el caso de otros dispositivos tecnológicos debe de ser reportado a la subgerencia de tecnologías de información y comunicaciones.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 7 de 32

- El traslado de los recursos tecnológicos físicos se realizará a través de la Subgerencia de Gestión Administrativa y la configuración estará a cargo de la Subgerencia de Tecnologías de la Información y las Comunicaciones.
- Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información debe ser reportado a la Subgerencia de Tecnologías de la Información y las Comunicaciones en la mayor brevedad posible.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones es la única dependencia autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales. En todo caso, privilegiando la legalidad en su uso y el respeto por la propiedad intelectual y los derechos de autor.
- Los equipos deben quedar apagados cada vez que el colaborador no se encuentre en la Agencia y no requiera realizar actividades vía remota.
- Definir y documentar la gestión de cambios en las instalaciones de procesamiento de información y los sistemas de información.

Política de uso del correo electrónico

La Agencia, en su propósito de asegurar el buen uso del correo electrónico institucional, define lo siguiente:

- El correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los colaboradores de la Agencia. Por lo anterior: El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Agencia.
- En cumplimiento de la iniciativa del uso aceptable del papel y la Eficiencia Administrativa, se debe optar por el uso del correo electrónico al envío de documentos físicos, siempre que las disposiciones legales lo permitan.
- Los mensajes de correo están respaldados por la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.), en tal caso se funda la legalidad de los mensajes de datos y las implicaciones legales que conlleva el mal uso de estos.
- No se permite el uso de correos masivos tanto internos como externos, salvo a través de las cuentas autorizadas para tal fin.
- Todo mensaje SOSPECHOSO, SPAM o CADENA debe ser inmediatamente reportado a la Subgerencia de Tecnologías de la Información y las Comunicaciones como incidente de seguridad de la información según el Procedimiento Gestión Incidentes Seguridad P2_ TIC. No está permitido el envío y/o reenvío de mensajes en cadena, debido a que puede ser contenido de virus, en especial si contiene archivos adjuntos con extensiones.exe, bat, prg, .bak, .pif, tengan explícitas referencias no relacionadas con la misión de la Entidad (como, por ejemplo: contenidos eróticos, alusiones a personajes famosos).
- La cuenta de correo institucional no debe ser registrada en páginas o sitios publicitarios, de comercio electrónico, deportivos, casinos, o a cualquier otra ajena a los fines institucionales.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 8 de 32

- No se permite el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
- No se dará uso del correo electrónico de la Agencia, para distribuir información institucional de carácter reservado o clasificado, sin el previo análisis y autorización del líder de cada dependencia, al que corresponde la clasificación del activo.
- El envío de mensajes desde el correo electrónico debe contener una leyenda de confidencialidad y aplicarse en la firma institucional de todos los usuarios de la Agencia, para el caso de mensajes que contengan esta característica o etiqueta.
- El único servicio de correo electrónico autorizado para el manejo de la información institucional en la Entidad es el asignado por la Subgerencia de Tecnologías de la información, y que cuenta con el dominio @agenciaatenea.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad.

Política de uso de internet

La Agencia, en su propósito de asegurar el buen uso del servicio de acceso a internet, define:

- La Entidad permite el acceso al servicio de internet, estableciendo directrices que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, minimizando la exposición a riesgos de, pérdidas de información, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones es la encargada de autorizar y aplicar los cambios solicitados de permisos de navegación a los usuarios de La Agencia, previa solicitud del jefe de cada una de las dependencias.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones implementa herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales así mismo controla el acceso a la información contenida en portales de almacenamiento en el internet para prevenir la fuga de información.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones implementara los controles necesarios para evitar el acceso a redes sociales no autorizadas o diferentes a las institucionales, sistemas de mensajería instantánea, páginas con contenido ofensivo, insultante, injurioso y violatorio de los derechos de autor; así como el acceso a sistemas de almacenamiento en la nube y cuentas de correo no institucional. En caso de ser requerido por las funciones del cargo, el jefe inmediato debe remitir la solicitud con la respectiva justificación a La Subgerencia de Tecnologías de la Información y las Comunicaciones, para que sea evaluado y autorizado según corresponda.
- La Agencia se reserva el derecho de monitorear los accesos y las conexiones a diferentes sitios, páginas o recursos de acceso vía internet; y por tanto el uso del servicio de internet de todos los colaboradores, además de limitar el acceso a determinadas páginas de Internet, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines de la Entidad.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 9 de 32

Política para uso de dispositivos móviles

La Agencia, en su propósito de asegurar el buen uso de dispositivos móviles, define:

- Los dispositivos móviles que sean asignados por la Agencia deberán mantener la configuración respectiva para restringir la instalación de software, la responsabilidad sobre la gestión, control y medidas que prevengan su robo o sustracción, se encuentran bajo la responsabilidad de cada usuario. Los dispositivos móviles deben estar configurados para acceder a través de credenciales de acuerdo con la asignación.
- Los dispositivos móviles de la Agencia que sean retirados de las instalaciones deben contener mecanismo de cifrado de tal forma que evite divulgación de información en caso de pérdida o robo.
- Todos los dispositivos móviles asignados deben tener instalado el antivirus institucional.
- El uso de conexión a la red para los dispositivos móviles ajenos a la Agencia es segmentado para proveer únicamente el servicio de internet, restringiendo el acceso a la data y navegación interna.

Política de uso de mensajería instantánea y redes sociales

La Agencia, en su propósito de asegurar el buen uso de los recursos asociados al acceso de redes sociales, define, las pautas generales para asegurar una adecuada protección de la información, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

- La información que se publique o divulgue por cualquier medio de Internet, de cualquier colaborador de la Agencia, que sea creado a nombre personal en redes sociales como -pero sin limitarse: Twitter®, Facebook®, YouTube®, blogs, Instagram, se considera fuera del alcance del Sistema de Gestión de Seguridad de la Información y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que lo genere.
- Toda información distribuida en las redes sociales que sea originada por la entidad debe ser autorizada por los líderes de cada dependencia para ser socializada y publicada por el responsable con competencia directa.
- No se debe utilizar el nombre de la Agencia en redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la Entidad.
- Las personas designadas para el manejo y gestión de contenido en las redes sociales de la Agencia deben acatar las directrices dadas en el presente documento.
- La dependencia que requiera la apertura de una red social bajo el dominio de la Agencia debe presentar una solicitud motivada, relacionando la necesidad, objeto y alcance de la cuenta institucional, enunciando los datos personales de los colaboradores que realizarán la administración de la red social, con aplicabilidad sólo en caso de autorización por parte del directo responsable en la gestión de las redes sociales de la entidad
- Los responsables de cada red social deberán aplicar complejidad en las contraseñas de las cuentas institucionales, acatando los protocolos de seguridad de estas y realizando el cambio

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 10 de 32

periódicamente. Los correos asociados la red social y de recuperación de contraseñas, deben ser institucionales y en ningún caso de uso personal.

