


	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	

## Política de Seguridad y Privacidad de la Información



Capital

Bogotá D.C., septiembre de 2020

	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	

## TABLA DE CONTENIDO

1.	Introducción.....	3
2.	Objetivo.....	4
2.1	Objetivos específicos.....	4
3.	Alcance y aplicabilidad .....	4
4.	Definiciones .....	5
5.	Marco Legal .....	7
6.	Política de Seguridad y Privacidad de la Información.....	10
7.	Responsabilidades .....	12
7.1	Compromiso de la Gerencia .....	12
7.2	Compromiso Comité Institucional de Gestión y Desempeño de Capital .....	12
7.3	Compromiso Oficina de Control Interno .....	13
7.4	Compromiso Área de Sistemas .....	13
7.5	Responsabilidades de los propietarios de la información .....	14
7.6	Responsabilidades de los funcionarios, contratistas y terceros usuarios de la información .....	15

	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	



## 1. Introducción

Capital ha querido definir las responsabilidades y conductas que se deben mantener para conformar un ambiente seguro en la Entidad, las cuales se establecen a través de su Política de Seguridad y Privacidad de la Información, Manual de Políticas Complementarias de Seguridad de la Información y Manual del Sistema de Gestión de Seguridad de la Información, para que soporten el manejo de la información y se constituyan como parte fundamental de Sistema de Gestión de Seguridad de la Información de Capital convirtiéndose así en la base para la implementación de controles, procedimientos y estándares definidos.<sup>1</sup>

La Gerencia de Capital, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información-SGSI buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y la ciudadanía, todo enmarcado en el estricto cumplimiento de las Leyes y en concordancia con la misión y visión de la Entidad.

Para Capital, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad, disponibilidad y privacidad de esta, acorde con las necesidades de los diferentes grupos de valor que se identifiquen en la Entidad.

<sup>1</sup><https://www.icetex.gov.co/dnnpro5/Portals/0/Documentos/La%20Institucion/manuales/Manualseguridadinformacion.pdf>  
Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	 <small>ALCALDÍA MAYOR DE BOGOTÁ D.C.</small>
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	

## 2 Objetivo

Asegurar y administrar la información y los recursos tecnológicos para que sean accedidos solo por aquellas personas que tienen la necesidad legítima para el cumplimiento de sus funciones (confidencialidad), que este y sea protegida contra las alteraciones no planeadas y realizadas con o sin intención (integridad) y que esté disponible cuando esta sea requerida (disponibilidad), adicionalmente debe disminuir con el impacto de riesgos, amenazas y vulnerabilidades y reducir las ocurrencias de cualquier ataque a esta.



### 2.1 Objetivos específicos

- Consolidar la seguridad de la información como una línea estratégica en Capital definiendo, comunicando y generando la cultura de buenas prácticas para el acceso, uso y manejo de la información y recursos tecnológicos, por parte de todos los funcionarios, contratistas y terceros relacionados con Capital.
- Proteger los activos de información, y salvaguardar la plataforma tecnológica en aras de proteger la imagen, los intereses y el buen nombre de la Entidad, gestionando las amenazas y vulnerabilidades en la plataforma tecnológica para reducir los riesgos asociados con la seguridad de la información y dar cumplimiento a los lineamientos establecidos en la Política de Gobierno Digital y Seguridad Digital respecto a la Seguridad de la Información.

## 3 Alcance y aplicabilidad

La Política de Seguridad y Privacidad de la Información es aplicable para todas las funciones administrativas y de control, esta debe ser cumplida por cada uno de los funcionarios, proveedores, socios de negocio y terceros que laboren o presten servicios para Capital, con el fin de dar cumplimiento adecuado a sus funciones y mantener un nivel de protección a la información.

La política pretende afianzar la satisfacción de las partes interesadas priorizando la confidencialidad, integridad, disponibilidad y privacidad de la información, bajo un enfoque de mejora continua y autocontrol en los procesos y en la prestación de los servicios.

	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	

#### 4 Definiciones

**Acceso a la Información:** Conjunto de técnicas para buscar, categorizar, modificar y acceder a la información que se encuentra en un sistema de bases de datos, bibliotecas, archivos e Internet.

**Acción Correctiva:** Medida orientada a eliminar la causa de cualquier amenaza, evento, riesgo o vulnerabilidad asociada a la seguridad de la información.

