Asociación Colombiana de Ciudades Capitales	**Tipo de documento:** Política	**VERSIÓN 03**
	Macroproceso: Apoyo	**Vigente a partir de:** 25/11/2025
	Proceso: Gestión Tecnológica	
	Título: Política de Seguridad de la Información	**Código:** MA-GT-PLT-01

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA ASOCIACIÓN COLOMBIANA DE CIUDADES CAPITALES - ASOCAPITALES

Proceso: Gestión Tecnológica

Bogotá D.C

Asociación Colombiana de Ciudades Capitales	**Tipo de documento:** Política	**VERSIÓN 03**
	Macroproceso: Apoyo	**Vigente a partir de:** 25/11/2025
	Proceso: Gestión Tecnológica	
	Título: Política de Seguridad de la Información	**Código:** MA-GT-PLT-01

Tabla de Contenido

Asociación Colombiana de Ciudades Capitales	**Tipo de documento:** Política	**VERSIÓN 03**
	Macroproceso: Apoyo	**Vigente a partir de:** 25/11/2025
	Proceso: Gestión Tecnológica	
	Título: Política de Seguridad de la Información	**Código:** MA-GT-PLT-01

1. OBJETIVO

Proteger, conservar y asegurar la información de la Asociación Colombiana de Ciudades Capitales - Asocapitales, y las herramientas tecnológicas utilizadas para su generación, procesamiento y disposición, con el fin de preservar la confidencialidad, integridad y disponibilidad frente amenazas internas o externas, deliberadas o accidentales.

2. ALCANCE

Esta política define los criterios y comportamientos que deben cumplir todos los empleados de la Asociación de planta, contratistas y terceros, con el objetivo de preservar la seguridad de la información.

3. DEFINICIONES

Activos de información: Bases de datos, documentación física y digital, software, hardware, equipos de comunicación, servicios informáticos y de comunicaciones, infraestructura (iluminación, energía, aire acondicionado, etc.) y las personas (son quienes generan, transmiten y destruyen información).

Amenaza: Una causa potencial de un incidente no deseado, el cual puede resultar en daño a un sistema u organización.

Análisis del riesgo: Proceso para comprender la naturaleza del riesgo y así mismo, determinar el nivel del mismo.

Comunicación del riesgo: Comunicar o intercambiar la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Se refiere a la capacidad de acceder y utilizar los recursos de información cuando sea necesario sin interferencias ni interrupciones no autorizadas.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una amenaza con relación a la probabilidad de ocurrencia.

Identificación del riesgo: Proceso para encontrar, enumerar y caracterizar los elementos del riesgo.

Impacto: Cambio adverso en el nivel de los objetivos del negocio logrado.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Probabilidad: Frecuencia o factibilidad de ocurrencia del riesgo.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Tratamiento del riesgo: Selección e implementación de las opciones o acciones apropiadas para ocuparse del riesgo.

Valor del impacto: Está determinado por el responsable del activo de información, quién provee el grado de afectación por incidentes o materialización de riesgos de los activos de información que tenga a cargo.

Vulnerabilidad: La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

Phishing: Los ataques de phishing son correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos diseñados para manipular personas para que descarguen malware.

Malware: El malware, abreviatura de "software malicioso", es cualquier código de software o programa informático escrito de manera intencionada para dañar un sistema informático o a sus usuarios.

4. NORMATIVIDAD

El incumplimiento de las políticas y procedimientos de seguridad, para los empleados de planta y/o contratistas constituye falta disciplinaria conforme a lo señalado al artículo 4 en el numeral 4 del artículo 4 de la Ley 1581 de 2012.

Artículo 4. Definiciones. Principios para el Tratamiento de Datos Personales.

En el desarrollo, interpretación y aplicación de la presente ley, se aplicarán, de manera armónica e integral, los siguientes principios:

Principio de seguridad: La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma.

5. INTRODUCCIÓN

La Política de Seguridad de la Información es la declaración general que representa la posición de la administración de la Asociación Colombiana de Ciudades Capitales Asocapitales con respecto a la protección de los activos de información (los empleados de

planta y/o contratistas del a Asociación, la información, los procesos, las tecnologías de información incluido el hardware y el software).

La Asociación debe contar con plataformas apropiadas protegiendo los mecanismos de tratamiento, almacenamiento y comunicación donde están contenidos y soportados sus servicios de consulta, registro, validación y realización de trámites del sistema de Seguridad, contando con personal competente y comprometido con una cultura de seguridad reflejada en la aceptación y aplicación de las directrices establecidas.

Con la implementación de políticas en seguridad de la información, la Asociación busca dar cumplimiento a disposiciones legales y regulatorias emitidas por los diferentes organismos estatales y salvaguardar la información de la Asociación.