- El Sistema de Gestión de Seguridad de la Información realizará la verificación de las medidas y controles implementados de seguridad, encaminadas a evitar el acceso abusivo a la plataforma, que puedan afectar la imagen y la credibilidad de la entidad.
- No se deben vincular cuentas de correo electrónico personales en las redes sociales que se apertura bajo el dominio de la Agencia.
- No se recomienda la administración de las redes sociales la Agencia en dispositivos móviles personales

Política de clasificación de la información La Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea" consiente de aplicar el nivel de protección apropiado de acuerdo con el tipo de calificación establecido por las disposiciones legales, define lo siguiente:

- Las categorías de calificación de la información que se adoptaran son: INFORMACIÓN PÚBLICA, INFORMACIÓN PÚBLICA RESERVADA e INFORMACIÓN PÚBLICA CLASIFICADA.
- Todos los activos de información indiferente de su medio de almacenamiento deben ser clasificados de acuerdo con los lineamientos institucionales creados para tal fin. Esta actividad debe ser realizada por los responsables sobre la gestión de los activos.
- Toda la documentación o información generada en la Agencia debe contener clasificación.
- Se desarrollan e implementan las directrices para el etiquetado de la información de acuerdo con las categorías definidas y adoptadas, las cuales permitirán reconocer fácilmente la clasificación del activo de información.
- La información que se intercambie en cumplimiento de acuerdos institucionales con otras entidades debe incluir la clasificación e informar al destinatario la interpretación de la clasificación con el fin de que este le asigne las protecciones requeridas.
- En el caso de los sistemas de información que contienen información sensible o crítica se deben implementar mecanismos que indiquen la clasificación e identificación del contenido.

Política para la transferencia de información

La Agencia, en su propósito de asegurar una adecuada aplicabilidad de los procesos de transferencia de información, define:

- Los responsables, en la gestión de activos de información de cada una de las dependencias, son los encargados de proteger la información transferida al interior y exterior de La Agencia.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones, realiza el control del uso de sistemas de transferencia de archivos vía FTP a terceros, para lo cual dicho mecanismo de transmisión se implementa de manera segura.
- Los canales de red usados para la transferencia de información deberán contar con un mecanismo que no permita la fuga o interceptación de información, en su defecto la información que viaje por estos deberá estar cifrada.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 11 de 32

- Las transferencias de información deben de estar amparadas por acuerdos interinstitucionales o de confidencialidad que permitan mantener los estándares de seguridad sobre esta.

Política de control y gestión de acceso

La Agencia, en su propósito de asegurar una adecuada control y gestión de acceso, define:

- La Subgerencia de Tecnologías de la Información y las Comunicaciones establecerá las directrices para la gestión de usuarios dónde se detalle el uso de credenciales únicas, autenticación multifactor, así mismo; para el uso de identificaciones compartidas o grupales por razones justificadas, establecer los tiempos de bloqueo o modificación de cuentas por inactividad, intentos fallidos, cambio de roles o retiro.
- Se debe mantener un registro centralizado de los accesos suministrados.
- Los accesos se deben realizar por las herramientas autorizadas, no se permiten el uso de software de acceso remoto no licenciado o autorizado, por la Agencia.
- Todo aplicativo informático o software debe ser adquirido u aprobado, para su uso e instalación en la infraestructura de la Agencia, por Subgerencia de Tecnologías de la Información y las Comunicaciones.
- El control de acceso a la Información se realiza aplicando el principio de mínimo privilegio necesario para la realización de las actividades asignadas.
- El acceso a la información se realiza de acuerdo con los niveles de calificación de la información y perfil asignado al usuario.
- Para el acceso a los espacios de archivo tanto en las dependencias como el Archivo Central, se debe dar aplicación a los controles y directrices establecidos por la subgerencia administrativa.
- Los colaboradores que, tengan bajo su responsabilidad la custodia de información física almacenada en los archivadores que se encuentra en las oficinas, deben mantener el control de acceso a esta información; por lo tanto, debe estar bajo llave. Se recomienda que las llaves se guarden en un sitio seguro, dando cumplimiento a lo establecido en la presente política.
- Los accesos a activos digitales, con privilegios especiales deben contar con la aprobación de la Subgerencia de Tecnologías de la Información y las Comunicaciones y estar debidamente justificados por el solicitante.
- Los responsables del manejo de usuarios privilegiados deben aceptar su responsabilidad frente al uso del usuario asignado.
- Los administradores funcionales de los sistemas de información deben realizar revisiones periódicas por lo menos una semestral de los usuarios activos en los diferentes sistemas de información, dominio y red.
- Es responsabilidad de los líderes de cada dependencia, notificar al proceso de gestión humana y a los administradores de TI la desvinculación de un funcionario, cesiones y terminaciones anticipadas de contratista para que sean retirados los accesos de todos los sistemas incluidos los accesos físicos a las diferentes instalaciones de la Agencia.
- En el caso de los contratistas se debe realizar la configuración automática para que el día de la terminación del contrato sean inhabilitadas las credenciales asignadas.
- La agencia se reserva el derecho de uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD).

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 12 de 32

- El propietario del activo de información será responsable de autorizar el acceso a los sistemas y a la información bajo su administración, asegurando que cada solicitud de acceso esté alineada con las funciones, competencias y responsabilidades del usuario.
- Los propietarios de los activos deberán definir los requisitos de seguridad de la información aplicables al uso del activo, los niveles de permiso requeridos para su acceso y las restricciones asociadas, manteniendo trazabilidad de las autorizaciones que otorguen.
- Toda asignación o modificación de accesos deberá ser solicitada por el propietario del activo y aprobada mediante las herramientas y/o medios que sean definidos, considerando el principio de mínimo privilegio y la segregación de funciones.

Segregación de Funciones como Control de Seguridad de la Información

En el marco del Sistema de Gestión de Seguridad de la Información – SGSI, la Agencia adopta la Segregación de Funciones como un control para mitigar riesgos asociados al uso indebido de privilegios, errores no intencionados y accesos no autorizados sobre los activos de información.

Este control se orienta exclusivamente desde la perspectiva de seguridad de la información y no modifica la estructura organizacional ni las responsabilidades funcionales de los procesos.

En consecuencia:

- Para los procesos que involucren el acceso, tratamiento o administración de activos de información, deberán implementarse controles que eviten la concentración de privilegios críticos en una misma persona.
- Como mínimo, se deberá asegurar la diferenciación de las siguientes funciones de seguridad:
 - Autorización de accesos o cambios sobre el activo.
 - Ejecución técnica de la acción autorizada.
 - Verificación y seguimiento del control aplicado.
- En los entornos tecnológicos se deberá preservar la separación lógica entre ambientes de desarrollo, pruebas y producción, como medida de protección de la integridad y disponibilidad de la información.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones implementará mecanismos técnicos que permitan la asignación diferenciada de perfiles y privilegios, garantizando trazabilidad y control.
- Los propietarios de los activos de información serán responsables de validar periódicamente los niveles de acceso asignados, desde la óptica del riesgo y la protección del activo.
- Las situaciones en las que, por restricciones operativas, no sea posible aplicar plenamente este control, deberán ser documentadas mediante memorando dirigido a la Subgerencia TIC, indicando la justificación y los controles compensatorios adoptados.

Gestión de accesos a plataformas tecnológicas externas

La Agencia reconoce que determinados procesos institucionales requieren el uso de plataformas tecnológicas administradas por entidades externas del orden distrital o nacional (portales

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 13 de 32

gubernamentales, sistemas de información sectoriales, plataformas de reporte, entre otros). Teniendo en cuenta que la administración técnica de dichas plataformas corresponde a la entidad propietaria del sistema, se establecen las siguientes directrices:

