# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

## Contenido

## 1. INTRODUCCION

La adopción de políticas, normas y procedimientos de seguridad de la información obedece a una decisión estratégica de la Secretaria de Tecnologías de Información de la Gobernación Del Valle Del Cauca, con el fin de definir el SGSI, a través del análisis, diseño e implementación de los objetivos, requisitos de seguridad, procesos, procedimientos, planes, políticas, controles con formatos, el tamaño, la tecnología y estructura de la misma.

En la actualidad la información para la Gobernación del Valle del Cauca, se reconoce como un activo supremamente valioso y en la medida que los sistemas de información apoyan cada vez más los procesos misionales y de apoyo, y en razón de lo anterior se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de la misma.

Se ha definido que las políticas de seguridad de la información deben identificar responsabilidades y establecer los objetivos para una protección apropiada de los activos de información de la entidad, contando además con manuales para usuarios finales. La implementación de las políticas busca reducir el riesgo de que en forma accidental o intencional se divulgue, modifique, destruya o use en forma indebida la información de la entidad.

Al mismo tiempo las políticas habilitan a la secretaria de las TIC y sus programas como responsables de dictar la normatividad de la gestión de seguridad de la información, y para orientar y mejorar la administración de seguridad de los activos de información. Finalmente también contempla el proveer las bases para el seguimiento y monitoreo en la entidad.

La Gobernación Del Valle Del Cauca, desde sus directivas pretende mantener un esquema de seguridad que permita asegurar constantemente la confidencialidad, integridad y disponibilidad de la información, siendo ésta, su activo más valioso. Para ello adopta, establece, implementa, opera, verifica y mejora un Sistema de Gestión de Seguridad de la Información (SGSI).

Con base en lo anterior se debe integrar a todo el personal de la entidad para que, conozca, participe y cumpla los lineamientos, políticas, procedimientos y demás directrices estipuladas en el SGSI, tal como lo establece el plan de uso y apropiación

de las TIC el cual interactúa de manera articulada con la dimensión Gestión del Conocimiento y la Innovación asociada a la Política Gestión estrategia del talento humano de que trata el Modelo Integrado de Planeación y Gestión (MIPG). Para este efecto se elaborara un documento que contemple el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI.

## 2. OBJETIVOS

### 2.1. Objetivo General

Establecer los lineamientos que permitan proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de la GOBERNACIÓN DEL VALLE DEL CAUCA, teniendo en cuenta los procesos, la operación, los objetivos de negocio y los requisitos legales vigentes en la entidad.

### 2.2. Objetivos Específicos

* Definir la política de seguridad y privacidad de la información de la GOBERNACION DEL VALLE DEL CAUCA.

* Definir los lineamientos a ser considerados para diseñar e implementar el Sistema de Gestión de Seguridad de la Información alineado con las necesidades, los procesos, los objetivos y la operación de la GOBERNACIÓN DEL VALLE DEL CAUCA.

* Dar conformidad y cumplimiento a las leyes, regulaciones y normativas que le aplican a la GOBERNACIÓN DEL VALLE DEL CAUCA en el desarrollo de su misión.

* Proteger los activos de información de la GOBERNACIÓN DEL VALLE DEL CAUCA.

* Mantener un sistema de políticas, manuales, procedimientos y estándares actualizados, a efectos de asegurar su vigencia y un nivel de eficacia, que permitan minimizar el nivel de riesgo de los activos de información de la GOBERNACIÓN DEL VALLE DEL CAUCA.

* Fortalecer la cultura de seguridad de la información en funcionarios, terceros y clientes de GOBERNACIÓN DEL VALLE DEL CAUCA, mediante la definición de una estrategia de uso y apropiación de la política.

* Garantizar la continuidad de negocio frente a la materialización de incidentes de seguridad basados en la norma ISO 27035.

* Definir una estrategia de continuidad de los procesos de la entidad frente a incidentes de seguridad de la Información.

## 3. ALCANCE

La política de Seguridad de la Información es aplicable en todo el ciclo el ciclo de vida de los activos de información de la GOBERNACIÓN DEL VALLE DEL CAUCA, incluyendo creación, distribución, almacenamiento y destrucción. De igual forma para todos los funcionarios, contratistas y terceros que desempeñen alguna labor en la entidad. El alcance abarca desde el enunciado de la política, pasando por los lineamientos para la implementación del Sistema Seguridad y Privacidad de la Información, la matriz de riesgo, la definición de los indicadores para el monitoreo de cumplimiento de la política hasta la definición de una estrategia para la adopción de la política en la entidad.

## 4. MARCO REGULATORIO Y NORMATIVO

La Gobernación Del Valle Del Cauca, como entidad pública, al igual que cualquier organismo del estado, se encuentra cubierta por un marco normativo y regulatorio en todo lo relacionado con la seguridad de la información, como también un marco

de referencia de las mejores prácticas para el desarrollo e implementación del Sistema de Gestión de Seguridad de la Información.

Se tiene en cuenta especialmente la nueva Estrategia de Gobierno Digital, que se evidencia en el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones 1078 de 2015, comprende cuatro grandes propósitos: lograr que los ciudadanos cuenten con servicios en línea de muy alta calidad, impulsar el empoderamiento y la colaboración de los ciudadanos con el Gobierno, encontrar diferentes formas para que la gestión en las entidades públicas sea óptima gracias al uso estratégico de la tecnología y garantizar la seguridad y la privacidad de la información.

A continuación se relacionan las demás normas, leyes, decretos y resoluciones que aplican para el establecimiento, implementación y operación del SGSI en la GOBERNACIÓN DEL VALLE DEL CAUCA:

* NTC-ISO/IEC 27001- 27002:2013
* Decreto 2693 de 2012 MinTic
* Decreto 1008 de 2018 MinTic.
* Decreto 1414 de 2017 de MinTic.
* Ley 1712 de 2014
* Ley 1273 de 2009
* Decreto 1078 de 2015 MinTic
* Ley 1581 de 2012.
* Decreto 415 de 2016 MinTic
* Ordenanza Dptal. 430 de 2016.
* Decreto 1377 de 2013
* Ley 1266 de 2008

Adicionalmente se considera de manera especial que El Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, que el Decreto 1078 de 2015 fue modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

Se tendrán en cuenta e incluirán nuevas normas, leyes, decretos y resoluciones que se generen en esta materia y temas relacionados.

## 5. POLITICA DE SEGURIDAD DE LA INFORMACION DE LA GOBERNACIÓN DEL VALLE DEL CAUCA

### 5.1. Política General

Se define la Política de Seguridad de la Información como la manifestación que hace la alta dirección de la Gobernación Del Valle Del Cauca, sobre la intención institucional de definir las bases para gestionar de manera adecuada y efectiva, la seguridad de la información; garantizando la confidencialidad, integridad y disponibilidad de sus activos de información.

La Gobernación del Valle de; Cauca pretende mediante la adopción e implementación de un Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información.

La GOBERNACIÓN DEL VALLE DEL CAUCA asume el compromiso de implementar el sistema de Gestión de la Seguridad de la Información para proteger los activos de información de los procesos misionales, comprometiéndose a:

5.1.1. La gestión de los riesgos de los activos de información teniendo en cuenta el nivel de tolerancia al riesgo de la entidad.

5.1.2 Una gestión integral de riesgos basada en la implementación de controles físicos y digitales orientados a la prevención de incidentes.

5.1.3. La implementación de políticas de seguridad de alto nivel y de políticas complementarias por cada dominio de la norma ISO/IEC 27001:2013, para asegurar la confidencialidad, integridad y disponibilidad de la información institucional.

5.1.4. El fomento de la cultura y toma de conciencia entre el personal (funcionarios, contratistas, proveedores y terceros) sobre la importancia de la seguridad de la información.

5.1.5. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.

5.1.6. Proteger 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 (ej.: proveedores o clientes), o como resultado de un servicio interno en Outsourcing.