Las políticas del sistema de gestión de seguridad de la información se definen según su orden de importancia en:

Primer Nivel: Corresponde a la Política de Seguridad de la Información, la cual es una directriz global que establece qué y por qué se quiere proteger. Su definición y actualización está alineada con la planeación estratégica de la organización.

Segundo Nivel: Corresponde a la Política General de Seguridad de la Información, la cual establece las responsabilidades generales aplicables a toda la Asociación en lo que respecta al uso adecuado de los activos para la gestión de la información

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Nuestra política de seguridad de la información es la directriz global que establece los objetivos de protección, garantizando la disponibilidad, integridad y confidencialidad de los activos y sistemas informáticos de la Asociación. Define los procedimientos necesarios para proteger estos activos y sistemas. La definición y actualización de esta política se orienta hacia los procesos clave de nuestra organización, abarcando tanto las actividades misionales como las de apoyo, estratégicas y de evaluación.

Los principales objetivos de esta política son:

- Contar con plataformas apropiadas que protejan los mecanismos de tratamiento, almacenamiento y comunicación donde están contenidos y soportados los servicios de consulta, registro, validación y realización de procesos y procedimientos de la Asociación Colombiana de Ciudades Capitales Asocapitales.
- Educar al personal para lograr colaboradores competentes y comprometidos con una cultura de seguridad de la información reflejada en la aceptación y aplicación de las directrices de seguridad.

7. POLÍTICA GENERAL

Nuestra política de seguridad se basa en tres principios fundamentales: Disponibilidad, integridad y confidencialidad de la información. Nos comprometemos a garantizar que nuestros sistemas y recursos estén disponibles en todo momento cuando sean necesarios, que la información se mantenga completa y sin alteraciones no autorizadas, y que se proteja contra cualquier acceso no autorizado que pueda comprometer su confidencialidad. Mediante medidas de control y monitoreo continuo, nos esforzamos por salvaguardar la información sensible y crítica de nuestra organización, generando confianza tanto en nuestros empleados de planta, contratistas y en las partes interesadas.

7.1. Política seguridad física y del entorno

La Asociación de Ciudades Capitales Asocapitales, debe implementar medidas a través de la Dirección General para proteger el perímetro de seguridad de sus instalaciones físicas. Estas medidas tienen como objetivo controlar el acceso y la permanencia del personal tanto en la oficina como en áreas restringidas.

7.2. Política seguridad de las operaciones

La Dirección General, con el respaldo de su equipo de sistemas, debe llevar a cabo copias de seguridad de los sistemas de información utilizados en la Asociación. Este proceso garantiza la disponibilidad y la integridad de los datos, asegurando que estén disponibles cuando se necesiten y que permanezcan completos y sin alteraciones.

7.3. Política seguridad de las comunicaciones

La Dirección General establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y los servicios tecnológicos que dependan de ellas, asegurando su funcionamiento óptimo en todo momento.

Asimismo, el proceso de comunicaciones y relacionamiento institucional se encargará de actualizar de manera regular la información en los medios de comunicación de la Asociación los cuales son el sitio web y redes sociales. Esto garantizará una comunicación efectiva y actualizada con los miembros y el público en general, fortaleciendo la imagen y la transparencia de la Asociación.

7.4. Política seguridad digital

Todos los empleados de planta y contratistas que utilicen los recursos tecnológicos de la asociación, tienen la responsabilidad de adherirse a las políticas establecidas para su uso aceptable. Esto implica no solo respetar las directrices sobre acceso y uso de la tecnología, sino también proteger la confidencialidad y la integridad de los datos de la organización. Es esencial comprender que cualquier violación a estas políticas no solo puede poner en peligro la continuidad de la operación, sino también afectar la reputación y la seguridad de la Asociación. Por lo tanto, es responsabilidad de cada persona garantizar un uso adecuado y seguro de los recursos tecnológicos en todo momento. Para ello, deben acatar las siguientes disposiciones:

1. **Uso del correo electrónico**: El correo electrónico institucional es una herramienta fundamental para respaldar la ejecución de las funciones y obligaciones de todos los empleados, tanto los de planta como los contratistas dentro de la Asociación. Su uso se facilitará siguiendo los términos establecidos a continuación:

   1.1. El único servicio de correo electrónico autorizado para el manejo o transmisión de la información de la Asociación es el entregado por la Dirección General, el cual está asociado al dominio **@asocapitales.co**

   1.2. El servicio de correo electrónico debe ser empleado únicamente para enviar o recibir mensajes de carácter institucional, en consecuencia, no puede ser utilizado con fines personales, comerciales, económicos o cualquier otro ajeno a los propósitos de la Asociación.