- La gestión, custodia y control de las credenciales de acceso a plataformas de entidades externas es responsabilidad del Gerente, Subgerente o Jefe de Oficina de la dependencia funcional a la que corresponde el proceso institucional soportado en dicha plataforma, independientemente de quién sea el usuario operativo del sistema.
- Cada dependencia funcional identificará las plataformas externas asociadas a sus procesos y designará un funcionario o contratista responsable del acceso, quien será el único autorizado para operar las credenciales asignadas. Dicha designación deberá quedar documentada mediante memorando interno o correo electrónico institucional suscrito directamente por el Gerente, Subgerente o Jefe de Oficina de la dependencia, sin delegación de esta comunicación a asistentes u otros colaboradores. El mensaje de designación deberá indicar como mínimo: nombre completo del designado, plataforma asignada, fecha de inicio y fecha estimada de finalización. Esta documentación deberá conservarse en la dependencia, actualizarse ante cualquier cambio de responsable y revisarse para verificar su vigencia.
- La solicitud de creación, modificación o revocación de usuarios ante la entidad externa deberá ser gestionada directamente por el responsable de la dependencia funcional o por quien la entidad externa defina como interlocutor válido, sin intermediación de la Subgerencia TIC. Cuando se requiera actualización o cambio de contraseña de credenciales institucionales, esta deberá adelantarse de acuerdo con las directrices de la entidad, y gestionada por Gerente, Subgerente o Jefe de Oficina de la dependencia, quien comunicará mediante memorando o correo electrónico al funcionario o contratista designado las novedades .
- Ante ausencias temporales del funcionario o contratista designado (vacaciones, licencia, incapacidad u otra), el Gerente, Subgerente o Jefe de Oficina deberá gestionar la continuidad del acceso de la siguiente manera: si se trata de credenciales personales asignadas por la entidad externa, gestionará directamente ante dicha entidad la reasignación o inactivación temporal según sus directrices; si se trata de credenciales institucionales, realizará la reasignación interna a otro funcionario o contratista de la dependencia por el tiempo que dure la ausencia, modificando las contraseñas de acceso. En ningún caso esta gestión podrá trasladarse a la Subgerencia TIC.
- Al momento de desvinculación, cesión o terminación de contrato de un colaborador con acceso a plataformas externas, el Gerente, Subgerente o Jefe de Oficina deberá gestionar de manera inmediata -y en ningún caso después del último día de vinculación- la revocación del acceso directamente ante la entidad correspondiente. Si se trata de credenciales institucionales, deberá realizarse el cambio de contraseña y la reasignación a otro funcionario o contratista de la dependencia. Esta responsabilidad no podrá recaer en la persona desvinculada.
- La Subgerencia TIC no administra, custodia ni gestiona credenciales de plataformas de entidades externas. Su rol se limita a recibir el reporte de incidentes de seguridad asociados y a orientar en buenas prácticas cuando sea requerido por la dependencia funcional.
- Todo incidente de seguridad relacionado con estos accesos (pérdida de credenciales, acceso no autorizado, uso indebido, entre otros) deberá reportarse a la Subgerencia TIC conforme al Procedimiento de Gestión de Incidentes. e

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 14 de 32

Política de establecimiento, uso y protección de claves de acceso

La Agencia, en su propósito de asegurar una adecuada gestión de claves de acceso, define:

- Ningún usuario deberá acceder a la red o a los servicios de La Agencia, utilizando una cuenta de usuario o credenciales de otro usuario.
- Toda acción realizada usando la clave de acceso es responsabilidad directa del usuario al que se le asignó las credenciales.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.
- El cambio de contraseña solo debe ser solicitado por el titular de la cuenta, comunicándose a la Subgerencia de Tecnologías de la Información y las Comunicaciones, en donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por su jefe inmediato (previa autorización por parte de la Subgerencia de Tecnologías de la Información y las Comunicaciones).
- Los colaboradores propenderán por no dejar visibles las credenciales asignadas.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones Implementará mecanismos para que los usuarios cambien su contraseña de acceso al usarla por primera vez en los sistemas de información o servicios a los que se les permita el acceso; así como implementar una política de red que solicite cambio de credenciales en periodos definidos.
- Las claves o contraseñas de acceso deben contener los siguientes requisitos de seguridad:
 - Tener mínimo ocho (8) caracteres alfanuméricos.
 - Cada vez que se cambien estas deben ser distintas por lo menos de las últimas doce anteriores.
 - La contraseña debe ser cambiada cada sesenta (60) días.
 - El sistema/aplicación debe informar al usuario el vencimiento de la credencial como mínimo 10 días antes de que esto ocurra.
 - No debe contener el nombre de usuario y caracteres consecutivos como - abcd,123456

Manejo de contraseñas para administradores de TI

La Agencia, en su propósito de asegurar una adecuada gestión de las contraseñas por los administradores de TI, define:

- Se debe garantizar en las plataformas de tecnología que el ingreso a la administración en lo posible se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.
- Las contraseñas referentes a las cuentas “predefinidas” incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.
- Los administradores de TI pertenecientes a la Subgerencia de Tecnologías de la Información y las Comunicaciones no deben dar a conocer sus credenciales institucionales de acceso a los

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 15 de 32

sistemas de información a terceros, sin previa autorización escrita del Subgerente de Tecnologías de la Información y las Comunicaciones.

- Los Administradores de TI pertenecientes a la Subgerencia de Tecnologías de la Información y las Comunicaciones deben emplear obligatoriamente contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación que posee la entidad de acuerdo con el rol asignado.

Política en la relación con proveedores

La Agencia, en su propósito de asegurar un adecuado relacionamiento con los proveedores, define:

- Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas, es responsabilidad directa de los supervisores a cargo y para ello tendrán en cuenta las medidas necesarias de acuerdos de confidencialidad, protección de datos personales y las políticas de seguridad de la información, definidas por la entidad.
- Se deben establecer obligaciones dentro de los contratos con terceros que contemplen aplicación de estándares y mejores prácticas de gestión de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.
- Se deben establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de La Agencia, las cuales deben ser divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios y posteriormente por los supervisores.
- En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una cláusula que contemple el cumplimiento de las políticas, procedimientos y directrices relacionados con la seguridad de la información
- Los funcionarios de La Agencia que tengan responsabilidad como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.
- Todo proveedor y/o contratistas debe estar informado de las políticas y directrices que componen el Sistema de Gestión de Seguridad de la Información -SGSI.
- Todo proveedor y/o contratistas debe realizar la devolución de los activos de información asignados por la Agencia.
- Se deben establecer mecanismos o condiciones con los contratistas o proveedores que permitan realizar la gestión de cambios en los servicios suministrados

Política para el uso de servicios en la nube

La Agencia, en su propósito de asegurar un adecuado despliegue y operación de servicios en nube, define:

- En el uso de servicios en la nube contratados por la Agencia se deben gestionar los riesgos de seguridad.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 16 de 32

- El proveedor deberá informar de inmediato cualquier incidente de seguridad que afecte la confidencialidad, integridad o disponibilidad de los datos alojados en la nube, asegurando que la Agencia pueda responder de manera oportuna.
- Identificar y definir la responsabilidad compartida de la seguridad de la información y los esfuerzos de colaboración entre el proveedor del servicio y la Agencia. En caso de que los acuerdos de servicios estén predefinidos y no están abiertos a negociación la Agencia debe revisar los definidos y validar que se contemplen los requisitos de confidencialidad, integridad, disponibilidad y manejo de la información de la entidad.
- La Agencia, actuando como cliente del servicio en la nube definirá si debe exigir al proveedor de servicio que se notifique antes de realizar cambios sustanciales que afecten la entidad, como los relacionados a continuación, pero sin limitarse:
 - Cambios de hardware o software, reconfiguraciones y demás que afecten o cambien la oferta de servicios en la nube.
 - Realizar tratamiento de información en una nueva jurisdicción geográfica o legal.
 - Uso de proveedores de servicios similares o subcontratados.
- La entidad, en el uso de sus capacidades de nube, incluirá componentes y/o herramientas basadas en inteligencia artificial (IA), previamente identificadas y valoradas desde una perspectiva integral del riesgo. Dichas herramientas podrán ser nativas desplegadas por el proveedor del servicio o vinculadas por la entidad en sus sistemas de información o aplicaciones de misión específica.