5.1.7, Se mitigaran los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente, y se 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. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

5.1.8. Se protegerá la información de las amenazas originadas por parte del personal de la GOBERNACIÓN DEL VALLE DEL CAUCA.

5.1.9. Se generara conciencia para el cambio organizacional requerido para la apropiación de la Seguridad y Privacidad de la Información

5.1.10. Se protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

5.1.11. Se controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

5.1.12. Se implementará control de acceso a la información, sistemas y recursos de red.

5.1.13. Se garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

5.1.14. Se 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.

5.1.15. Se garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

5.1.16. Se garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Adicionalmente como parte de la política de Seguridad de la Información se contará con las siguientes directrices:

### 5.2. Deberes individuales de los usuarios de la información

5.2.1. Usar la información de la GOBERNACIÓN DEL VALLE DEL CAUCA únicamente para propósitos del negocio autorizado y en cumplimiento de su labor.

5.2.2. Respetar la confidencialidad de la información de la GOBERNACIÓN DEL VALLE DEL CAUCA.

5.2.3. No compartir perfiles de usuario, contraseñas, sesiones en estaciones de trabajo, documentos o cualquier tipo de información confidencial.

5.2.4. No anotar y/o almacenar en logares visibles las contraseñas de acceso a los sistemas.

5.2.5. Ajustarse a las directrices de clasificación de la información.

5.2.6. Bloquear la sesión de la estación de trabajo al momento de ausentarse de la misma.

5.2.7. Las impresiones deben ser recogidas al momento de generarlas, no se deben dejar por largos periodos de tiempo en la impresora.

5.2.8. Devolver y no conservar ningún tipo de copia sus activos de información, en buen estado, una vez cese su relación laboral con la Entidad

5.2.9 Está estrictamente prohibido la divulgación, cambio, retiro o pérdida no autorizada de información de la Entidad almacenada en medios físicos removibles, como USB, cintas magnéticas, entre otros.

5.2.10 Está estrictamente prohibido utilizar software no licenciado en los recursos tecnológicos, copiar software licenciado de la GOBERNACIÓN DEL VALLE para utilizar en computadores personales, ya sea en su domicilio o en cualquier otra instalación y/o entregarlos a terceros.

### 5.3. Deberes de los Responsables de personal

5.3.1. Conceder autorizaciones de acceso a la información acorde con las funciones a ser realizadas por las personas a quienes le coordinan el trabajo.

5.3.2. Asegurar que los privilegios de acceso individuales reflejen una adecuada segregación de funciones. Un usuario no debe tener los permisos suficientes para originar, registrar y corregir/verificar una transacción sensitiva del negocio sin controles adecuados o una revisión independiente.

5.3.3. Restringir el acceso del personal a aquellas áreas que hayan sido restringidas por razones de seguridad.

5.3.4. Ser el responsable de conocer, solicitar y ratificar los privilegios de acceso a los empleados que le reportan.

5.3.5. Conservar los registros de los empleados con privilegios de acceso a la información. Adicionalmente, la Secretaria de las TIC como encargada de la Seguridad de la Información, debe mantener actualizadas las autorizaciones y perfiles de usuario basándose en los archivos de Recursos Humanos y/o contratación (gestión del Outsourcing), donde se encuentran todos los empleados y las áreas a las que pertenecen, al igual que como se establece en la Política de roles y Perfiles.

5.3.6. Los contratos de Outsourcing o con terceras personas, deben identificar claramente los acuerdos relacionados con la propiedad de la información y la no divulgación de información confidencial.

5.3.7. Cuando un empleado se ausenta de su trabajo por un período de tiempo superior al mínimo establecido para cumplir con las regulaciones su superior inmediato debe:

a. Determinar si los accesos a los recursos físicos y a la información deben ser suspendidos.

b. Notificar la fecha en que el acceso debe ser suspendido, de ser necesario.
c. Recoger los equipos de seguridad como por ejemplo llaves, claves, computadoras, etc.
d. Cuando un empleado se encuentra por fuera de las funciones de la GOBERNACIÓN DEL VALLE DEL CAUCA, ya sea por licencia, permiso sindical, suspensión, encargo, etc., el acceso a los recursos físicos y a la información debe ser inmediatamente suspendido por solicitud de su jefe inmediato, de ser necesario.

5.3.8. Cuando un empleado es retirado (voluntaria o involuntariamente), su jefe inmediato es responsable por:

a. Solicitar la revocación de las autorizaciones.
b. Revocar o restringir los privilegios de acceso antes de notificarle la terminación del contrato, si es apropiado.

c. Recoger los equipos, los dispositivos físicos y la revocación de las autorizaciones a los sistemas de información.

### 5.4. Directrices relacionadas con el manejo de información confidencial

5.4.1. Los documentos con esta información no pueden ser dejados desatendidos o inseguros.

5.4.2. Debe indicar el usuario dueño o fuente de información en la primera página o cubierta, o en algún repositorio central.

5.4.3. Debe ser apropiadamente autorizado para la divulgación de acuerdo con los estándares de clasificación de la información por parte de los propietarios.

5.4.4. La divulgación cualquiera que fuere su medio, verbal, escrita, telefónica o electrónica, debe ser efectuada sobre la base de la necesidad de conocerla de acuerdo a sus funciones.

5.4.5. Reuniones relacionadas con el manejo de esta información deben llevarse a cabo en áreas de oficinas cerradas.

5.4.6. No debe ser accedida o enviada a través de cualquier tecnología de fácil acceso, tales como teléfonos celulares o inalámbricos.

5.4.7. Para propósitos de seguridad toda la información debe ser etiquetada con la clasificación respectiva.

5.4.8. El etiquetado debe ser fácilmente leíble a simple vista.

5.4.9. Antes de divulgarse verbalmente información clasificada como Restringida o Confidencial debe indicarse su clasificación.

5.4.10. El acceso o distribución de información de Uso Interno debe estar limitado a empleados u otros con la necesidad de conocerla o usarla para cumplir con sus funciones.

5.4.11. Documentos que contengan información Confidencial deben ser impresos en un área segura o con la supervisión adecuada.

5.4.12. Distribución de información confidencial debe ser limitada a personas o grupos con la necesidad de conocerla o usarla para cumplir con sus funciones.

5.4.13. Los mecanismos de entrega utilizados para información Restringida, deben contemplar confirmación de recibo.

5.4.14. Estas políticas aplican tanto a los originales como a todas las copias de la información.

5.4.15. Acceso a información confidencial que se encuentre almacenada debe ser adecuadamente controlado. Esto incluye información confidencial almacenada externamente o copias de respaldo.

5.4.16. Las copias de respaldo de información confidencial deben ser protegidas de destrucción intencionada o accidental. Algunos métodos de protección pueden incluir contenedores a prueba de fuego, contenedores asegurados y almacenamiento externo.

5.4.17. Información almacenada por períodos prolongados debe ser revisada regularmente para verificar su legibilidad.

5.4.18. Las personas que tienen acceso remoto a la información de la GOBERNACIÓN DEL VALLE DEL CAUCA son responsables por la seguridad de la información con los mismos niveles de control requeridos dentro de la GOBERNACIÓN DEL VALLE DEL CAUCA.

## 5.5. Uso adecuado de Software.

5.5.1. En las estaciones de trabajo de la GOBERNACIÓN DEL VALLE DEL CAUCA sólo se puede instalar software desarrollado o adquirido legalmente y cuya licencia de uso esté a nombre de la GOBERNACIÓN DEL VALLE DEL CAUCA.

5.5.2. La coordinación y ejecución de mantenimiento de programas o aplicaciones instaladas en las estaciones de trabajo es del equipo de trabajo del programa de Gestión de Soluciones T.I de la Secretaria de Tecnologías de Información y Comunicaciones.

5.5.3. Las estaciones de trabajo de la GOBERNACIÓN DEL VALLE DEL CAUCA deben ser utilizadas por los empleados, proveedores o contratistas sólo para el desarrollo de las funciones normales de su trabajo.

