Nombre de la política: **POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LOS SERVICIOS**

1. Declaratoria	La Gobernación del Departamento del Cauca se compromete, en el marco del Modelo de **Seguridad y Privacidad de la Información - MSPI de la entidad,** a implementar la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios, que permita proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en el mapa de procesos de la entidad, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir la ocurrencia de incidentes de seguridad digital, dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación masiva de las TIC, a través de políticas y programas para mejorar la calidad de vida de los Caucanos mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información - MSPI.
2. Objetivos	1. Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información. 2. Facilitar de manera integral la gestión de los riesgos de seguridad y privacidad de la información, de seguridad digital y la continuidad de las operaciones de los servicios. 3. Mitigar el impacto de los incidentes de seguridad y privacidad de la información, de seguridad digital de forma efectiva, eficaz y eficiente. 4. Establecer los mecanismos de aseguramiento físicos y digitales, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información de la Gobernación del Departamento del Cauca. 5. Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.

	6. Generar un cambio organizacional a través de la concienciación y apropiación de la seguridad y privacidad de la información y la seguridad digital. 7. Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la Información, Seguridad digital y Protección de la Información Personal. 8. Definir, operar y mantener el Plan de Continuidad de la Operación de los servicios de Gobernación del Departamento del Cauca.
3. Alcance	La Política de Seguridad de la Información, Seguridad Digital y Continuidad de los Servicios de la Gobernación del Departamento del Cauca, aplica a todos los procesos, niveles funcionales y organizacionales de las Secretarías, oficinas de la entidad, así como a funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones y/o actividades, compartan, utilicen, recolecten, procesen, intercambien o consulten su información con la entidad, así como a los entes de Control, entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información, independientemente de su ubicación. Así mismo, la presente política aplica para toda la información creada, procesada o utilizada por la Gobernación del Departamento del Cauca, sin importar el medio, formato, presentación o lugar en el cual se encuentre

4. Marco normativo	Decreto 1078 de 2015, modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1, incluye la seguridad de la información entre los principios de la Política de Gobierno Digital; de igual manera, en el artículo 2.2.9.1.2.1, se establece que la Política de Gobierno Digital se desarrollará a través de componentes y habilitadores transversales; Seguridad de la información, Arquitectura y Servicios Ciudadanos Digitales, que permite el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.
	Artículo 2.2.22.2.1 del Decreto 1083 de 2015, tal como fue sustituido por el Decreto 1499 de 2017, regula las políticas de Gestión y Desempeño institucional, entre las que se encuentra las de *"11. Gobierno Digital, antes Gobierno en Linea"* y *"12. Seguridad Digital"*
	CONPES 3995 del 1 de julio de 2020, establece la Política Nacional de confianza y Seguridad Digital por la creciente participación de ciudadanos en el entorno digital, la alta dependencia de la infraestructura digital y el aumento en el uso y adopción de nuevas Tecnologías de la Información y las Comunicaciones (TIC) que traen consigo una serie de riesgos e incertidumbres relacionados con la seguridad digital.
	Resolución 001519 de 24 de agosto del 2020, por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 de 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital y datos abiertos.
	Decreto 338 del 8 de marzo de 2022, por medio del cual se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de Seguridad Digital.

5. Términos y definiciones	**Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.
	Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.
	Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.
	Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.
	Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados
	Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.
	Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera
	Información: Datos relacionados que tienen significado para la entidad1 . La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada

6. Lineamientos	**POLÍTICAS ESPECÍFICAS DE MANEJO DE INFORMACIÓN** 1. **Política de Seguridad de los Recursos Humanos. El Comité Institucional de Gestión y Desempeño, el área de Gestión del Talento Humano de la Gobernación del Departamento del Cauca, deben desplegar esfuerzos para generar conciencia y apropiación en los servidores públicos, sobre sus responsabilidades en el marco del Modelo de Seguridad y Privacidad de la Información, con el fin de reducir el riesgo, el mal uso de las instalaciones y de los recursos tecnológicos, y así asegurar la confidencialidad, disponibilidad e integridad de la información y activos de información.** **PARÁGRAFO**: Con el mismo fin, el Área de Gestión del Talento Humano y el Grupo de Contratación de la Gobernación del Departamento del Cauca incluirá en las minutas de los contratos y convenios, cualquiera que sea su naturaleza o modalidad, cláusulas y

obligaciones para el cumplimiento de la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios, las cuales deberán ser divulgadas a través de los supervisores de los contratos y responsables de procesos a proveedores, a operadores y todas aquellas personas o terceros que en razón del cumplimiento de sus funciones y obligaciones compartan, utilicen, recolecten, procesen, intercambien o consulten su información de la entidad.

El Área de Gestión del Talento Humano y/o el Grupo de Contratación realiza el proceso de desvinculación, licencias, vacaciones o cambio de labores de los servidores públicos y contratistas llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin, así mismo, los directores, jefes, supervisores de contrato o líderes deben informar la desvinculación o cambio de labores de acuerdo con los procedimientos, está información debe ser entregada oportunamente al proceso de TI.

El incumplimiento o violación de las políticas de seguridad de la información de la entidad, por parte de los colaboradores o terceros, se les aplicará lo establecido en el proceso de investigaciones disciplinarias penales.

La entidad debe incorporar los roles y responsabilidades en seguridad de la información dentro de las funciones y obligaciones contractuales de los Colaboradores y terceros.

2. **Política de dispositivos móviles:** Los funcionarios y contratista o terceros no están autorizados a cambiar la configuración, ni la instalación/desinstalación de las aplicaciones móviles de los dispositivos móviles institucionales que se le entreguen como recurso para la ejecución de sus obligaciones o funciones.

Es responsabilidad del servidor público al que se le asignó el dispositivo móvil evitar la instalación de programas desde fuentes desconocidas, evitar el uso de redes inalámbricas públicas, y mantener desactivadas las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados. Los servidores públicos deben evitar conectar los dispositivos móviles institucionales a puertos USB de computadores públicos, hoteles o cafés internet, terminales, y demás sitios de acceso público.

Los servidores públicos y contratistas deben notificar sobre los dispositivos móviles institucionales con sospecha de infección por malware al personal técnico responsable de la entidad para el proceso de análisis, evaluación y tratamiento.

La entidad establece las condiciones para el uso seguro de los dispositivos móviles institucionales (portátiles, teléfonos inteligentes, tabletas, entre otros), que hagan uso de servicios de la entidad como son: establecer contraseñas de acceso robustas, cifrar la información almacenada, mantener el dispositivo móvil con el sistema operativo siempre actualizado y con un antivirus activo.

3. **Política de Trabajo en Casa:** La entidad establece los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos y contratistas de la entidad, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.

La entidad revisa la seguridad física y del entorno del sitio en casa donde se va a trabajar, con el fin de proteger la confidencialidad, integridad y disponibilidad.
Toda información gestionada por la entidad, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales con la entidad.
La entidad brinda los lineamientos de seguridad digital para la protección de la información a la que se tiene acceso, se procesa o almacena en lugares en los que se realiza Trabajo en Casa y se hace uso de los recursos tecnológicos autorizados por la entidad para el desarrollo de las actividades de Trabajo en Casa. (Regulado trabajo en casa y trabajo remoto, normatividad distinta tener muy en cuenta)

4. **Política de Gestión de Activos:** El Área de Gestión del Talento Humano, el Grupo de Bienes y Servicios con el acompañamiento permanente del Grupo de Gestión Tecnológica y Tics, establecerá y divulgará los lineamientos específicos para la identificación, clasificación, valoración, rotulado y buen uso de los activos de información. Es responsabilidad del líder de proceso, jefe de área o director, la identificación y reporte de nuevos activos de información, así mismo mantener actualizada la valoración de estos, con el objetivo de garantizar su protección. Dichos lineamientos se impartirán teniendo en cuenta los siguiente literales, que serán consolidados y publicados.