Política de gestión de los incidentes de la seguridad de la información

La Agencia, en su propósito de asegurar una adecuada gestión de los incidentes de información, define:

- Garantizar que los eventos e incidentes de seguridad que se presenten con los activos de información sean comunicados y atendidos oportunamente, empleando el Procedimiento Gestión Incidentes Seguridad, con el fin de tomar oportunamente las acciones correctivas de acuerdo con el procedimiento de gestión de acciones de mejora.
- Establecer los respondientes para la atención de incidentes dentro de la Agencia.
- Identificar y documentar contacto con autoridades, grupos de interés que manejen cuestiones relacionados con seguridad de la información e incidentes.
- Asegurar una gestión consistente y eficaz de la evidencia relacionada con incidentes de seguridad de la información para efectos de acciones disciplinarias y legales.
- Fortalecer y mejorar los controles de seguridad de la información a través de la documentación y conocimiento de los incidentes de seguridad que se presenten en la entidad.
- Desplegar y activar los planes de recuperación ante desastres de la plataforma tecnológica (DRP), cuando la evaluación integral del incidente, así lo requiera.

Política de seguridad de la información durante la interrupción

La Agencia, en su propósito de asegurar una adecuada gestión de las interrupciones en su operación tecnológica, define:

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 17 de 32

- Se debe definir el conjunto de procedimientos y estrategias para contrarrestar las interrupciones en las actividades misionales de la entidad, proteger sus procesos críticos contra fallas mayores en los sistemas de información o contra desastres y asegurar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una contingencia.
- Prevenir interrupciones en las actividades de la plataforma informática de la Agencia que, van en detrimento de los procesos críticos de TI afectados por situaciones no previstas o desastres.
- Los proveedores de servicios TI críticos deberán contar con alternativas de continuidad, lo cual, es estipulado en las condiciones de contratación por cada uno de los responsables.
- Los requisitos de seguridad de la información deben incluirse en los procesos de gestión de la continuidad del negocio.
- Se debe desarrollar e implementar un Plan de recuperación de TI, para asegurar que los procesos misionales de TI de la Agencia, los cuales serán restaurados dentro de escalas de tiempo razonables. El plan de acción que permitirá la recuperación de los servicios de TI, se desarrollará teniendo en cuenta los siguientes aspectos:
 - Identificación y asignación de prioridades a los procesos críticos de TI de la Agencia de acuerdo con su impacto en el cumplimiento de la misión de la entidad.
 - Documentación de la estrategia de continuidad TI.
 - Documentación del plan de recuperación de TI, de acuerdo con la estrategia definida anteriormente.
 - Plan de pruebas para la estrategia de recuperación de los servicios de TI.

Política de cumplimiento de requisitos legales, estatutarios, reglamentarios y contractuales

La Agencia, en su propósito de asegurar una adecuada aplicabilidad para el cumplimiento de requisitos legales, estatutarios, reglamentarios y contractuales, define:

- La entidad debe gestionar riesgos para prevenir el incumplimiento de obligaciones legales relacionadas con seguridad de la información.
- Todos los sistemas de información que capturen datos personales deben cumplir con la política de protección de datos personales definida por la Agencia.
- Se debe identificar, documentar y actualizar los requisitos legales y reglamentados relacionados con seguridad de la información.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones deberá garantizar que todo el software que se ejecute esté protegido por derechos de autor y requiera licencia de uso o software de libre distribución y uso.
- La entidad mantiene prueba y evidencia de propiedad del licenciamiento adquirido.
- Los colaboradores de la Agencia deben cumplir con las Leyes de derechos de autor y acuerdos de licenciamiento de software, se recuerda que es ilegal duplicar software y documentación sin la autorización del propietario bajo los principios de derechos de autor y, la reproducción no autorizada es una violación a la Ley.

Definición de excepciones y desviaciones:

Cuando el cumplimiento de una política, control o directriz de seguridad no sea posible, o su aplicación represente un riesgo mayor para la operación, el Jefe de Oficina, Gerente/Subgerente o Director

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 18 de 32

deberá solicitar formalmente una excepción ante la Subgerencia de Tecnologías de la Información y las Comunicaciones. Esta solicitud deberá estar debidamente soportada, indicando la justificación, el tiempo de vigencia de la excepción y los controles alternos que se implementarán.

Las desviaciones frente a las políticas de seguridad deberán registrarse y analizarse, evaluando su impacto y definiendo, según corresponda, la implementación de acciones correctivas y las medidas aplicables.

Política de tratamiento de datos personales

La Agencia, en su propósito de asegurar una adecuada aplicabilidad del tratamiento de datos personales, define:

- En cualquiera sea el caso el tratamiento de datos personales se realizará conforme la Ley 1581 de 2012, sus Decretos reglamentarios y la Política de Tratamiento de Datos Personales
- Datos de menores de edad: El tratamiento de los datos personales de menores de edad es facultativo y debe realizarse con autorización de los padres de familia o representantes legales del menor, en concordancia con lo establecido por la Ley 1098 de 2006 “Código de Infancia y Adolescencia” y la Política de Tratamiento de Datos Personales.
- Datos personales y biométricos: En la(s) sede(s) de la Agencia en donde se realice recolección de datos personales y datos biométricos -como huellas e imágenes, se deben fijar avisos/habladores, con el fin que los titulares registrados en la Entidad conozcan sus derechos.
- Sesiones virtuales: Se debe informar los asistentes que se va a realizar la grabación de esta, de tal forma que si algún asistente no está de acuerdo lo debe indicar al organizador; si no se recibe alguna observación, se da por entendido que ha dado su aprobación.
- Se promueve la realización de evaluaciones de impacto a la privacidad de la información, en plataformas, herramientas o sistemas de información a desplegar por parte de la entidad en sus infraestructuras tecnológicas propias o de terceros, y mediante las cuales se capturen y procesos dato catalogados como personales.
- Se adopta el principio de responsabilidad demostrada, como guía para la aplicabilidad de las políticas de protección de datos personales.

Política de revisión independiente de la seguridad de la información.

La Agencia, en su propósito de mantener una adecuada independencia en la definición y adopción del marco de políticas de seguridad de la información, define:

- Garantizar el funcionamiento del sistema de gestión de seguridad de la información de acuerdo con las políticas y procedimientos implementados en la Agencia.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 19 de 32

- A través de la Oficina de Control Interno de Gestión se realizarán las verificaciones del cumplimiento de objetivos, controles, políticas y procedimientos de seguridad de la Información.
- Todos los líderes de proceso deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información en la dependencia bajo su responsabilidad.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones a través del Sistema de Gestión de Seguridad de la Información realizará revisiones esporádicas no programadas con el fin verificar el cumplimiento de las políticas de seguridad de la información en las instalaciones de la Agencia.

Política de cumplimiento

La Agencia, en su propósito de asegurar una adecuada aplicabilidad del cumplimiento de las políticas de seguridad de la información, define:

- Los diferentes aspectos contemplados en esta Política son de obligatorio cumplimiento para todos los colaboradores de la Agencia. En caso de que se infrinjan las políticas de seguridad de forma intencional o por desconocimiento, la Agencia tomará las acciones administrativas, disciplinarias y legales correspondientes.
- Con la aplicabilidad de las políticas establecidas se debe prevenir el incumplimiento de las leyes, estatutos, regulaciones y obligaciones contractuales que se relacionen con los controles de seguridad de la información.
- Cuando el cumplimiento de una política, control o directriz de seguridad no sea posible, o su aplicación represente un riesgo mayor para la operación, el Jefe de Oficina, Gerente/Subgerente o Director deberá solicitar formalmente una excepción ante la Subgerencia TIC. Esta solicitud deberá solicitar formalmente una excepción ante la Subgerencia TIC mediante memorando o a través de la herramienta de mesa de servicios institucional.