5.5.4. Los usuarios deben cumplir con la Legislación Colombiana que regula los derechos de autor.

## 5.6. Control de Virus.

5.6.1. Los computadores personales deben mantener activo un software antivirus, Sistema Operativo, Microsoft Office, licenciados y Actualizados y que su uso haya sido Autorizado por el equipo de trabajo del programa de Gestión de Soluciones T.I de la Secretaria de Tecnologías de Información y Comunicaciones.

5.6.2. Los servidores de archivos, groupware y correo electrónico deben mantener activo un software antivirus.

5.6.3. Los computadores personales y servidores deben ser analizados contra virus periódica y automáticamente.

5.6.4. Cualquier información que venga por medio electrónico o magnético como correo electrónico o información de INTERNET, debe ser revisada por un software antivirus antes de ser descargada y utilizada.

5.6.5. El equipo de trabajo del programa de Gestión de Soluciones T.I de la Secretaria de Tecnologías de Información y Comunicaciones es responsable por la actualización oportuna del software antivirus.

5.6.6. Es responsabilidad de los usuarios reportar todos los incidentes de infección de virus a las áreas encargadas.

5.6.7. Es responsabilidad de los usuarios tomar copias de la información y verificar que el respaldo esté libre de cualquier infección de virus.

5.6.8. El usuario debe asegurar que toda la información provenga de fuentes conocidas.

5.6.9. Ningún usuario puede escribir, distribuir o introducir software que conozca o sospeche que tiene virus.

**5.7. Control de Contraseñas.**

5.7.1. Los perfiles de usuario y la contraseña tienen que ser asignados individualmente para soportar el principio de responsabilidad individual.

5.7.2. Los usuarios no pueden prestar su contraseña, lo que se realice con su perfil queda bajo la responsabilidad del dueño.

5.7.3. El usuario no debe compartir, escribir o revelar su contraseña.

5.7.4. Las contraseñas individuales no deben ser mostradas en texto claro. Todos los sistemas de procesamiento deben eliminar la visualización de contraseñas ya sea en pantallas o en impresoras.

5.7.5. Las contraseñas deben cambiarse con regularidad. La duración máxima de la contraseña debe ser un tiempo razonable (máximo 60 días).

5.7.6. Si un sistema no obliga al cambio de contraseña, es responsabilidad del usuario realizar este cambio.

5.7.7. No se deben repetir contraseñas utilizadas anteriormente, en los últimos cinco cambios.

5.7.8. Debe verificarse la identidad del usuario antes de que las contraseñas o perfiles de usuario sean habilitados nuevamente. Solo se puede cambiar una contraseña cuando el perfil de usuario pertenezca a quien solicita el cambio.

5.7.9. La identificación del usuario y su contraseña no deben ser iguales.

5.7.10. Las contraseñas deben ser cuidadosamente seleccionadas para que no sean adivinadas fácilmente, por lo tanto se deben tener en cuenta las siguientes recomendaciones:

a. No utilizar el primer o segundo nombre, los apellidos, el nombre del esposo, el nombre de sus hijos, etc., en ninguna forma (reversado, diminutivos, etc.)
b. No utilizar otra información fácil de obtener acerca de Usted. Esto incluye: Placa o marca del carro, número del teléfono, marca, nombre del edificio, etc.
c. No use contraseñas que contengan sólo números o sólo letras.
d. No utilice palabras contenidas en el diccionario u otras listas de palabras.
e. Use contraseñas fáciles de recordar para que no tenga que escribirlas.
f. No use el nombre del perfil de usuario en ninguna forma como por ejemplo: reversado o duplicado.

5.7.11. Siempre que el Administrador de contraseñas asigne una contraseña, es responsabilidad del usuario cambiarla en su primer uso.

**5.8. Copias de respaldo de información (Backup):**

5.8.1. Se debe contar con un sistema automático para la recolección de copias de respaldo.

5.8.2. Las copias de respaldo deben tener el mismo nivel de protección de la información que poseen en su fuente original.

5.8.3. Los medios magnéticos que contienen información deben ser almacenados en lugares físicamente seguros.

5.8.4. Los usuarios responsables por respaldar la información, también son responsables de facilitar la oportuna restauración de la información.

5.8.5. Los medios magnéticos deben tener rótulos visibles y legibles tanto internos como externos.

5.8.6. Se debe mantener suficientes respaldos de la información para que en caso de contingencia se pueda recuperar la información oportunamente.

5.8.7. Para responder adecuadamente a una contingencia, los respaldos de la información se deben almacenar en sitios externos.

5.8.8. Cualquier medio magnético que contenga información clasificada como restringida o confidencial, debe estar claramente identificada.

5.8.9. Al enviar Información clasificada como restringida o confidencial a terceros se debe exigir un acuse de recibo.

5.8.10. Todos los medios que contengan información clasificada como restringida o confidencial y que finalice su ciclo de vida, deben ser sobre escritos o destruidos físicamente para que la información no pueda ser recuperada.

5.8.11. Es responsabilidad de los Administradores de las Plataformas, mantener respaldo de la configuración del sistema operativo y de los servicios que estas proveen.

## 5.9. Directrices relacionadas con el desarrollo del software para la GOBERNACIÓN DEL VALLE DEL CAUCA.

5.9.1. Los mecanismos de seguridad definidos para una aplicación específica no deben ser alterados, pasados por alto o comprometidos.

5.9.2. Los controles de seguridad deben ser documentados y deben permitir probar su efectividad.

5.9.3. El software desarrollado no debe presentar nuevas vulnerabilidades o reducir el nivel de seguridad existente.

5.9.4. Cualquier software que use funciones privilegiadas del sistema operativo debe ser aprobado por el equipo de trabajo del programa de Gestión de Soluciones T.I de la Secretaria de Tecnologías de Información y Comunicaciones.

5.9.5. El desarrollo y mantenimiento de software debe dejar las adecuadas pistas de auditoría (Registro de eventos).

5.9.6. El equipo de trabajo del programa de Gestión de Soluciones T.I de la Secretaria de Tecnologías de Información y Comunicaciones son responsables de efectuar pruebas para asegurar que se han cumplido los requerimientos de seguridad.

5.9.7. Todas las aplicaciones deben contar con documentación funcional y técnica.

## 5.10. Políticas de seguridad en el acceso a áreas restringidas.

5.10.1. El acceso a las áreas donde se procesa y almacena información de la GOBERNACIÓN DEL VALLE DEL CAUCA clasificada como restringida o confidencial debe ser autorizado a aquellos empleados con necesidades del negocio de accederla.

5.10.2. Servidores de aplicaciones y bases de datos, y otros dispositivos (excepto las estaciones de trabajo individuales) que son utilizadas para mantener funciones críticas del negocio, deben estar en un área de acceso restringido y separadas del ambiente de las oficinas.

5.10.3. Las puertas exteriores deben ser cerradas con llave o estar aseguradas de otra forma durante las horas no hábiles.

5.10.4. Áreas diseñadas como restringidas deben también tener controles de acceso especiales. El acceso a estas áreas debe ser únicamente para personal autorizado.

5.10.5. Los privilegios de acceso físico autorizados deben ser revisados periódicamente por los jefes de áreas, Secretarios, Directores, Subdirectores, Gerentes y de más personas con mando o designados para tal fin, de acceso restringido y revocados o modificados oportunamente a la terminación, transferencia o cambio en las funciones de una persona.

5.10.6. Los jefes, Secretarios, Directores, Subdirectores, Gerentes y de más personas con mando o designados para tal fin, y encargados de áreas de acceso restringido deben asegurar que los controles de acceso como llaves de seguridad o cerraduras con claves maestras sean cambiadas cuando el control haya sido comprometido.

5.10.7. Las cerraduras convencionales deben ser cambiadas periódicamente.

5.10.8. Se debe restringir el ingreso de dispositivos móviles (Tablet, celulares, cámaras digitales, etc.) a áreas catalogadas como restringidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la entidad como la remisión a la Oficina de Control Disciplinario, procuraduría, fiscalía, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

### 5.11 Política de manejo de documentos electrónicos

5.11.1. Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de la Gobernación Del Valle Del Cauca. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

5.11.2. Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera comprimida y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.