a. Inventario de Activos: Los activos del Departamento del Cauca, deben ser identificados, clasificados, valorados y controlados para garantizar su uso, protección y recuperación ante desastres. Por tal motivo, la Oficina de Gestión Tecnológica, diseñará una metodología con los lineamientos necesarios para llevar el inventario de los activos de información, discriminado por procesos y dependencia, tipo, nivel de criticidad, clasificación, ubicación, responsable, custodio, y demás atributos que la entidad defina; Los servidores públicos y contratistas deben hacer la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual o vinculación con la entidad.
b. Protección: Con el objetivo de establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información generada en el marco de sus funciones se encargarán de proteger la información, así como de mantener y actualizar el inventario de activos de información relacionados con sus servicios (información física o digital, software, hardware y recurso humano), bajo los parámetros que establezca la Oficina de Gestión Tecnológica. Al establecer propietarios de la información, estos deben garantizar que todos los activos de información reciban nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y/o requerimientos legales de retención.
c. Archivos de Gestión: El Comité Institucional Gestión y Desempeño, el área de Gestión del Talento Humano y Grupo Archivo General, deberán implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de acuerdo con las Tablas de Retención Documental, con el fin de proteger y

conservar la confidencialidad, integridad y disponibilidad de la información física y digital de la Gobernación del Departamento del Cauca.

d. Clasificación de la Información: El Comité Institucional de Gestión y Desempeño, el Área Gestión del Talento Humano, el Grupo de Archivo General con acompañamiento del Grupo de Gestión Tecnológica y Tics, deberán establecer una metodología para la clasificación y rotulado de la información de la Gobernación del Departamento del Cauca, en el marco de la Ley 594 de 2000 (Ley General de Archivos), la Ley 1712 de 2014, reglamentada por el Título 1 de la Parte 1 del Libro 2 del Decreto 1081 de 2015 y el Decreto 1080 de 2015 y demás normatividad que reglamente la clasificación de información de las entidades públicas del país. Así mismo, el Grupo de Gestión Tecnológica y Tics implementará una herramienta informática que permita rotular la información digital. De igual forma, el Comité Institucional de Gestión y Desempeño y el Área de Gestión del Talento Humano desarrollarán mecanismos para rotular la información física, de acuerdo con la metodología establecida.

5. Política de Control de Acceso: Los propietarios de los activos de información, teniendo en cuenta el tipo de activo y en supervisión de la oficina de Gestión Tecnológica; deberán establecer medidas de control de acceso a la información, nivel de red, sistema operativo, sistemas de información, servicios de tecnologías e infraestructura física (instalaciones y oficinas), revisión periódica del acceso otorgado, y desactivación o eliminación de las cuentas de usuario una vez finalizada la relación contractual. Todos los servidores públicos y contratistas con acceso a un sistema de información o a la red informática institucional, dispondrán de una única autorización de acceso compuesta de identificador de usuario y contraseña. Las credenciales de acceso (usuario y contraseña) son de uso personal e intransferible y es responsabilidad de cada usuario velar por el uso de las credenciales asignadas y serán responsables de las acciones realizadas por el usuario que les ha sido asignado. Todo esto con el fin de mitigar riesgos asociados al acceso a la información, infraestructura tecnológica e infraestructura física de personal no autorizado y así propender por salvaguardar la integridad, disponibilidad y confidencialidad de la información de la gobernación del Departamento del Cauca.

6. Política de Cifrado: La Oficina de Gestión Tecnológica pondrá a disposición de los usuarios herramientas que permitan el cifrado de la información clasificada y reservada para proteger su confidencialidad, integridad y disponibilidad. El cifrado de la información será liderado por el dueño y responsable del proceso de acuerdo con la clasificación de la información susceptible de ser cifrada. La clasificación de la información nos ha de servir para saber qué información debe ser cifrada para garantizar su confidencialidad e integridad. Dicha información puede ser:
   - Información sensible, de carácter personal o confidencial.
   - Registros con credenciales de autenticación.