5.2. Política de seguridad del recurso humano.

La Agencia, en su propósito de asegurar un adecuado entendimiento y aplicabilidad por parte del talento humano, de las políticas de seguridad de la información, define:

- Se debe asegurar que los funcionarios, contratistas y demás colaboradores de La Agencia, adopten sus responsabilidades en relación con las políticas de seguridad de la información y actúen de manera consistente frente a las mismas, con el fin de reducir los riesgos.
- Los acuerdos contractuales deben establecer la responsabilidad del colaborador en cuanto a seguridad de la información -derechos de autor, confidencialidad y no divulgación de la información durante y después del empleo.
- Establecer estrategias para que los colaboradores tomen conciencia sobre lo relacionado con seguridad de la información.
- Articular los procedimientos administrativos y disciplinarios en situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información, conforme a las normas que lo reglamenten en el sector público.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 20 de 32

- Implementar procedimientos que permitan identificar las novedades, desvinculaciones, terminaciones o cesiones de contrato, con el fin de retirar o modificar los accesos físicos y lógicos en la Agencia.

Política de trabajo a distancia

La Agencia, en su propósito de asegurar una adecuada gestión de la seguridad de la información, en entornos de trabajo a distancia, define:

- La Subgerencia de Tecnologías de la Información y las Comunicaciones propenderá por la identificación de necesidad y licenciamiento de la VPN - Virtual Private Network
- Se debe hacer uso de las herramientas colaborativas de Microsoft 365 para llevar a cabo el envío, recepción, transferencia y transmisión de información institucional. Además, de aprovechar el almacenamiento en la nube -OneDrive y SharePoint-, evitando el uso del almacenamiento local.
- Las actividades de acceso remoto (uso de VPN - Virtual Private Network) a los sistemas informáticos y activos de información de la Entidad, se autorizan de acuerdo con las necesidades específicas de la dependencia solicitante.
- Se recomienda que mientras se haga uso de VPN desde un equipo personal, éste tenga instalado y actualizado el antivirus y que el sistema operativo cuente con las actualizaciones de seguridad y licenciado.
- Configurar el mecanismo de autenticación multifactor (MFA) con el fin de fortalecer los controles de seguridad y evitar accesos no autorizados a la información
- La Subgerencia de Tecnologías de la Información y las Comunicaciones realizará las configuraciones de seguridad, aprovisionamientos y revocación de acceso a la VPN
- La Subgerencia de Tecnologías de la Información y las Comunicaciones se reserva el derecho de monitorear el uso de las herramientas de Microsoft 365 para garantizar el cumplimiento de las políticas establecidas y llevar a cabo revisiones periódicas para evaluar la seguridad de la información.
- Se aplicarán las definiciones y decisiones tomadas por la entidad y estipuladas en diferentes documentos internos como circulares, resoluciones y otro tipo, que brinden aplicabilidad en la materia.
- Todo dispositivo personal utilizado para acceder a la red, aplicaciones o información de la entidad debe contar con el sistema operativo y todo el software actualizado, incluyendo la instalación de un antivirus y los últimos parches de seguridad
- Todo dispositivo personal empleado para ejecutar actividades relacionadas con la Agencia no debe dejarse desatendido en lugares públicos o de fácil acceso para personas no autorizadas. Cuando no se utilicen, los dispositivos deben estar bloqueados.

Política de reporte de eventos de seguridad de la información

La Agencia, en su propósito de asegurar una adecuada gestión de los eventos asociados a la seguridad de la información, define:

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 21 de 32

- Los colaboradores y terceros deben reportar cualquier evento sospechoso observado en los activos de información.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones definirá y socializará los canales para el reporte de eventos e incidentes de seguridad de la información, detectados.

5.3. Política de seguridad física

Política de perímetros y entrada física

La Agencia, en su propósito de asegurar una adecuada gestión del acceso y perímetros seguros de entrada física, define:

- La Agencia gestiona el acceso a sus instalaciones físicas mediante controles de seguridad. El ingreso al edificio se realiza a través de un sistema de autenticación por huella digital. Adicionalmente, el acceso a las oficinas de la Agencia también se controla mediante un sistema biométrico de huella. Las instalaciones cuentan con un sistema de videovigilancia que refuerza la seguridad en las áreas comunes y de acceso.
- Los visitantes deben registrarse en la entrada, ser autorizados por un colaborador para ingresar y durante su estancia deben estar acompañados por el funcionario o contratista con el cual están desarrollando su actividad.
- Definir y usar perímetros de seguridad para proteger las áreas de procesamiento de información sensible o crítica, teniendo en cuenta:
 - Todas las puertas externas deberán tener mecanismos de control que eviten el acceso no autorizado.
 - Las puertas y ventanas se deben mantener cerradas con llave cuando no hay supervisión.
 - Prohibir el uso de equipo fotográfico, de video, audio u otro equipo de grabación cuando no se cuente con autorización para ello.
- Los controles de acceso físico a las instalaciones deben permitir el acceso únicamente al personal autorizado.
- Todos los colaboradores que tengan asignado el carné deben portarlo en lugar visible.
- Para el caso de las áreas de despacho y carga se debe:
 - Inspeccionar el material que ingresar para detectar presencia de materiales peligrosos.
 - Restringir para el personal identificado y autorizado.

Política de escritorio despejado y pantalla limpia

La Agencia, en su propósito de asegurar una adecuada gestión de entornos físicos y digitales ordenados y despejados, define:

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 22 de 32

- Los colaboradores y terceros que tienen algún vínculo con La Agencia deben conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- Todos los equipos y sistemas de información deben configurarse con una función de tiempo de espera o cierre de sesión automático.
- Los usuarios de los sistemas de información y comunicaciones de la Agencia deben bloquear la pantalla de su computador, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
- Los usuarios de los sistemas de información deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.
- Al imprimir documentos con información pública reservada y/o pública clasificada, deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

Política de protección contra amenazas físicas y ambientales

La Agencia, en su propósito de asegurar una adecuada protección de la información en las redes de datos y de su infraestructura de soporte, define:

- En las instalaciones del centro de datos o de los centros de cableado, No está permitido:
 - Fumar dentro de las instalaciones.
 - Introducir alimentos o bebidas.
 - El porte de armas de fuego, corto punzantes o similares.
 - Mover, desconectar y/o conectar equipo de cómputo sin autorización
 - Alterar software instalado en los equipos sin autorización.
 - Alterar o dañar las etiquetas de identificación de los recursos tecnológicos o sus conexiones físicas.
 - Extraer información de los equipos en dispositivos externos.
 - Abuso y/o mal uso de los recursos tecnológicos.
 - Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.
 - Modificar la configuración del equipo o intentarlo sin autorización
- Contar con herramientas que permitan registrar el acceso de los colaboradores a estas áreas.
- Revisar y actualizar periódicamente los derechos de acceso.
- Cada centro de cableado contiene llave de ingreso y/o tarjeta de acceso, las cuales deben permanecer custodiadas por el colaborador designado para tal fin.
- Considerar la implementación de controles contra incendios inundaciones, sobretensiones eléctricas y en general de las posibles amenazas físicas y ambientales.
- Los medios y equipos donde se almacena procesan o comunica la información (física o electrónica), deben mantenerse con las medidas de protección físicas y lógicas.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 23 de 32

Política de medios de almacenamiento

La Agencia, en su propósito de asegurar una adecuada gestión de los medios de almacenamiento de información en su entorno tecnológico, define:

- Los medios de almacenamiento extraíble pueden ocasionalmente generar riesgos para la Agencia al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada.
- El medio autorizado para almacenamiento es el perteneciente a las herramientas en la nube licenciadas por la entidad
- Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través de la Subgerencia de Tecnologías de la Información y las Comunicaciones y será objeto de auditorías de seguridad mediante las herramientas consideradas para tal fin.
- Solo se habilitarán los puertos de conexión de medios de almacenamiento extraíbles si existe una razón institucional para su uso.
- Se debe realizar monitoreo a la transferencia de información cuando sea necesario utilizar medios de almacenamiento extraíble.
- Se debe implementar un procedimiento para la transferencia de medios físicos, se entenderán todos los activos de información físicos.