5.11.3. Las comunicaciones electrónicas en lo posible, deben ser concretas, precisas y completas.

5.11.4. Las comunicaciones electrónicas oficiales hacia el exterior deben ser revisadas por un jefe inmediato, puede ser un coordinador de área, Lider, Subsecretario, Secretario; sin este requisito no serán consideradas como documentos oficiales de la Gobernación del Valle del Cauca.

5.11.5. Solamente se considera oficial un mensaje de correo electrónico que incluya el nombre y el cargo del funcionario de la Secretaria de donde lo envía.

5.11.6. Las comunicaciones oficiales y circulares de la Gobernación del Valle del Cauca deben ser escaneadas y enviadas desde el correo electrónico de quien los elabora al funcionario autorizado de manejar la cuenta de comunicados Generales, y deben estar debidamente firmadas por el Secretario de Despacho.

5.11.7. Los Comunicados Generales son comunicados emanados desde la administración central hacia la totalidad de los funcionarios; los cuales únicamente

deben ser enviados sólo por un funcionario de la secretaría General o de la oficina de comunicaciones y prensa, ésta persona sólo la autoriza el (la) Asesor (a) de Prensa y comunicaciones y/o el secretario General. El funcionario autorizado es quien realizará el filtro de los correos de interés general para luego ser enviados a todos los funcionarios de la Gobernación del Valle del Cauca. Además, no puede enviarse información con logotipos o propaganda de índole política, comercial o sindical.

5.11.8. Se deben conservar los niveles de seguridad en el manejo de la información electrónica conforme a los parámetros definidos institucionalmente para tal fin.

5.11.9. La asignación de cuentas de correo electrónico a contratistas será autorizado por el Secretario de Despacho del respectivo contrato.

5.11.10. Todas las direcciones de correo electrónico deben ser creadas usando el estándar establecido por el La Secretaria de las TIC para dicho fin.

5.11.11. Todos los funcionarios de la Gobernación del Valle del cauca tendrán correo electrónico personalizado.

5.11.12. El uso del correo electrónico para fines personales deberá ser racional.

5.11.13. Se establecerá un tamaño de buzón de correo para cada usuario, es decir un espacio en disco en el servidor de correo, destinado al almacenamiento de mensajes electrónicos de cada usuario.

5.11.14. El usuario responsable del buzón deberá dar un trámite ágil al correo electrónico recibido, es decir, diariamente debe leer, responder y eliminar o archivar en el disco duro local, solamente los mensajes que soporten información relevante para el desarrollo de sus labores en la entidad.

5.11.15. Todos los mensajes que superen un (1) mes de almacenamiento en el servidor podrán ser eliminados permanentemente de acuerdo a las políticas de limpieza del servidor y La Secretaria de las TIC no se responsabiliza por el backup de los buzones de correo electrónico.

5.11.16. El mantenimiento de la lista de contactos y del buzón será responsabilidad del usuario y deberá conservar únicamente los mensajes necesarios con el fin de no exceder el máximo límite de almacenamiento.

5.11.17. Los mensajes deben ser redactados de forma clara y concreta, evitando el uso de MAYUSCULAS sostenidas, que según normas internacionales de redacción en Internet, equivale a gritar.

5.11.18. En el nombre del destinatario y el asunto debe evitarse el uso de caracteres especiales como slash (/), tildes ('), guiones (-), etc.

5.11.19. Los mensajes de correo salientes siempre deben llevar en el campo "Asunto" una frase que haga referencia directa al contenido del texto.

5.11.20. Todos los mensajes de correo enviados deben contener como mínimo la siguiente información: Nombre: Cargo: Dependencia: Entidad: Teléfono.: - Ext. Email.

5.11.21. Ningún usuario deberá permitir a otro enviar correos utilizando su cuenta, sin aclarar el remitente.

5.11.22. La "confirmación de lectura" solo debe ser utilizada en situaciones estrictamente necesarias con el fin de evitar la congestión de mensajes.

5.11.23. Cuando un funcionario requiere ausentarse de la Entidad por un período superior a 8 días debe programar el correo electrónico para que automáticamente responda a los remitentes indicando fecha de llegada, nombre y dirección de correo electrónico de la persona encargada durante su ausencia.

5.11.24. El envío de mensajes a grupos de usuarios múltiples como "Todos los usuarios" cuyo tamaño pueda ocasionar saturación en el tráfico de la red ponen en riesgo la disponibilidad de los servicios informáticos de la Secretaria de las TIC al exceder su capacidad, por lo que este servicio se restringe para enviar mensajes hasta 20 usuarios máximo y que sean de carácter oficial. Como alternativa, cuando se desee publicar documentos o manuales se deben publicar en la Intranet. Por lo anterior, queda rotundamente prohibido enviar correos a más de 20 usuarios para

evitar spam y cualquier otro tipo de anomalía que afecte el buen uso de esta herramienta.

5.11.25. Antes de enviar un correo deberá verificarse que esté dirigido solamente a los interesados y/o a quienes deban conocer o decidir sobre el tema, evitando duplicidades o desmejoramiento en el servicio y operación de la red.

### 5.12 Política de manejo integral con gestión documental

Igualmente dentro del Manual de Gestión Documental y Organizacional MA-M9-P3-1 Se establecen los siguientes lineamentos que hace parte integral de la política de manejos de documentos electrónicos. En este sentido y con el ánimo de evidenciar procesos de transparencia en la gestión y el mejoramiento de los servicios a los ciudadanos, la Gobernación del Valle en asocio con el Archivo General de la Nación, han adelantado procesos de fortalecimiento a la gestión electrónica para potenciar la gestión documental en la región y con ello, el desarrollo del Departamento.

• La Gobernación del Valle del Cauca cuenta con Internet y servicios de correo electrónico, la Secretaria de las TIC reglamentará su utilización de acuerdo a las políticas y asignarán responsabilidades de acuerdo con la cantidad de cuentas habilitadas. En todo caso, las unidades de correspondencia tendrán el control de los mismos, garantizando el seguimiento de las comunicaciones oficiales recibidas y enviadas.

• Para los efectos de acceso y uso de los mensajes de datos del comercio electrónico y de las firmas digitales se deben atender las disposiciones de la Ley 527 de 1999 y demás normas relacionadas.

• Correos Electrónicos: Teniendo en cuenta el acuerdo 060 de 2001, las instituciones que son cubiertas por la ley 594 de 2000 están en la obligación de generar mecanismos para administrar las comunicaciones oficiales que se reciben y se despachan a través del correo electrónico. El encargado de la Central de Correspondencia debe capturar la misma información que la obtenida mediante el correo certificado.

• INSTRUCTIVO PARA MENSAJES ELECTRONICOS El mensaje electrónico es un sistema que permite intercambiar información con uno o más usuarios de cualquier lugar del mundo, a través del internet. Este medio se puede utilizar para enviar adjuntos como cartas, memorandos, circulares y cualquier otro documento que sea necesario para la sustentación del contenido, razón por la cual se recomienda tener en cuenta las disposiciones de esta guía para cada uno de estos casos. Para garantizar el éxito en el intercambio del correo electrónico, se presentan las siguientes sugerencias:

Es recomendable que las organizaciones que disponen de internet y servicios de correo electrónico, reglamentar su utilización y asignar responsabilidades con base en usuarios debidamente autorizados para el manejo de correo tanto masivo como institucional. NOTA: En la Gobernación del Valle se administraran los correos electrónicos de acuerdo con las políticas establecidas por la Secretaria de las TIC soportados en la ley 527 de 1999.