**Acción Preventiva:** Medida orientada a prevenir cualquier amenaza, evento, riesgo o vulnerabilidad asociada a la seguridad de la información.

**Activo de Información:** Datos o información que tienen un valor para una Entidad.

**Amenaza:** Circunstancia, suceso o persona con el potencial para dañar un sistema mediante la destrucción, divulgación, modificación de datos o negación de servicios.

**Análisis de Riesgo:** Método cualitativo o cuantitativo para la evaluación del impacto de riesgo en la toma de decisiones.

**Aplicaciones:** Es todo software que se utiliza para la gestión o manejo de la información.

**Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona en cualquiera de los sistemas de información de la entidad.

**Autorización:** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

**BackUp:** Parámetros que determinan que equipo o que información debe incluirse en una copia de respaldo dentro de la entidad.



**Confidencialidad:** Mantener la información oculta a individuos, entidades o procesos no autorizados.

**Control:** Procedimiento, procesos, políticas que permiten mantener el riesgo de la seguridad de la información por debajo del riesgo presente.

**Denegación de Servicio:** Es una acción iniciada por un ataque a un sistema objetivo, que provoca la denegación a los usuarios legítimos forzando su cierre o conllevando a una inoperatividad.

**Disponibilidad:** Mantener la información accesible a quien la necesita en el momento que la necesite.

**Dispositivo:** Es un ordenador que se puede utilizar para acceder a los servicios de red, computador Tablet, Smartphone.

	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	

**Evento:** Suceso identificado en un sistema, estado que deja al descubierto una brecha de seguridad.

**Ingeniería Social:** Método utilizado para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la divulgación de información.

**Integridad:** Prevenir la modificación no autorizada de la información.

Política: Medidas necesarias para garantizar la seguridad de las tecnologías de la información.

**Riesgo:** Posibilidad de que ocurra un contra tiempo.

Seguridad de la Información: Según ISO 27002 es la preservación de la confidencialidad, integridad y disponibilidad de la información.

**Seguridad Informática:** Encargada de diseñar las normas, procedimientos, métodos y técnicas destinadas a conseguir un sistema de gestión de seguridad de la información seguro y confiable.

**Seguridad Física:** Límites mínimos que se deben cumplir en cuanto a los perímetros de seguridad, de forma que se puedan establecer controles.



**Seguridad Lógica:** Integrar mecanismos y procedimientos que permitan monitorear el acceso a los activos de la información.

**SGSI Sistema de Gestión de Seguridad de la Información:** Es un mecanismo que permite preservar la confidencialidad, integridad y disponibilidad de la información.

**Usuario:** Cualquier persona que haga uso de los servicios de red proporcionados por la entidad tales como equipos de cómputo, sistemas de información y redes.

**Virus:** Es un tipo de software o aplicación que tiene como objetivo alterar el normal funcionamiento de los equipos tecnológicos, sin permiso o conocimiento de los usuarios.

Vulnerabilidad: Condición de un sistema que lo hace susceptible a una amenaza.



	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	

## 5 Marco Legal

Capital acoge las normas vigentes de seguridad de información, protección de datos personales y directrices de ciberseguridad a nivel nacional y territorial aplicando las prácticas y estándares recomendados para su cumplimiento.

TIPO	No.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
CONSTITUCIÓN POLÍTICA DE COLOMBIA	1991	1991	Artículo 15. "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. Disponible en Línea: <a href="http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15">http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15</a>	X		
Ley Estatutaria	1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República. Disponible en Línea: <a href="http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981">http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981</a> .	X		
Ley	23	1982	Sobre Derechos de Autor. Congreso de la República. Disponible en Línea <a href="http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431">http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431</a>	X		
Ley	527	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. Disponible en Línea: <a href="http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276">http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276</a> .	X		
Ley	1266	2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Disponible en Línea: <a href="http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488">http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488</a>	X		
Ley	1273	2009	Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y	X		



Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	

TIPO	No.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
			las comunicaciones, entre otras disposiciones". Disponible en Línea: <a href="http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492">http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492</a>			
Ley	1474	2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. Disponible en Línea: <a href="http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43292">http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43292</a> .	X		
Ley	1712	2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones. Disponible en Línea: <a href="http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882">http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882</a> .	X		
Decreto	235, Art.1-4	2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones pública	X		
Decreto	4632	2011	Por medio del cual se reglamenta parcialmente la Ley 1474 de 2011 en lo que se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones. Disponible en Línea: <a href="http://wsp.presidencia.gov.co/Normativa/Decretos/2011/Documents/Diciembre/09/de463209122011.pdf">http://wsp.presidencia.gov.co/Normativa/Decretos/2011/Documents/Diciembre/09/de463209122011.pdf</a>	X		
Decreto	2609	2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado". Disponible en Línea: <a href="http://www.mintic.gov.co/portal/604/articles3528_documento.pdf">http://www.mintic.gov.co/portal/604/articles3528_documento.pdf</a> .	X		
Decreto	1377	2013	Tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. Disponible en Línea: <a href="http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5364">http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5364</a> .	X		
Decreto	886	2014	Reglamentar la información mínima que debe contener el Registro Nacional de Bases de Datos, creado por la Ley 1581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los responsables del tratamiento.	X		



Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.



	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	

TIPO	No.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
			Disponible en línea: <a href="http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=57338">http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=57338</a> .			
Decreto	103	2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. Disponible en Línea: <a href="http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60556">http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60556</a> .	X		
Decreto	1494	2015	Por el cual se corrigen yerros en la Ley 1712 de 2014. Disponible en Línea: <a href="http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Decretos2015/DECRETO%201494%20DEL%2013%20DE%20JULIO%20DE%202015.pdf">http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Decretos2015/DECRETO%201494%20DEL%2013%20DE%20JULIO%20DE%202015.pdf</a> .	X		
Decreto	415	2016	Por el cual se adiciona el Decreto único Reglamentario del sector de la Función Pública, decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de información y las comunicaciones.	X		
Decreto	1499	2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.	X		
Decreto	1008	2018	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. Disponible en Línea: <a href="https://www.mintic.gov.co/portal/604/article-s-74903_documento.pdf">https://www.mintic.gov.co/portal/604/article-s-74903_documento.pdf</a> . Expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones	X		
Directiva	22	2011	Estandarización de la información de identificación, caracterización, ubicación y contacto de los ciudadanos y ciudadanas que capturan las entidades del Distrito Capital. Disponible en Línea: <a href="http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=45545">http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=45545</a> . Expedida por el Alcalde Mayor de Bogotá.		X	
Directiva	02	2019	Simplificación de interacción digital los ciudadanos y el estado. Expedida por presidente de la Republica.	X		

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	

TIPO	No.	AÑO	TEMA	ORIGEN		
				Nacional	Distrital	Otras
Resolución	305	2008	Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre. Expedida por: la Comisión Distrital de Sistemas (CDS) de Bogotá.		X	

### Documentos de Referencia

- Norma NTC/ISO27001:2013
- Norma NTC/ISO27002
- Manual de Sistema de Gestión de Seguridad de la Información.
- Declaración de Aplicabilidad SoA Capital.
- Instrumento de Evaluación MSPI.
- Guía Política General MSPI v1.
- Política de Seguridad de la Información Capital



## 6 Política de Seguridad y Privacidad de la Información

La Gerencia de Capital, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y sus ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y la visión de la entidad.

Para Capital, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se define en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones y/o toma de decisiones alrededor del SGSI estarán determinados por las siguientes premisas:

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.



	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	 <small>ALCALDÍA MAYOR DE BOGOTÁ D.C.</small>
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de Capital.
- Garantizar la continuidad del negocio frente a incidentes.
- Capital ha decidido definir, implementar, operar y mejorar de forma continua un SGSI, soportado en lineamientos claros alineados a las necesidades del negocio y a los requerimientos regulatorios.

Se establecen 11 principios de seguridad que soportan el SGSI de Capital:

1. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas, proveedores, socios de negocio o terceros.
2. Capital protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros o como resultado de un servicio interno en outsourcing.
3. Capital protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.
4. Capital protegerá su información de las amenazas originadas por parte del personal de la Entidad.
5. Capital protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
6. Capital controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
7. Capital implementará control de acceso a la información y recursos de red.
8. Capital garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
9. Capital garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
10. Capital garantizará la disponibilidad de sus procesos de un negocio y la continuidad de su operación basada en el impacto que puedan generar los eventos.

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	

11. Capital garantizará el cumplimiento de las obligaciones legales, contractuales y regulatorias establecidas.

La presente política general de seguridad de la información es una definición de las responsabilidades y la conducta aceptada para mantener un ambiente seguro en la entidad, el cual establece las políticas y normas relacionadas con el manejo de la información. Capital ha establecido como fundamentales los siguientes principios que soportan la política de seguridad de la información.