Política de seguridad del cableado

La Agencia, en su propósito de asegurar una adecuada protección en la transmisión de información y en el cuidado del cableado estructurado de redes y telecomunicaciones, define:

- Se implementan controles que permiten proteger las líneas eléctricas y de telecomunicaciones de cortes accidentales.
- Los cables de alimentación y comunicación deben estar separados para evitar interferencias.
- Implementar conductos blindados, cajas cerradas y alarmas en los puntos de terminación.
- Establecer mecanismos de acceso controlado a los paneles de conexión y centros de cableado.
- Se debe propender por el uso de cables de fibra óptica.

Política de mantenimiento de equipos

La Agencia, en su propósito de asegurar una adecuada gestión y control del mantenimiento de equipos bajo responsabilidad de la subgerencia de tecnologías de información y comunicaciones, define:

- Se establecer un cronograma para el mantenimiento de los equipos tecnológicos (UPS, routers, computadores, aires, Switch)
- Solo las personas autorizadas realizaran las reparaciones y mantenimientos respectivos.
- Cada mantenimiento debe contar con una ficha técnica que permita establecer el mantenimiento realizado, fecha, reparaciones, persona que realiza la actividad y quien recibe a satisfacción.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 24 de 32

- En caso de ser requerido un mantenimiento remoto, se solicitará la autorización de La Subgerencia de Tecnologías de la Información y las comunicaciones a través de un mecanismo seguro y licenciado por la Entidad.

Política de eliminación segura o reutilización de equipos

La Agencia, en su propósito de asegurar una adecuada eliminación de información en la reutilización de sus equipos, define:

- En los casos en que se almacene información en equipos que se encuentran en las salas de reuniones de la Entidad, salas de juntas y salones de capacitación; las personas que han realizado la reunión, en el momento que no se requiera su uso en estos dispositivos, deben eliminarla de forma permanente; con el fin de evitar que personas no autorizadas puedan conocerla.
- Cuando no se requiera la información contenida en un medio de almacenamiento reusable, se debe borrar para que no sea recuperable y registrar los resultados como prueba de la eliminación. En caso de los equipos en condición de alquiler, se debe realizar el borrado antes de la devolución y el formateo de estos en condición de bajo nivel.
- La información almacenada con nivel alto de confidencialidad o integridad en medios removibles debe contar con técnicas de cifrado para evitar accesos no autorizados.
- Para los medios que contienen información confidencial, se deben almacenar y disponer de forma segura, mediante incineración, destrucción a través de máquinas destinadas para tal fin o proceso de borrado seguro, de acuerdo con las directrices de la Subgerencia de Gestión Administrativa y la Subgerencia de Tecnologías de la Información y las comunicaciones.
- En cualquiera sea el caso de realizar destrucción o determinación de baja, de algún componente tecnológico, se ejecutará bajo las directrices del Sistema de Gestión Ambiental.
- En el uso de equipos compartidos, como los suministrados por la Agencia, en los espacios físicos de trabajo; cada colaborador deberá vincular las carpetas de almacenamiento de información con la herramienta provista por la entidad, para en ellas, salvaguardar su información.

5.4. Política de las operaciones TIC

La Agencia, en su propósito de asegurar una adecuada gestión de sus operaciones de tecnologías de información y comunicaciones, define:

Política de dispositivos tecnológicos y redundancias

- Se definen y documentan las actividades operacionales especificando las directrices para:
 - Copias de respaldo.
 - Reinicio y recuperación del sistema en caso de falla.
 - Manejo de errores y otras condiciones.
 - Contactos de soporte en caso de dificultades técnicas inesperadas.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 25 de 32

- Realizar seguimiento al uso de recursos y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema, considerando documentar planes de gestión de capacidad para los sistemas críticos de la misionalidad.
- Los servicios y dispositivos tecnológicos deben estar monitoreados en cuanto a: seguimiento de intentos de accesos fallidos y comportamientos anómalos.
- Los Colaboradores no deben instalar ningún tipo de canal de transmisión, módems, ni cambiar la configuración de sus equipos sin la previa aprobación de la Subgerencia de Tecnologías de la Información y las Comunicaciones.
- Los colaboradores no tienen permitido para descargar, utilizar e instalar software externo en los recursos tecnológicos institucionales a menos que sea aprobado e instalado por la Subgerencia de Tecnologías de la Información y las Comunicaciones.
- Implementar controles de detección, prevención y recuperación para proteger los activos de información contra ataques de código malicioso.
- La asignación de dispositivos tecnológicos deberá realizarse a través de registro y entregar con las configuraciones de: dominio, restricción de instalación de software, protección contra malware, des habilitación para borrado, bloqueo remoto, partición del disco duro y demás consideradas en las políticas anteriores.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones propenderá por:
 - Licenciar software de protección contra código malicioso en todos sus servidores, equipos de cómputo y los archivos intercambiados por correo electrónico tanto entrantes como salientes.
 - Establecer mecanismos para mantener actualizados todos los sistemas de procesamiento de información (parches de software y actualizaciones).
- Identificar los servicios tecnológicos más críticos y considerar la implementación de redundancias necesarias para garantizar la continuidad del servicio.

Política de accesos con privilegios.

La Agencia, en su propósito de asegurar una adecuada gestión de los accesos catalogados con privilegios, define:

- La asignación de los accesos con privilegios debe controlarse a través de un proceso.
- Las solicitudes deben ser realizadas y aprobadas por el responsable del activo de información.
- Los accesos con privilegios deben estar limitadas por un rango de tiempo específico.
- Revisar regularmente los accesos con privilegios otorgados.
- Se debe tener en cuenta que los accesos con privilegios son para realizar tareas administrativas dentro de los componentes tecnológicos y en ningún momento para realizar actividades de uso común del usuario.
- Los accesos con privilegios deben estar asociados a un usuario específico, si la cuenta contiene una identificación genérica no se debe hacer uso por varios administradores.

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 26 de 32

Política de acceso a sistemas y aplicaciones

La Agencia, en su propósito de asegurar una adecuada gestión de acceso a sistemas y aplicaciones define:

- El acceso a la información y a las funcionalidades de las aplicaciones se debe restringir, de acuerdo, con los niveles de autorización para cada usuario o grupo de usuarios.
- Los sistemas y aplicaciones deben mantenerse monitoreados y auditados.
- Las credenciales para acceder a los ambientes de pruebas y producción se deben diferenciar de forma que permitan identificar a cada usuario para cada ambiente.
- Se debe controlar el acceso a códigos fuente de programas y elementos asociados (diseños, especificaciones, planes de prueba, resultados), para evitar la introducción de funcionalidades no autorizadas o cambios involuntarios, así mismo, para mantener la confidencialidad de la propiedad intelectual, por tal motivo:
 - Las librerías de programas fuente, no deberían estar contenidas en los ambientes de producción.
 - Establecer un repositorio formal para el almacenamiento.
 - Controlar los cambios para el mantenimiento y copia de las librerías de fuentes de programas.
 - Mantener un registro de auditoría de todos los accesos
- Se debe mantener los siguientes componentes, pero sin limitarse;
 - Validar las credenciales de acceso al completar todos los datos de entrada, en caso de error el sistema no deberá informar cual es el dato correcto o incorrecto.
 - Proteger contra intentos de ingreso mediante ataques de fuerza bruta.
 - Mantener registro de intentos exitosos y fallidos de acceso.
 - No mantener visible la contraseña que se está ingresando.
 - No transmitir contraseñas en texto claro en las redes o medios de comunicación.
 - No dar la opción al usuario de recordar las credenciales
 - Datos de acceso (fecha y hora de inicio de sesión exitoso)
 - Finalizar las sesiones inactivas después de un periodo de inactividad de tiempo, con especial rigurosidad para lugares públicos, externos o dispositivos móviles.
 - Bloqueo de credenciales tras 3 intentos máximos erróneos.
 - Bloqueo de los equipos de cómputo tras 5 minutos de inactividad