CARACTERISTICAS DE REDACCION Y LA PRESENTACION De acuerdo con las plantillas que vienen definidas en la mayoría de los servicios del internet, a continuación se identifican las partes del correo electrónico:

ENCABEZAMIENTO: De informa a los receptores quien es el remitente del mensaje. Para indica la dirección del destinatario Asunto es el resumen que da una idea, por adelantado, de lo Tratado en el correo. Se recomienda una frase corta y lo más Descriptiva posible del contenido del mensaje.

CUERPO DE TEXTO: Se recomienda que el saludo y la despedida sean como una carta normal. Se sugiere escribir el mensaje, teniendo en cuenta las reglas básicas de ortografía (tildes, mayúsculas, diéresis, puntuación, entre otros). Se aconseja incorporar una firma al final de cualquier mensaje, aunque solo sea el nombre. También puede incluir el cargo, la organización, el departamento, el teléfono y la extensión.

### 5.13. Recomendaciones

Se recomienda no utilizar el correo electrónico para resolver temas complejos.

Se recomienda no participar en cadenas de mensajes. Este tipo de mensajes consumen recursos de la red y del correo que son costosos y adicionalmente distraen el trabajo. Generalmente este tipo de correos se usa para recoger direcciones electrónicas y para luego enviar mensajes de propaganda o de todo tipo, también son muy usados para propagar virus.

Se recomienda utilizar las letras mayúsculas solo en los casos necesarios.

Antes de contestar un mensaje individual o a través de una lista, se debería tener en cuenta lo que se va a contestar y lo que es imprescindible para entender el contexto del mensaje.

Se recomienda utilizar el campo con copia oculta (CCO), cuando se envié o se responda un mensaje que incluya múltiples direcciones, o cuando se envíen mensajes que incluyan muchas personas o grupos corporativos. Esto con el fin de no publicar las direcciones de correo y que después se utilicen para enviar correos basura.

Se recomienda ser breve.

Se sugiere pensar en el tiempo del destinatario y en los costos de la comunicación.

Los mensajes deberían ser cortos y concisos.

Se debe tener cuidado con los archivos adjuntos, se recomienda no adjuntar archivos con virus o con un tamaño que no pueda recibir o descargar el destinatario.

Se recomienda no utilizar formatos o codificaciones propios de los mensajes, sino los compactibles con el internet, porque hay que tener en cuenta que no todos los usuarios utilizan el mismo programa de correo electrónico ni su mismo sistema operativo.

Se recomienda tener el menor número posible de mensajes en la bandeja de entrada, para ello se sugiere crear carpetas, las cuales se pueden organizar por temas o series documentales, labores, proyectos, mensajes pendientes, años entre otros.

Cuando el software no reorganice el texto se sugiere dar formato al mismo, con una resolución del 75% ciento del zoom para facilitar la impresión.

## 5.14 Política Complementaria

Como complemento a la política relacionada con el manejo, se formulan los siguientes principios orientadores para el manejo de los documentos electrónicos. Orientación al usuario y al ciudadano: Todas las actividades desplegadas en desarrollo de la política estarán orientadas a que los documentos electrónicos sirvan como fuente de información a las dependencias y a la comunidad en general.

Transparencia: Los documentos de la Gobernación del Valle del Cauca son considerados como evidencia de las actuaciones de la administración, respaldan las actuaciones de los servidores públicos y deben estar disponibles para el ejercicio del control ciudadano.

Eficiencia: Dentro de las actividades diarias, la Gobernación del Valle Del Cauca producirá solamente los documentos electrónicos necesarios para el cumplimiento de sus objetivos, funciones y procesos.

Cero Papel: La Gobernación del Valle del Cauca se encuentra comprometida con la política "cero papel" del estado Colombiano. En este sentido se adoptan buenas prácticas para la reducción del uso de papel y se propenderá por la formación de nuevos hábitos en los servidores públicos.

Acceso: La Gobernación del Valle del Cauca con respecto a los accesos a documentos de archivo, respeta a cabalidad el derecho de los ciudadanos a consultar la información que conservan los archivos públicos, en los términos consagrados por la Ley.

Cumplimiento Legal: La Gobernación del Valle del Cauca, adopta la reglamentación y política documental con respecto a la salvaguarda del patrimonio documental de la nación y de la conservación y la difusión del acervo documental que lo integra y del que se le confía en custodia.

5.14.1. La política de manejo de documentos electrónicos está integrado con el sistema de gestión Integral.

5.14.2. La política de manejo de documentos electrónicos es transversal a todas las dependencias de la Gobernación.

5.14.3. Cada documento electrónico generado tiene asociado un responsable.

5.14.4. Cada documento electrónico generado por la Gobernación hará parte de su sistema de gestión documental.

5.14.5. Cada documento electrónico deberá ser identificado, tramitado y organizado, usando las tablas de retención documental y demás lineamientos que se encuentran definidos en el manual de gestión documental y organizacional MA-M9-P3-1.

5.14.6. Cada documento electrónico debe tener garantizada su trazabilidad a través de todo su ciclo de vida.

5.14.7. Todos los documentos electrónicos deben tener una valoración que permitirá determinar una clasificación para determinar los procedimientos que aplican para su disposición final, garantizando su preservación a largo plazo.

5.14.8. La Gobernación del Valle del Cauca divulgara adecuadamente la metodología para la creación, uso, mantenimiento, retención, acceso y preservación de los documentos electrónicos.

5.14.9. La Secretaria de las Tecnologías de la Información y las Comunicaciones revisara permanentemente la política de manejo de documentos electrónicos.

## 6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION EN LA GOBERNACIÓN DEL VALLE DEL CAUCA.

En esta política se definen los roles y responsabilidades de la Seguridad de la Información, específicamente con respecto a la protección de los activos de información. Esta política se aplica a todos los funcionarios, contratistas y terceros de la entidad sin excepción, en donde cada uno de los cuales cumple un rol en la administración de la seguridad de la información. Todos funcionarios, contratistas y terceros de la entidad son responsables de mantener un ambiente seguro, en tanto que el Equipo de La Secretaria de las TIC, Los enlaces TIC en otras dependencias, los CIO de los municipios y entidades descentralizadas o adscritas a la Gobernación del Valle del Cauca, las dependencias y entes descentralizados , Los miembros de los Comités TIC de La Gobernación y del Departamento y el Oficial de Seguridad de la Información debe monitorear el cumplimiento de las políticas de seguridad definidas y realizar las actualizaciones que sean necesarias.

Las políticas deben ser revisadas mínimo una vez por periodo de gobierno o cuando se produzca un cambio relevante en la operación que implique realizar ajustes o producto de los cambios en el entorno tecnológico y/o de las necesidades de la operación.

Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información, en especial las relacionadas con el comité de seguridad de la información (o quien haga sus veces) y del oficial de seguridad de la información.

### 6.1. Apoyo de la Alta Dirección.

Las directivas de la Gobernación Del Valle Del Cauca, deben apoyar activamente la seguridad de la información dentro de la entidad, definir un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información. Este compromiso se verá reflejado a través de:

6.1.1. Se debe crear al interior de la entidad un comité de seguridad de la información o uno quien haga sus veces, que sea interdisciplinario y formalizado por una resolución interna.

6.1.2. La Secretaria de las TIC de la GOBERNACIÓN DEL VALLE DEL CAUCA debe mantener dentro de sus colaboradores un funcionario o contratista con el perfil de Oficial de Seguridad de la Información, quien será el encargado de todo lo relacionado con la seguridad de la información y cuyas funciones estarán caracterizadas y definidas en la presente política.

6.1.3. Se debe velar por el cumplimiento de las políticas de seguridad de la información, comprometerse para que los funcionarios a su cargo, conozcan y apliquen las políticas de seguridad de la información.

6.1.4. Se deben asignar responsabilidades "a las áreas y personas" asociadas a temas de la seguridad de la información.

6.1.5. La alta dirección de la GOBERNACIÓN DEL VALLE DEL CAUCA o el Comité de seguridad de la Información (o quien haga sus veces), debe apoyar, facilitar y mantener cuando se requiera relaciones con empresas, entidades u organismos que presten asesoría especializada en seguridad de la información.