   1.3. Cualquier mensaje considerado SPAM, cadena, phishing, o que provenga de un remitente o contenga contenido sospechoso, debe ser reportado de manera inmediata al responsable del rol de sistemas de la Asociación. Esta medida es crucial, ya que dichos mensajes podrían contener virus u otros tipos de malware que representen una amenaza para la seguridad de nuestros sistemas y datos.

   1.4. La cuenta de correo electrónico no debe ser proporcionada en páginas o sitios web publicitarios, de comercio electrónico, deportivos, casinos o cualquier otro tipo de plataforma que no esté relacionada con los objetivos y propósitos de la Asociación.

   1.5. Está totalmente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos y que atenten contra la integridad moral de las personas o instituciones.

2. **Uso del internet:** El acceso a Internet se proporciona con el fin de facilitar la realización de actividades laborales relacionadas con las responsabilidades y funciones asignadas a los empleados dentro de la Asociación. Es importante destacar que el acceso a Internet

debe utilizarse de manera responsable y ética, evitando cualquier actividad que pueda comprometer la seguridad de la red. Para ello, se deben acatar las siguientes indicaciones:

2.1. Se prohíbe expresamente enviar, descargar y visualizar páginas web con contenido insultante, ofensivo, injurioso, obsceno o que atente contra la integridad moral de las personas o instituciones.

2.2. Se prohíbe expresamente enviar y descargar cualquier tipo de Software o archivo de fuentes externas y de procedencia desconocida, con el fin de salvaguardar la integridad de los sistemas informáticos y proteger la seguridad de la información de la Asociación.

2.3. Abstenerse de propagar intencionalmente virus o cualquier tipo de código malicioso que puedan comprometer la seguridad y el funcionamiento de los sistemas informáticos de la Asociación.

La Asociación se reserva el derecho de monitorear tanto los accesos como el uso del servicio de Internet con el fin de garantizar el cumplimiento de las políticas de seguridad establecidas y proteger la integridad de los sistemas de la organización. Además, se podrán implementar restricciones para limitar el acceso a determinadas páginas de Internet que representen un riesgo potencial para la seguridad informática o que estén en conflicto con los objetivos y valores de la asociación.

3. **Uso de los recursos tecnológicos:** Los recursos tecnológicos de la Asociación son esenciales para respaldar las labores, responsabilidades y obligaciones tanto de los empleados de planta como de los contratistas. En este sentido, su uso se encuentra sujeto a rigurosas directrices en materia de seguridad de la información:

3.1. Los equipos informáticos proporcionados por la Asociación serán utilizados exclusivamente por el empleado de planta o contratista al que hayan sido asignados, y bajo su completa responsabilidad. Estos equipos deberán ser

empleados únicamente para el cumplimiento de las funciones del cargo o las obligaciones asignadas, por lo tanto, no podrán ser utilizados para fines personales.

3.2. Se permite exclusivamente el uso de software licenciado por la Asociación, así como aquel que esté autorizado por la Dirección General, incluso en los casos en los que no se requiera una licencia. El uso de software ilegal o no autorizado está terminantemente prohibido.

3.3. Todos los empleados de la Asociación están obligados a realizar y mantener actualizadas sus copias de respaldo y guardando la información en la herramienta proporcionada por la Asociación.

3.4. Solo las personas designadas por la Dirección General son las únicas autorizadas para realizar modificaciones o actualizaciones en los recursos tecnológicos, incluyendo acciones como destapar, agregar, desconectar, retirar, revisar o reparar sus componentes asi como su mantenimiento.

3.5. La Dirección General, a través de su rol de sistemas, es la única autorizada para trasladar elementos y recursos tecnológicos de un puesto a otro, con el fin de mantener un control del inventario y garantizar la correcta asignación y utilización de los recursos de la Asociación.

3.6. La pérdida o daño de elementos o recursos tecnológicos deberá ser informada inmediatamente a la Dirección General.

3.7. Cualquier pérdida de información debe ser reportada de inmediato a la Dirección General, proporcionando un detalle completo de la situación para facilitar su pronta atención y resolución.

4. **Uso de los sistemas o herramientas de información:** Todos los empleados de planta y contratistas de la Asociación tienen la responsabilidad de proteger la información a la

que acceden y procesan, así como de prevenir su pérdida, alteración, destrucción y uso indebido. Con este fin, se establecen los siguientes lineamientos:

4.1. Las credenciales de acceso a los recursos informáticos (nombre de usuario y contraseña) son estrictamente personales e intransferibles. No deben ser reveladas a terceros ni utilizar las credenciales de otras personas.

4.2. Todo empleado de la Asociación sea de planta o contratista es responsable del cambio periódico de sus contraseñas de acceso a los sistemas de información o recursos informáticos, dichas contraseñas deben tener una longitud mínima de 8 caracteres incluyendo combinación de letras (mayúsculas y minúsculas), números y caracteres especiales como @, #, $, %, etc. Esto aumenta la complejidad de la contraseña.