- La confidencialidad de la información del negocio y de terceros para ser mantenida independientemente del medio o formato donde se encuentre.
- La integridad de la información del negocio debe preservarse independientemente de su residencia temporal o permanente y la forma como se transmita.
- La disponibilidad de la información de la Entidad debe estar disponible (valga la redundancia) cuando se requiera.
- La privacidad y reserva de la información de la Entidad debe ser preservada.

Las anteriores definiciones acorde a la norma NTC/ISO:27001.2013

## 7 Responsabilidades



### 7.1 Compromiso de la Gerencia

La Gerencia de Capital aprueba esta Política de Seguridad y Privacidad de la Información como muestra de su compromiso al diseño e implementación del SGSI para que así se garantice la seguridad de la información de la Entidad.

- La revisión y aprobación de la Políticas de Seguridad y Privacidad de la Información y el Manual de Políticas Complementarias de Seguridad de la Información.
- La promoción activa de una cultura de seguridad.
- Divulgar la Política General de la Seguridad de la Información y el Manual de Políticas de Seguridad de la Información.
- Asegurar los recursos económicos necesarios para implementar y mantener el SGSI.
- Velar por el cumplimiento de los lineamientos establecidos en esta Política General de Seguridad de la Información y el Manual de Políticas de Seguridad de la Información.

### 7.2 Compromiso Comité Institucional de Gestión y Desempeño de Capital

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	



- Actualizar y presentar la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.
- Verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.
- La Gerente y/o jefe de área es el responsable de hacer cumplir las normas y políticas de seguridad de la información establecidas por la Gerencia en Capital.

### 7.3 Compromiso Oficina de Control Interno

- Las auditorías y seguimientos a los sistemas de información se realizarán de manera preventiva por la Oficina de Control Interno con el acompañamiento del Área de Sistemas.
- La Oficina de Control Interno debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información de Capital a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.
- La Oficina de Control Interno debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance del Sistema de Gestión de Seguridad de la Información, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.
- La Oficina de Control Interno debe informar a las áreas responsables los hallazgos de las auditorías.

### 7.4 Compromiso Área de Sistemas

- El Área de Sistemas es la responsable de la elaboración y/o modificación y/o actualización y/o eliminación e implementación, monitoreo y seguimiento de la Política de Seguridad y Privacidad de la Información, asegurando así los recursos adecuados y promoviendo una cultura activa de seguridad en la Entidad.
- Establecer, mantener y divulgar las políticas y procedimientos de servicios de tecnología, incluida esta política de seguridad y privacidad de información, el uso de los servicios tecnológicos en toda la entidad de acuerdo a las mejores prácticas y lineamientos de la Gerencias de Capital, directrices del Gobierno Nacional y Distrital.
- El Área de Sistemas lidera la definición de parámetros para el establecimiento de hardware, software y comunicaciones, así como de la arquitectura tecnológica. Sin embargo, la administración de la información en la fase de registro tanto en aplicativos como bases de datos, es responsabilidad de cada área, con el fin de evitar

	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	 ALCALDÍA MAYOR DE BOGOTÁ D.C.
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	

modificación no autorizada o intencional o el uso indebido de los activos de la organización.



- Mantener la custodia de la información que reposa en los diferentes sistemas de información, bases de datos y aplicativos de la Entidad.
- Proporcionar medidas de seguridad físicas, lógicas y procedimentales para la protección de la información digital de la Entidad.
- Aplicar y hacer cumplir la Política de Seguridad y Privacidad de la Información y sus componentes.
- Administrar las reglas y atributos de acceso a los equipos de cómputo, sistemas de información, aplicativos y demás fuentes de información al servicio de Capital.
- Analizar, aplicar y mantener los controles de seguridad implementados para asegurar los datos e información gestionados en la Entidad.
- Habilitar/Deshabilitar el reconocimiento y operación de Dispositivos de Almacenamiento externo de acuerdo con las directrices emitidas de parte de la Gerencia y las diferentes áreas.
- Implementar los mecanismos de controles necesarios y pertinentes para verificar el cumplimiento de la presente política.
- Garantizar la disponibilidad de los servicios y así mismo programar o informar a todos los usuarios cualquier problema o mantenimiento que pueda afectar la normal prestación de estos; así como gestionar su acceso de acuerdo a las solicitudes recibidas de las diferentes Áreas siguiendo el procedimiento establecido.
- Determinar las estrategias para el mejoramiento continuo del servicio tecnológico, la optimización de los recursos tecnológicos, las mejoras en los sistemas de información con miras a un gobierno de tecnologías consolidado.
- Brindar el soporte necesario a los usuarios a través de los canales de mesa de ayuda actualmente implementados en la entidad.