Se deben establecer tres niveles diferentes de gestión de la seguridad de la información, en la participación de la definición y aplicación del SGSI:

* Estratégico: - Dirigir y proveer: Definir los grandes lineamientos directivos o gerenciales para la seguridad de la información y la política global del SGSI, coordinar y aprobar los recursos.

* Táctico: - Implementar y optimizar: Diseñar e Implementar el SGSI, establecer objetivos concretos / específicos, gestionar los recursos.

* Operacional: - Ejecutar y reportar: Alcanzar los objetivos específicos mediante procesos técnicos.

En la administración de la seguridad de la información participan todos los colaboradores de la Gobernación Del Valle Del Cauca, siguiendo uno o más de los siguientes roles:

* Comité de Seguridad de la Información (o quien haga sus veces).
* Oficial de Seguridad de la Información.
* Funcionarios, contratistas, proveedores y terceros.
* Responsable de la información.
* Administradores de sistemas.
* Gestores de Seguridad de la Información por áreas

### 6.2. Oficial o Gestor de la Seguridad de la Información.

El Oficial de la Seguridad de la Información debe desarrollar todas las actividades de coordinación de la seguridad de la información. La GOBERNACIÓN DEL VALLE DEL CAUCA debe contar con un colaborador, funcionario o contratista que cumpla con la función de Oficial de Seguridad de la Información que asuma las tareas y responsabilidades que conlleva este rol:

6.2.1. Formular, definir y actualizar políticas, normas, procedimientos y estándares definidos en el SGSI, junto con el comité de seguridad de la información.

6.2.2. Mantener actualizado el análisis y evaluación del riesgo sobre los activos de información de la Gobernación Del Valle Del Cauca. Dentro de este propósito se debe mantener definida y actualizada una metodología e instrumentos de levantamiento de activos de información y una política y metodología de gestión de riesgos.

.

6.2.3. Socializar la guía de activos de Información y registrar los activos de información conforme a la ley 1712.

6.2.4. Evaluar, apoyar, dar visto bueno y emitir conceptos técnicos, sobre nuevas soluciones o plataformas tecnológicas a adquirir o implementar en La GOBERNACIÓN DEL VALLE DEL CAUCA, independiente de la dependencia.

6.2.5. Asesorar en la aplicación de la metodología para el mantenimiento de los planes de contingencia y continuidad del negocio.

6.2.6. Evaluar, seleccionar e implantar herramientas que faciliten la labor de seguridad de la información.

6.2.7. Dar los lineamientos para controlar el acceso a los sistemas de información y la modificación de privilegios.

6.2.8. Promover en la GOBERNACIÓN DEL VALLE DEL CAUCA la formación, educación y el entrenamiento en seguridad de la información.

6.2.9. Mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes.

6.2.10. Recibir capacitación en el tema de seguridad de la información.

6.2.11. Realizar estudios o consultas de pruebas de seguridad en todos los ambientes informáticos de la entidad.

6.2.12. Proyectar, proponer, presentar y someter a consideración del Comité, las políticas, normas, acciones o buenas prácticas necesarias para incorporar y/o aplicar en la Gestión de la Seguridad de la Información de la entidad.

6.2.13. Crear y revisar los acuerdos de confidencialidad con funcionarios, contratistas proveedores y terceros.

6.2.14. Apoyar la implementación de los lineamientos dispuestos por MINTIC en cumplimiento de las disposiciones reglamentarias vigentes para entidades del orden nacional y la Estrategia Gobierno Digital.

El Oficial o gestor de Seguridad de la Información podrá convocar diferentes funcionarios para formar grupos interdisciplinarios que apoyen la definición e

implementación de los diferentes temas de seguridad de la información. De igual forma será el encargado de coordinar el conocimiento y las experiencias disponibles en la entidad a fin de brindar ayuda en la toma de decisiones en materia de seguridad de la Información. Ésta persona podrá obtener asesoramiento de otros organismos o entidades, con el objeto de optimizar su gestión, se habilitará el contacto con todas las áreas, dependencias o unidades organizativas internas.

6.2.15 Verificar la aceptación y aprobación Riesgos identificados; y de sus respectivos planes de tratamiento. Evaluación de riesgos residuales.

6.2.16 Revisar y actualizar periódicamente los inventarios de activos de información, definiendo responsabilidades, criticidad, sensibilidad, reserva, protección adecuada y las infraestructuras Críticas.

### 6.3. Todas las Dependencias, Secretarias y Oficinas de La GOBERNACIÓN DEL VALLE DEL CAUCA.

Todas las dependencias de la entidad deben tener en cuenta y cumplir los siguientes lineamientos:

6.3.1. Toda adquisición e implementación de una solución o plataforma tecnológica (hardware o software), debe contar con el visto bueno, concepto técnico y acompañamiento de la Secretaria de las TIC y el Oficial de Seguridad de la Información, en donde se evalúen los aspectos de viabilidad técnica al momento previo de la realización de la liberación de pedido, compatibilidad, capacidad, integridad y disponibilidad, tanto desde la óptica de infraestructura de TI, como el de seguridad de la información.

6.3.2. Todo requerimiento, incidente, problema o cambio debe ser reportado y tramitado por la mesa de ayuda de la Secretaria de las TIC, único medio valido y autorizado para estos fines.

6.3.3 El personal de SETIC, está autorizado para realizar o supervisar el mantenimiento, cambios de partes, cambio de aplicativos, y/o otra actividad que

genere modificaciones que afecten la seguridad en los equipos de propiedad de la GOBERNACIÓN DEL VALLE.

6.3.4. Incluir y tener en cuenta los lineamientos y políticas de Seguridad de la información en la gestión de la contratación con terceros, proveedores y contratistas, así como en la gestión de proyectos, independientemente del tipo de proyecto.

6.3.5. Cumplir y apoyar el cumplimiento de todas las políticas, normas, manuales y procedimientos de seguridad de la información.

### 6.4. Departamento Administrativo y de Desarrollo Institucional.

Esta dependencia debe cumplir las funciones de:

6.4.1. Asegurar que los empleados y contratistas durante el proceso de selección, comprenden sus responsabilidades, los términos y las condiciones de contratación y que son idóneos en los roles para los que se contratan.

6.4.2. Asegurar de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la GOBERNACIÓN DEL VALLE DEL CAUCA.

6.4.3. Contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.

6.4.4. Proteger los intereses de la GOBERNACIÓN DEL VALLE DEL CAUCA, incorporando un procedimiento como parte del proceso de cambio o terminación de las responsabilidades del empleo o contrato.

6.4.5. Gestionar la notificación a todo el personal que ingresa a laborar en la GOBERNACIÓN DEL VALLE DEL CAUCA de sus obligaciones respecto del cumplimiento de las Políticas de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella se deriven.

6.4.6. Notificar, divulgar y socializar la presente Política a todo el personal, los cambios que en ella se produzcan, la implementación de la suscripción de los compromisos de confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad de la información de acuerdo con las necesidades y coordinadas previamente con el Oficial de Seguridad de la Información.

6.4.7. Incorporar dentro de sus procedimientos el cumplimiento de la firma de un acuerdo de confidencialidad definido por el Oficial de Seguridad de la Información, El Departamento Administrativo Jurídico y aprobado por el Comité de Seguridad (o quien haga sus veces), esta actividad se realizara con la emisión de los conceptos técnicos y una vez sea aprobado por el Departamento Administrativo Jurídico o quien haga sus veces, se incorporara al resto de documentos oficiales.

6.4.8. Conocer, comprender y aplicar la Política de Seguridad de la información de la GOBERNACIÓN DEL VALLE DEL CAUCA en los procedimientos que apliquen a su trabajo.

### 6.5. Departamento Administrativo de Jurídica.

6.5.1. Debe incluir y tener en cuenta los lineamientos y políticas de Seguridad de la información en la gestión de la contratación con terceros, proveedores y contratistas.