Política de gestión de vulnerabilidades

La Agencia, en su propósito de asegurar una adecuada gestión de las vulnerabilidades, define:

- Identificar y definir las estrategias de monitoreo de vulnerabilidades técnicas, que permitan identificar y responder en tiempo real a eventos sospechosos dentro de la red, tales como accesos no autorizados, transferencias anómalas de datos o actividades maliciosas.
- Se debe exigir a los proveedores de servicios tecnológicos la notificación y plan de remediación de vulnerabilidades.
- Realizar pruebas planificadas y documentadas para evaluar vulnerabilidades.
- Validar riesgos del despliegue de actualizaciones de firmware o sistemas operativos antes de su instalación.

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 27 de 32

Como parte del proceso de gestión de vulnerabilidades, la Agencia ATENEA implementará el monitoreo y análisis de amenazas, utilizando herramientas tecnológicas y fuentes de información, que permitan anticipar y mitigar riesgos de seguridad digital.

La Agencia realizará el monitoreo continuo de eventos y alertas emitidas por la plataforma de análisis de comportamiento que se encuentre licenciada e implementada, así como boletines de seguridad, avisos de vulnerabilidades y notificaciones críticas provenientes del COLCERT y otras fuentes oficiales.

El proceso permitirá detectar indicadores de compromiso, identificar tendencias de riesgo, priorizar acciones de tratamiento y comunicar oportunamente recomendaciones a los responsables de la operación tecnológica.

Política de controles criptográficos

La Agencia, en su propósito de asegurar una adecuada gestión de los controles criptográficos, define:

- Implementar controles para proteger activos de información catalogados como reservados, fortaleciendo la confidencialidad, disponibilidad e integridad, mediante el uso de herramientas criptográficas.
- La Agencia no establece una directriz de ciclo de vida de llaves criptográficas, toda vez que, la asignación de la clave para el cifrado de la información en la herramienta, la establece el usuario que genera o administra la información a cifrar, teniendo siempre presente que, en caso de olvidar la clave, la información cifrada no es recuperable.
- Se debe contar con herramientas que permitan el cifrado de información en medios de almacenamiento.

Política de respaldo y restauración de información

La Agencia, en su propósito de asegurar una adecuada gestión en el respaldo y restauración de la información, define:

- Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.
- Los administradores de la plataforma que realiza las copias de seguridad verificarán la correcta ejecución de los procesos de copias de respaldo.
- Los administradores de la plataforma de copias de respaldo de la entidad, mensualmente deben generar tareas de restauración aleatorias de la información de las bases de datos definidas por la Subgerencia de Tecnologías de la Información y las Comunicaciones, quedando registradas en el formato definido para tal fin; estas restauraciones deben ser documentadas, con el fin de garantizar la continuidad de las actividades realizadas en la Agencia, usando las herramientas

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 28 de 32

tecnológicas en caso de presentarse la no disponibilidad de la información almacenada en las bases de datos.

- Es responsabilidad de los colaboradores almacenar la información en los medios dispuestos por la Subgerencia de Tecnologías de la Información y las Comunicaciones, con el fin de generar las copias en las unidades correspondientes.
- Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información.
- Teniendo en cuenta que, la información generada, producida y tratada por el colaborador es producto de la ejecución de actividades institucionales no se entregaran copias de respaldo de la información contenida en correos electrónicos, sistemas de información, estaciones de trabajo y unidades de almacenamiento.
- Mantener custodiadas copias idénticas de sistemas operativos que respondan a eventos de contingencia y disminuyan el impacto en caso de falla irreversible.

Política de seguridad de las comunicaciones

La Agencia, en su propósito de asegurar una adecuada gestión en la seguridad de las comunicaciones, define:

- Implementar mecanismos de control que permitan mantener la disponibilidad de las redes de datos, sistemas de comunicaciones e instalaciones de procesamiento de la Agencia.
- Segmentar los servicios de información, usuarios y sistemas, controlando así el tráfico.
- Los servicios de red deben estar protegidos a través de medios de autenticación.
- Implementar los mecanismos técnicos requeridos para la conexión segura con los servicios de red.
- Disponer de zona DMZ entre la red interna y externa con el objetivo limitar conexiones desde la red interna hacia Internet y conexiones desde internet hacia la red interna.
- Se debe disponer de servicio de internet para visitantes de la entidad.
- Se protegen los diferentes sitios web públicos de la entidad, con certificados de sitio seguro (SSL).

Política de registro y seguimiento de eventos de sistemas de información y comunicaciones

La Agencia, en su propósito de asegurar una adecuada gestión en el registro y seguimiento a los eventos en los sistemas de información y comunicaciones, define:

- Identificar los sistemas críticos de la Agencia y documentar una metodología de revisión y escritura de eventos (Event Logs), que permita identificar las actividades por usuario, excepciones, fallas y eventos de seguridad que no den espacio a la alteración, uso no autorizado o repudio, en caso de presentarse materialización del riesgo y ser utilizados como medio probatorio.
- Mantener los relojes de todos los dispositivos tecnológicos con una única fuente de referencia, esto con el fin de mantener la exactitud del tiempo y permita correlacionar los eventos y logs.
- Los logs de eventos deben conservarse por un período mínimo de seis (6) meses. Para sistemas críticos o que involucren normativas de cumplimiento, la Subgerencia TIC puede definir un tiempo de retención superior al mínimo, de acuerdo con la capacidad tecnológica de

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 29 de 32

almacenamiento disponible. Para los demás logs operativos y de aplicaciones internas, el tiempo de retención también será definido por la Subgerencia TIC, garantizando siempre el cumplimiento del período mínimo establecido. En todos los casos, la eliminación de logs debe realizarse de manera segura, conforme a las mejores prácticas de seguridad de la información.

Política de adquisición, desarrollo y mantenimiento de sistemas de información

La Agencia, en su propósito de asegurar una adecuada gestión en la adquisición, desarrollo y mantenimiento de sistemas de información, define:

- Garantizar que la seguridad es parte integral del ciclo de vida de los sistemas de información.
- Documentar directrices de control de instalación y cambios de los sistemas, para mantener operativas las aplicaciones basadas en estos y que permitan procedimientos de retroceso (RollBack) exitosos.
- Definir y documentar los requisitos de seguridad para la adquisición, desarrollo de los sistemas y mejoras de los existentes.
- Se debe aplicar mecanismos de auditoría a todos los sistemas de información y se evaluará su tiempo de retención teniendo en cuenta la capacidad de almacenamiento institucional, en todo caso, este no debe ser inferior a 3 meses.
- Garantizar la separación de los entornos de desarrollo, pruebas y producción de los sistemas de información.
- Definir y documentar los entornos para el almacenamiento de los códigos y sus versiones.
- Ejecutar revisiones periódicas al licenciamiento de software y desinstalar de los equipos de cómputo, el software que no se encuentre licenciado.
- Establecer y documentar las prácticas seguras, criterios de solicitud y pruebas de calidad y aceptación sobre el desarrollo
- Las solicitudes para uso de software libre serán avaladas previo concepto del oficial de seguridad.
- Las actividades de instalación de software y actualización de los archivos de configuración del sistema solo pueden ser realizadas por personal de la Subgerencia de Tecnologías de la Información y las Comunicaciones, por tanto, está prohibido modificar, alterar o programar cualquier tipo de configuración.
- Asegurar que las bases de datos utilizadas en ambientes de prueba sobre las etapas de desarrollo de soluciones de información no corresponden a información real o la misma debe ser modificada para tales fines.
- El desarrollo de aplicativos o sistemas de información diseñado por terceros debe estar bajo estándares de desarrollo de la Subgerencia de Tecnologías de la Información y las Comunicaciones y alineado a las políticas de seguridad de la información.
- Los datos de prueba no deben contener datos personales o información sensible, de ser necesario este contenido se deben utilizar mecanismos de enmascaramiento o sustitución de datos.
- Se aplicará el concepto de transparencia algorítmica, en los sistemas de información desarrollados por la entidad o sobre los cuales sea propietaria del código fuente. En todo caso ante solicitudes de entrega de información de código fuente, estructura de bases de datos e

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 30 de 32

información contenida en los sistemas de información; primará el derecho a la protección de la información personal, la reglamentación en la materia y la potestad del solicitante.

- En la adquisición, desarrollo o mantenimiento de sistemas de información la Agencia, puede incorporar componentes, motores y algoritmos de inteligencia artificial (IA), bajo parámetros de validación y evaluación del riesgo en el tratamiento y protección de la información personal y el sesgo algorítmico.

Adicionalmente, la Agencia adopta los principios de codificación segura como práctica obligatoria en todo desarrollo de software institucional, con el fin de prevenir vulnerabilidades y proteger la integridad, confidencialidad y disponibilidad de la información procesada.

Para tal fin:

- La codificación deberá ajustarse a los estándares de seguridad reconocidos (ISO/IEC 27002:2022 - Control 8.28, OWASP Top 10, CWE/SANS 25).
- Se debe validar y sanear toda entrada y salida de datos, evitando inyecciones, ejecución de código no autorizado o exposición de información sensible.
- Los mecanismos de autenticación y gestión de sesiones deberán implementarse de manera segura, evitando el almacenamiento de credenciales en texto plano o la reutilización de tokens.
- Los mensajes de error no deben revelar información técnica interna.
- Se debe garantizar el control de versiones y las revisiones de código antes del paso a producción.
- El uso de librerías externas o de código abierto debe provenir de fuentes verificadas y mantenerse actualizado.
- Se ejecutarán revisiones de seguridad sobre el código fuente antes de su liberación.
- La Subgerencia de Tecnologías de la Información y las Comunicaciones podrá establecer una guía institucional de desarrollo seguro, la cual detallará las prácticas, herramientas y controles técnicos que deben aplicarse en las fases de diseño, codificación, pruebas y despliegue de software institucional
- Se deberán mantener inventarios actualizados de dependencias, librerías y módulos externos empleados en los desarrollos, garantizando su actualización periódica y la sustitución inmediata ante alertas de seguridad (CVE)

Política de protección de la información durante auditorías

Cuando se considere realizar auditorías a los sistemas de información y demás componentes de almacenamiento de esta, se debe tener en cuenta lo siguiente:

- La auditoría debe contemplar de manera específica el sistema al cual requiere acceso.
- Los accesos solo serán autorizados en modo lectura.
- Si se requiere un acceso diferente al modo lectura, se otorgará para copias aisladas del sistema con todos los parámetros de seguimiento de seguridad -logs.
- Si las pruebas afectan la disponibilidad estas deben realizarse fuera del horario laboral

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 31 de 32

5.5. Declaración de Aplicabilidad

La Declaración de Aplicabilidad (Statement of Applicability - SOA) es un documento que detalla los controles de seguridad implementados, en proceso o planificados en la Agencia, junto con las justificaciones para aquellos que no serán aplicados.

Para el caso específico de la Agencia Distrital para la Educación Superior, la Ciencia y la Tecnología "Atenea", este tipo de análisis se hace evaluando el cumplimiento de la norma ISO 27002:2022, para cada uno de los controles establecidos en los dominios o temas relacionados con la gestión de la seguridad de la información que este estándar especifica.

6. ANEXOS

No aplica

7. DOCUMENTOS DE REFERENCIA

- Política de Seguridad y Privacidad de la Información
- Política de Tratamiento y Protección de Datos Personales
- Procedimiento de Gestión de Activos de Información
- Procedimiento Gestión de Incidentes de Seguridad de la Información
- Procedimiento Gestión de Vulnerabilidades
- Gestión de Acceso a Servicios Tecnológicos

8. RELACIÓN DE FORMATOS

CODIGO	NOMBRE DEL FORMATO
F1_M1_TIC	Acta entrega y devolución de Equipos

9. CONTROL DE CAMBIOS

Fecha	Versión	Descripción del Cambio
09/12/2025	V4 M1_TIC	En atención a las oportunidades de mejora identificados en las auditorías realizadas, se actualizó el M1_TIC incorporando en la Política de control y gestión de acceso lineamientos sobre segregación de funciones como control de seguridad de la información y la gestión de accesos a plataformas tecnológicas de entidades externas, estableciendo que la responsabilidad de custodia y control de dichas credenciales recae en el Gerente, Subgerente o Jefe de Oficina del área funcional correspondiente; y en la Política de cumplimiento el tratamiento formal de excepciones y desviaciones frente a las directrices del SGSI.
26/05/2025	V3 M1_TIC	Se actualizó el M1_TIC Manual de Políticas de Seguridad de la Información incorporando: (i) proceso de monitoreo y análisis de amenazas dentro de la Política de gestión de vulnerabilidades, formalizando el uso de herramientas como Darktrace y boletines del COLCERT, (ii) la incorporación del formato Acta de Entrega y Devolución

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA

	Manual de Políticas de Seguridad de la Información	CÓDIGO: M1_TIC
		VERSIÓN: 5
	Gestión de Tecnologías de la Información y las Comunicaciones	FECHA DE APROBACION: 30/07/2026
		Página: 32 de 32

		de Equipos en la Política de gestión de activos de información y en la Relación de Formatos para garantizar la trazabilidad del ciclo de vida de los bienes tecnológicos asignados, y (iii) el tratamiento de excepciones y desviaciones frente al cumplimiento de las directrices del SGSI dentro de la Política de cumplimiento.(iv) Se incluye la responsabilidad del propietario del activo de información en la autorización del suministro de accesos a los sistemas bajo su custodia, dentro de la Política de control y gestión de acceso
16/01/2023	2 GTI-MA-02	Actualización del formato y código del documento y de la política de trabajo en casa, junto con la revisión y ajuste de definiciones. Alineación con el Procedimiento de Elaboración, Modificación o Anulación de Documentos y Control de Documentos. Incorporación de normatividad asociada.
07/12/2022	1 GTI-MA-02	Modificación de pie de página según manual de identidad de atenea y asignación cuadro control de cambios

VALIDACIÓN	NOMBRE	CARGO	FECHA
Elaboró	María Alejandra Suarez	Contratista – Subgerencia e Tecnologías de Información y las Comunicaciones	15/07/2026
Revisó	Juan Pablo Ceballos	Contratista – Subgerencia e Tecnologías de la Información y las Comunicaciones	15/07/2026
Aprobó	Carlos Andrés Ballesteros	Subgerente de Tecnologías de la Información y las Comunicaciones	30/07/2026

NOMBRE Y FIRMA DEL LÍDER DE PROCESO

Piensa en el medio ambiente, antes de imprimir este documento.

Cualquier copia impresa de este documento se considera como COPIA NO CONTROLADA