- Información almacenada en dispositivos personales o de terceros (incluidos los servicios de nube pública o privada) que carecen de los controles de seguridad adecuados.
- Información transferida a través de redes de telecomunicación no confiables o en soportes de almacenamiento físicos no protegidos adecuadamente.

Uso de firma electrónica: Se hará uso de la firma electrónica en aquellos escenarios en los que sea imprescindible garantizar la autenticidad y el no repudio de la información, como para realizar trámites con las Administraciones Públicas o emitir facturas. De acuerdo con la disponibilidad de recursos se tendrá que elegir qué tipo de certificado de representación legal que se quiere implantar:

- Certificado de persona jurídica;
- Certificado de pertenencia a empresa;
- Certificado de representante;
- Certificado de factura electrónica.

Se debe seleccionar el prestador de servicios que generará nuestros certificados. Además, controlaremos: periodo de validez, posibilidad de revocación, cumplimiento con la legislación (prestadores cualificados) y gestión de su almacenamiento. Por lo cual establece técnicas criptográficas y cifrado como son: Cifrado de la información cuando se requiere transferir o almacenar información sensible o crítica, uso de protocolos seguros para las redes Wifi, uso de protocolo HTTPS con un nivel de cifrado actualizado. El acceso remoto a la red y los sistemas de información de la entidad desde una red externa será a través de conexiones seguras.

7. **Política de Privacidad:** La Gobernación del Departamento del Cauca, deberá disponer, a través del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, de los controles necesarios para la protección de la información de los servidores públicos, contratistas y partes interesadas externas, en los términos de la Ley 1581 de 2012 y sus decretos reglamentarios, así como la política de tratamiento de datos personales de la gobernación del Departamento del Cauca.

PARÁGRAFO 1. Mientras se definen los roles en el marco de la presente política, el rol de Oficial de Seguridad y Privacidad de la Información en la Gobernación del Cauca será ejercido por: el servidor público líder del Grupo de Gestión Tecnológica (Secretaría General), el servidor público líder de Servicios Informáticos del Sector Educativo SISE (Secretaría de Educación y Cultura) y el servidor público líder del Programa Proceso de Gestión Administrativa y Financiera - Gestión de Insumos (Secretaría de Salud) o quien delegue el Representante Legal de la entidad.

PARÁGRAFO 2. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, deberá diseñar un formato de autorización y uso de datos personales, así como su

tratamiento, en lo que respecta al uso de datos semiprivados, privados y sensibles; dicho formato debe ser claro y detallado en lo referente a la recolección de la información de los servidores públicos y contratistas de la Gobernación del Departamento del Cauca; formato que será aprobado por la Oficina Asesora Jurídica y deberá ser firmado por todos los servidores públicos y contratistas como parte de sus obligaciones.

PARÁGRAFO 3. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, diseñará y actualizará los formatos de autorización, por parte de los ciudadanos, de la captación y uso de imágenes, videos o cualquier medio audiovisual, de conformidad con lo dispuesto en las normas vigentes sobre protección de datos personales, en especial la Ley 1581 de 2012 y el Decreto 1074 de 2015, asi como su autorización libre, expresa e inequívoca a la Gobernación del Departamento del Cauca o a quien éste autorice o encargue, para el uso del recurso audiovisual en el marco del cumplimiento de su misión. Los formatos deberán prever la opción en que el ciudadano sea menor de edad y se deberá establecer un procedimiento para el caso en que el ciudadano no autorice dicho tratamiento. Dichos formatos deberán ser revisados y aprobados, en su orden, por la Oficina de Prensa y por la Oficina Asesora Jurídica.

PARÁGRAFO 4. La toma de material audiovisual a los ciudadanos mayores o menores de edad sólo se podrá realizar por los servidores públicos o contratistas avalados por la Oficina de Prensa y en cumplimiento de las funciones de acompañamiento a programas propios de la gobernación del Departamento del Cauca o donde éste fuere invitado de manera oficial. Los datos que se recolecten sólo podrán ser tratados para el cumplimiento de la finalidad para la cual se ha dispuesto el tratamiento.