## 7.5 Responsabilidades de los propietarios de la información

Son propietarios de la información cada uno de los directores, así como los jefes de las áreas donde se genera, procesa y mantiene información, en cualquier medio, propia del desarrollo de sus actividades.

- Valorar y clasificar la información que está bajo su administración y/o generación. Autorizar, restringir y delimitar a los demás usuarios de la entidad el acceso a la información de acuerdo a los roles y responsabilidades de los diferentes funcionarios, contratistas o terceros que por sus actividades requieran acceder a consultar, crear o modificar parte o la totalidad de la información.
- El almacenamiento en herramientas de la nube (Cloud) como es el caso de Gsuite, como medio de salvaguarda y protección de la información contenida y gestionada

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	 <small>ALCALDÍA MAYOR DE BOGOTÁ D.C.</small>
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	



a diario por cada uno de los usuarios, es decir el uso adecuado de los recursos de la entidad, aclarando y liberando de responsabilidades al Área de sistemas, por fallas como la pérdida de información del usuario causada por una falla repentina del hardware o software o bien humana.

- Determinar los tiempos de retención de la información en conjunto con el grupo de Gestión Documental y Correspondencia y las áreas que se encarguen de su protección y almacenamiento de acuerdo a las determinaciones y políticas de la entidad como de los entes externos y las normas o leyes vigentes.
- Determinar y evaluar de forma permanente los riesgos asociados a la información, así como los controles implementados para el acceso y gestión de la administración comunicando cualquier anomalía o mejora tanto a los usuarios como a los custodios de esta.
- Acoger e informar los requisitos de esta política a todos los funcionarios, contratistas y terceros en las diferentes dependencias de la entidad.

## **7.6 Responsabilidades de los funcionarios, contratistas y terceros usuarios de la información**

- Los funcionarios que realicen labores para Capital tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.
- Los usuarios de los sistemas y aplicativos deberán reportar al Área de Sistemas las inconsistencias, anomalías y nuevos requerimientos.
- Utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados en el Manual de Funciones, Código Disciplinario Único – Ley 734 de 2002 o Contrato.
- Manejar la Información de la entidad y rendir cuentas por el uso y protección de tal información, mientras que esté bajo su custodia. Esta puede ser física o electrónica e igualmente almacenada en cualquier medio.
- Proteger la información a la cual acceden y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Evitar la divulgación no autorizada o el uso indebido de la información.
- Cumplir con todos los controles establecidos por los propietarios de la información y los custodios de esta.
- Informar a sus superiores sobre la violación de estas políticas o si conocen de alguna falta a alguna de ellas.
- Proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.
- Reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

Si este documento se encuentra impreso no se garantiza su vigencia, por lo tanto, es copia No Controlada. La versión vigente reposará en la intranet institucional. Verificar su vigencia en el listado maestro de documentos.

	<b>POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN</b>	<b>CODIGO: AGRI-SI-PO-002</b>	
		<b>VERSIÓN: 05</b>	
		<b>FECHA: APROBADO EN SESIÓN CIGD DEL 24/09/2020</b>	
		<b>RESPONSABLE: SISTEMAS</b>	

- Proteger los equipos de cómputo, de comunicaciones y demás dispositivos tecnológicos designados para el desarrollo de sus funciones y obligaciones.
- Usar software autorizado que haya sido adquirido legalmente por la entidad. No está permitido la instalación ni uso de software diferente al Institucional sin el consentimiento de sus superiores y visto bueno de Sistemas.
- Divulgar, aplicar y el cumplir con la presente Política.
- Aceptar y reconocer que en cualquier momento y sin previo aviso, la Gerencia de la entidad puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos y archivos de los correos electrónicos institucionales, sitios web institucionales y redes sociales propiedad de la entidad, al igual que las unidades de red institucionales, computadoras, servidores u otros medios de almacenamiento propios de la entidad. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.
- Proteger y resguardar su información personal que no esté relacionada con sus funciones en la entidad. Capital no es responsable por la pérdida de información, desfalco o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito, etc.