6.5.2. Es responsabilidad de esta dependencia velar por el cumplimiento de la política de seguridad de la información en el desarrollo de sus funciones, con sus funcionario contratistas, proveedores y con terceros. Así mismo, asesorar en materia legal a La GOBERNACIÓN DEL VALLE DEL CAUCA en lo que se refiere a la seguridad de la información.

6.5.3. Esta área, debe exigir para todo contrato con proveedores, terceros, contratistas, etc., la firma del acuerdo de confidencialidad y apoyar la supervisión del cumplimiento de las políticas de Seguridad de la Información. Para lo anterior, se definirá un Normograma en donde se identifiquen las leyes, decretos y artículos de la constitución Colombiana aplicable a la entidad en relación a la Seguridad de la Información. Esta herramienta será apoyo tanto para la Departamento Administrativo Jurídico o quien haga sus veces como para las demás áreas misionales de la entidad.

6.5.4. Conocer, comprender y aplicar la Política de Seguridad de la información de la GOBERNACIÓN DEL VALLE DEL CAUCA en los procedimientos que apliquen a su trabajo.

## 6.6. Secretaria de Tecnologías de Información y Comunicaciones.

La Secretaria de Tecnologías de Información y Comunicaciones, debe cumplir la función de cubrir los requerimientos de seguridad de la información, definidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de La GOBERNACIÓN DEL VALLE DEL CAUCA.

Todo lo anterior dentro de los marcos de operación, desarrollo, gobierno, cumplimiento y de buenas prácticas que sean establecidas en la entidad, ejemplo: (Marco de Referencia de Arquitectura Empresarial, ITIL, COBIT, SOA, Gobierno Digital, etc.).

La Secretaria de Tecnologías de Información y Comunicaciones debe dar el visto bueno, concepto técnico y acompañamiento a todas las nuevas instalaciones de procesamiento de la información, soluciones o plataformas tecnológicas. (Hardware o software), en donde se evalúen los aspectos de viabilidad técnica, compatibilidad y capacidad.

6.6.1. Los nuevos recursos de procesamiento de información deben y serán autorizados por la Secretaria de Tecnologías de Información y Comunicaciones, según aplique, considerando su propósito y uso, a fin de garantizar que se cumplan

todas las políticas y requerimientos de seguridad de la información, así como los lineamientos de arquitectura tecnológica.

6.6.2. Todas las nuevas adquisiciones e instalaciones de soluciones o plataformas tecnológicas (Hardware o software) de la GOBERNACIÓN DEL VALLE DEL CAUCA, deben contar con el visto bueno y concepto técnico de la Secretaria de Tecnologías de Información y Comunicaciones y del Oficial de Seguridad de la Información, en donde se evalúen los aspectos de viabilidad técnica (estudios, diseño, arquitectura), compatibilidad, capacidad, integridad, disponibilidad y confidencialidad.

6.6.3. Cuando aplique, el propietario de la información con el asesoramiento Grupo de Informática, deben, verificar el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas que ya están en operación o en producción en la entidad.

6.6.4. Se restringe el uso de equipos o elementos personales de procesamiento de información en el lugar de trabajo. En consecuencia, su uso será evaluado en cada caso y deberá ser autorizado por la Secretaria de Tecnologías de Información y Comunicaciones.

6.6.5. Conocer, comprender y aplicar la Política de Seguridad de la información de la GOBERNACIÓN DEL VALLE DEL CAUCA en los procedimientos que apliquen a su trabajo.

### 6.7. Oficina de Control Interno

6.7.1. La Oficina de Control Interno de la GOBERNACIÓN DEL VALLE DEL CAUCA, o en su defecto quien sea propuesto por el Comité de Seguridad de la Información debe de practicar auditorías periódicas sobre los sistemas de información y toda la plataforma tecnológica instalada y en operación (software y hardware), como mínimo una vez al año o en caso de presentarse cambios sustanciales en los recursos tecnológicos de la entidad, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información

establecidas por esta Política y por las normas, procedimientos y prácticas que de ella deriven.

6.7.2. Conocer, comprender y aplicar la Política de Seguridad de la información de la GOBERNACIÓN DEL VALLE DEL CAUCA en los procedimientos que apliquen a su trabajo.

### 6.8. Funcionarios – contratistas de la GOBERNACIÓN DEL VALLE DEL CAUCA.

Los usuarios de la información (funcionarios – contratistas – proveedores - terceros) y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer y cumplir la Política de Seguridad de la Información vigente. Los funcionarios – contratistas – proveedores - terceros de la GOBERNACIÓN DEL VALLE DEL CAUCA, deben:

6.8.1. Conocer, comprender y aplicar la Política de Seguridad de la información de la GOBERNACIÓN DEL VALLE DEL CAUCA en los procedimientos que apliquen a su trabajo.

6.8.2. Llevar a cabo su trabajo, asegurándose de que sus acciones no producen ninguna infracción de seguridad de la información.

6.8.3. Comunicar las incidencias de seguridad de la información que detecte al Oficial de Seguridad de la Información.

6.8.4. Hacer uso de las mejores prácticas definidas en la entidad para todos los temas relacionados con la seguridad de la información.

6.8.5. Cumplir con el acuerdo de confidencialidad firmado con la entidad.

6.8.6. Reportar al Oficial de Seguridad de la Información cualquier anormalidad que atente contra la seguridad de la información en la Entidad.

## 6.9. Responsables de la Información.

El propietario de un activo de información, entendiéndose como tal, aquel que es el responsable de dicho activo, tendrá las siguientes responsabilidades:

6.9.1. Definir si el activo de información está afectado por la Ley de Protección de Datos y aplicarle en su caso, los procedimientos correspondientes.

6.9.2. Definir quiénes pueden tener acceso a la información, cómo y cuándo, de acuerdo con la clasificación interna de la información y la función a desempeñar.

6.9.3. Informar al Oficial de Seguridad de la Información cuando detecte cualquier incidente de seguridad de la información, para tratarlo y corregirlo mediante la aplicación de controles.

6.9.4. Implementar las medidas de seguridad de la información necesarias en su área para evitar fraudes, robos o interrupción en los servicios.

6.9.5. En los casos que aplique, asegurarse de que el personal; funcionarios, contratistas y proveedores tienen cláusulas de confidencialidad en sus contratos y son conscientes de sus responsabilidades.

6.9.6. Conocer, comprender y aplicar la Política de Seguridad de la información de la GOBERNACIÓN DEL VALLE DEL CAUCA en los procedimientos que apliquen a su trabajo.

## 6.10. Administradores de los Sistemas o Plataformas de TI.

Los administradores de los diferentes sistemas o de las diferentes plataformas de TI, deben en forma activa implementar las políticas, normas, estándares, formatos

y procedimientos, para brindar un nivel apropiado de seguridad de la información. Deberán:

6.10.1. Conocer y cumplir las políticas de seguridad de la información.

6.10.2. Conocer, comprender y aplicar la Política de Seguridad de la información de la GOBERNACIÓN DEL VALLE DEL CAUCA en los procedimientos que apliquen a su trabajo.

6.10.3. Dentro de sus funciones de administración de los sistemas de información o plataformas tecnológicas, aplicar los lineamientos o políticas de seguridad de la información que le sean comunicadas y apliquen a su línea de administración.

6.10.4. Informar al Oficial de Seguridad de la Información cuando detecte cualquier incidente de seguridad de la información y sugerir controles o contramedidas para su tratamiento.

6.10.5. Documentar los aspectos de seguridad de la información aplicados dentro de su línea de gestión y su respectivo control de cambios.

### 6.11. Contratistas Proveedores y/o Terceros.

La GOBERNACIÓN DEL VALLE DEL CAUCA debe establecer para los contratistas, terceros y proveedores las mismas restricciones de acceso a la información que a un usuario interno. Además, el acceso a la información debe limitarse a lo mínimo indispensable para cumplir con la actividad asignada o contratada. Las excepciones deben ser analizadas y aprobadas por el Responsable de la Información y el Oficial de Seguridad de la Información de la entidad. Esto incluye tanto acceso físico como lógico a los activos de información.