4.3. En caso de ausencia de un empleado de la Asociación, el acceso a su estación de trabajo deberá ser solicitado por su jefe inmediato a la Dirección General para su validación y autorización correspondiente.

4.4. En caso de que un empleado de la Asociación cese de sus funciones o finalice la ejecución de su contrato, todos los privilegios de acceso a los recursos informáticos otorgados serán suspendidos de manera inmediata.

4.5. Se recomienda que todos los sistemas de información y recursos informáticos que admiten la autenticación de dos factores tengan esta función activada de manera obligatoria. Esto asegura un nivel extra de seguridad al acceder a estos sistemas, al requerir la verificación de la identidad a través de múltiples métodos, fortaleciendo así la protección de la información.

8. CUMPLIMIENTO

Estas políticas a todo nivel, son obligatorias, por lo tanto, deben ser cumplidas por los empleados, contratistas y terceros que interactúen con los Sistemas de Información y demás recursos informáticos de la Asociación.

Se define el incumplimiento como toda conducta de cualquier colaborador de la Asociación que no respete las políticas. Entre los ejemplos de incumplimiento se incluyen, sin limitarse a ellos:

- Los empleados de planta y/o contratistas que sean negligentes en la aplicación de medidas de seguridad y control dentro de la organización.
- Una acción o inacción por parte de un empleado de planta y/o contratista que contribuye a la violación de las normas orientadas al buen uso de la información.
- Un empleado de planta y/o contratistas que no resuelve o remite inmediatamente a una autoridad superior los problemas de seguridad de la información que sean detectados.
- Los empleados de planta y/o contratistas que no tomen las medidas correspondientes ante una queja o un incidente de seguridad.

Todos los empleados de planta y/o contratistas de la Asociación son responsables de implementar las Políticas y procedimientos de seguridad que se contemplan o son referenciados en este documento y sus complementarios.

Los empleados de planta y/o contratistas tienen establecidas dentro de su contrato laboral cláusulas de confidencialidad de la información.

Los contratistas, consultores y terceros que estén involucrados en incidentes de incumplimiento pueden verse inmersos en el inicio de un procedimiento sancionatorio contractual de acuerdo con las condiciones que en el contrato se han establecido.

9. NOTIFICACIONES DE INCIDENTES

Toda violación de estas políticas se deberá notificar inmediatamente a través de la cuenta o correo sistemas@asocapitales.co

Se busca asegurar que todos comprendan y respeten las políticas con el fin de reducir al mínimo el riesgo, protegiendo a todas las personas, así como a la Asociación.

Se deberán notificar situaciones tales como:

- Personas ajenas a la Asociación en centros de cómputo sin la debía autorización.
- Correos con virus.

- Reinicio de los equipos de cómputo o enrutadores.
- Mala utilización de recursos.
- Uso ilegal del software.
- Mal uso de información corporativa.
- Alteración de información.

Y todas las que se describen en la política de seguridad de la información.

Las políticas de seguridad de la información de la Asociación fueron diseñadas para ajustarse o exceder, sin contravenir, las medidas de protección establecidas en las leyes y regulaciones, por lo tanto si algún empleado de planta y/o contratista de la Asociación considera que alguna política de seguridad de información está en conflicto con las leyes y regulaciones existentes, tiene la responsabilidad de reportar en forma inmediata dicha situación a través de la cuenta sistemas@asocapitales.co donde será atendida.

10. ROLES

Usuario:

Todo empleado de planta, contratista, ente regulador, socios de negocios, y terceros entre otros que estén involucrados con información de la Asociación Colombiana de Ciudades Capitales Asocapitales.

Líder de Seguridad:

El líder de seguridad de la Asociación Colombiana de Ciudades Capitales Asocapitales será el profesional de apoyo rol sistemas.

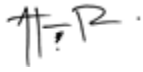
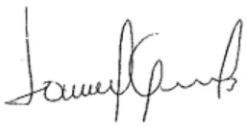
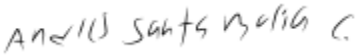
11. RESPONSABLE DEL DOCUMENTO

Gestión Tecnológica o quien haga sus veces, de la Asociación Colombiana de Ciudades Capitales Asocapitales.

12. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE LOS CAMBIOS	FECHA
01	Documento Nuevo	01/11/2023
02	Ajuste y actualización en la política de seguridad general	09/05/2024
03	Cambio de forma en documento	25/11/2025

13. FIRMAS

		
Elaboró: Aldemar Ruiz Palacios	**Revisó:** Lady Jasmín Gélvez	**Aprobó:** Andrés Santamaría Garrido
Cargo: Profesional de apoyo	**Cargo:** Directora Administrativa, Financiera y Gestión Humana	**Cargo:** Director General