6.11.1. Los contratistas, proveedores y terceros que tengan acceso a los activos de información, están obligados a cumplir las políticas de Seguridad de la Información de la GOBERNACIÓN DEL VALLE DEL CAUCA.

6.11.2. Todo acceso por parte de personal externo debe ser autorizado por un responsable interno, quien asume la responsabilidad por las acciones que pueda realizar el mismo.

6.11.3. El personal externo debe firmar un acuerdo de confidencialidad o un acuerdo de no-divulgación antes de obtener acceso a información de la entidad.

6.11.4. A los proveedores, solo se les dará acceso a los sistemas de información de la GOBERNACIÓN DEL VALLE DEL CAUCA, únicamente bajo un requerimiento formal y previa aprobación del dueño o responsable del activo de información y solo cuando sea necesario.

6.11.5. Todas las conexiones que se originan desde redes o equipos externos hacia la GOBERNACIÓN DEL VALLE DEL CAUCA, deben limitarse únicamente a los servidores y aplicaciones necesarios. Si es posible, estos servidores destino de las conexiones deben estar físicamente o lógicamente separados de la red interna de la entidad por medio de una zona desmilitarizada (DMZ).

6.11.6. En los contratos de procesamiento de datos externos se debe especificar los requerimientos de seguridad y acciones a tomar en caso de violación de los contratos.

6.11.7. Todos los contratos deben incluir una cláusula donde se establezca el derecho de la GOBERNACIÓN DEL VALLE DEL CAUCA de nombrar a un representante autorizado para evaluar la estructura de control interna del proveedor.

6.11.8. Los contratistas, proveedores y terceros deben comunicar los incidentes de seguridad de la información que detecten, al respectivo supervisor del contrato, para hacer el trámite o seguir el conducto regular. Los procedimientos de gestión de incidentes estarán basados en lo establecido en la norma ISO 27035.

### 6.12. Cooperación Interinstitucional.

A efectos de intercambiar experiencias y obtener asesoramiento para el mejoramiento de las prácticas y controles de seguridad, el Oficial de Seguridad de

la Información debe y podrá mantener contactos con entidades, organismos o empresas especializados en temas relativos a la seguridad de la Información, como por ejemplo:

* Ministerio de Tecnologías de Información y comunicaciones
* Alta Consejería TIC
* CSIRT de la Policía Nacional
* ColCert
* Instituto Colombiano de Normas Técnicas ICONTEC
* Empresas especializadas del sector privado
* Academia
* Registraduria
* Otros Organismos

En las actividades de asesoramiento, cuando se presente intercambio de información de seguridad, no se divulgará información confidencial perteneciente a la GOBERNACIÓN DEL VALLE DEL CAUCA a personas no autorizadas.

El intercambio de información confidencial para fines de asesoramiento o de transmisión de experiencias, sólo se permite cuando previamente se haya firmado un Acuerdo de Confidencialidad, el cual debe ser de obligatorio cumplimiento para el personal que participen en los temas que se tratan.

### 6.13. Servicios Tercerizados o en Outsourcing.

Los contratos o acuerdos de tercerización total o parcial de servicios, para la administración y/o control de sistemas de información, redes y/o plataformas tecnológicas de la GOBERNACIÓN DEL VALLE DEL CAUCA, deben contemplar los siguientes aspectos:

6.13.1. Deben describir la forma en que se cumplirán los requisitos legales aplicables.

6.13.2. La GOBERNACIÓN DEL VALLE DEL CAUCA como entidad contratante, es la que determina los lineamientos, políticas, manuales, estándares y demás

parámetros de Seguridad de la Información que se deben aplicar, así como es quien aprueba cualquier ajuste o cambio de las mismas.

6.13.3. La GOBERNACIÓN DEL VALLE DEL CAUCA tiene el derecho de auditar cualquier aspecto de los servicios o actividades tercerizadas en forma directa o a través de la contratación de servicios ad hoc.

6.13.4. Deben establecer los medios de comunicación y socialización, para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad de la información.

6.13.5. Deben definir la forma o metodología con la que se mantendrá y comprobará la integridad y confidencialidad de los activos de la entidad.

6.13.6. Deben definir los controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible de la entidad.

6.13.7. Deben definir la forma o metodología que usaran para garantizar la disponibilidad de los servicios ante la ocurrencia de desastres.

6.13.8. Deben definir los niveles de seguridad física y del entorno que se asignarán al equipamiento tercerizado.

6.13.9. Se debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.

6.13.10. Se deben establecer dentro de los acuerdos de confidencialidad o de no divulgación, el cumplimiento de las políticas de seguridad y de los respectivos controles de seguridad implementados en la entidad.

6.13.11. Se deben definir y determinar de niveles de disponibilidad aceptable.

6.13.12. Se deben garantizar ambientes aislados, si se ha contratado un servicio de procesamiento de la información de la entidad.

6.13.13. El proveedor debe y es responsable de informar de manera inmediata al supervisor del contrato de cualquier brecha o incidente de seguridad, que pueda comprometer los activos de información de La GOBERNACIÓN DEL VALLE DEL CAUCA.

6.13.14. Cualquier contratista, proveedor o tercero de la entidad debe informar de violaciones a la seguridad de la información por parte de proveedores, al respectivo supervisor del contrato, para hacer el trámite o seguir el conducto regular.

## 6.14. Acuerdos de Confidencialidad.

6.14.1. Todos los funcionarios, contratistas, proveedores y terceros, que deban realizar labores dentro de la GOBERNACIÓN DEL VALLE DEL CAUCA, ya sea por medios lógicos o físicos que involucren el manejo de información, deben conocer, entender, firmar y aceptar el correspondiente acuerdo de confidencialidad de la información.

6.14.2. Se debe revisar a intervalos de tiempo regulares el texto, de los acuerdos de confidencialidad, avalando que reflejan las necesidades de la entidad para la protección y seguridad de la información.

## 7. Revisión del SGSI.

La Alta Dirección y el Comité de Seguridad de la Información, debe revisar el Sistema de Gestión de Seguridad de la Información (SGSI) de La GOBERNACIÓN DEL VALLE DEL CAUCA a intervalos planificados, (por lo menos una por periodo), para asegurar su conveniencia, suficiencia y eficacia. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios del SGSI, incluidos la política de seguridad y los objetivos de seguridad. Los resultados de las revisiones se deben documentar claramente y se deben llevar registros. Esta revisión cumplirá con los lineamientos establecidos en el procedimiento de revisión del Sistema Integrado de Gestión.

De la misma manera, las políticas de seguridad de la información, normas, procedimientos, estándares, controles, formatos y procedimientos, deben ser revisados y actualizados sistemáticamente, de forma periódica y planificada (mínimo una vez por periodo o cada vez que ocurra un cambio sustancial en los activos de información), por parte del Oficial de seguridad de la Información y por el Comité de Seguridad de la Información o en su defecto si se requiere una revisión independiente; se debe realizar por un organismo, empresa o consultor externo especializado, en cuyo caso debe seguir los lineamientos de la norma NTC-ISO/IEC 27001:2013 y debe ser realizada por alguien con las credenciales de AUDITOR LIDER (Lead Auditor) 27001 vigentes o Auditor CISA preferiblemente.

| ELABORÓ | REVISÓ | APROBÓ |
|---|---|---|
| **Nombre**: Ricardo Ramirez Sabogal y Luz Astrid Palma | **Nombre:** Oscar Julio Molano - Frank Alexander Ramírez O. | Comité Coordinador del SIG<br>Acta No. 008 |
| **Cargo**: Agentes de Cambio | **Cargo**: Lider de programa y oficial de seguridad de la información - Secretario de las TIC. | |
| Firma: | Firma: | |
| Fecha: 04-06-2019 | Fecha: 04-06-2019 | Fecha: 12 DIC 2019 |