8. **Política de seguridad física del entorno:** La Gobernación del Departamento del Cauca, a través del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, debe adoptar medidas para la protección del perímetro de seguridad de sus instalaciones físicas para controlar el acceso y permanencia del personal en las oficinas, instalaciones y áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones), con el fin de mitigar los riesgos, amenazas externas, ambientales y evitar afectación a la confidencialidad, integridad y disponibilidad de la información de la entidad.

PARÁGRAFO 1. El Comité Institucional de Gestión y Desempeño, el Área de Gestión del Talento Humano bajo la supervisión del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, deberá garantizar la protección de los datos, semiprivados, privados y sensible recolectados de los servidores públicos, contratistas y visitantes, en lo que refiere el artículo 9 del presente decreto y establecer mecanismos alternativos para quienes no autorizan el tratamiento de sus datos.

PARÁGRAFO 2. Todos los servidores públicos, contratistas y visitantes que se encuentren en las instalaciones físicas de la Gobernación del Departamento del Cauca deben estar debidamente identificados, con un carné, documento o distintivo que acredite su tipo de vinculación, en casó de carné debe portarse en un lugar visible.

PARÁGRAFO 3. El personal de empresas, cooperativas o entidades que desempeñen funciones de forma permanente o eventuales en las instalaciones de la Gobernación del Departamento del Cauca, deben estar identificados con carné y chalecos o distintivos de la empresa o entidad.

9. **Política de seguridad de las operaciones:** La Oficina de Gestión Tecnológica de la Gobernación del Departamento del Cauca, será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación. Así mismo, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información trabajará a través del comité institucional, para que los cambios efectuados sobre los recursos tecnológicos y sistemas de información en ambientes de producción sean controlados y debidamente autorizados, así mismo implementará mecanismos para controlar la información en los ambientes de desarrollo y prueba. De igual manera, proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con el crecimiento de la entidad, al igual que desarrollará mecanismos de contingencias y recuperación ante desastres con el fin de propender por la disponibilidad de los servicios de TI en el marco de la operación TI de la Gobernación del Departamento del Cauca.

La Oficina de Gestión Tecnológica, deberá realizar y mantener copias de seguridad de la información de la entidad en medio digital y el Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, velará que ésta sea reportada por el responsable de esta o líder de proceso, con el objetivo de recuperarla en caso de cualquier tipo de falla. La Oficina de Gestión Tecnológica efectuará las copias respectivas, de acuerdo con el esquema definido previamente, en un procedimiento que enmarque la gestión de las copias de seguridad de la información digital, sistemas de información, bases de datos y demás recursos tecnológicos de la entidad.

El diseño de este procedimiento se hará bajo la dirección de la Oficina de Gestión Tecnológica, con el apoyo de los líderes de proceso y deberá estar alineado con la gestión documental de la entidad, con el fin de determinar la información a respaldar, la periodicidad, los tiempos de retención, recuperación, restauración y los mecanismos para generar el menor impacto en la prestación del servicio durante el tiempo de la indisponibilidad de la información.

PARÁGRAFO. En el evento que alguna dependencia opere una plataforma tecnológica fuera de las instalaciones físicas y en el marco de las funciones misionales u operacionales de la Gobernación del Departamento del Cauca, deberá cumplir con lo establecido en la presente política y los procedimientos dispuestos por el Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, para tal fin.

10. **Política de Seguridad de las Comunicaciones:** La Oficina Gestión Tecnológica, establecerá los mecanismos necesarios para proveer la disponibilidad de las redes y de los servicios tecnológicos que dependen de ellas; así mismo, dispondrá y monitorea los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información de la Gobernación del Departamento del Cauca.

La Oficina Asesora de Planeación establecerá mecanismos estratégicos para que el intercambio de información con las partes interesadas internas o externas, se realice asegurando su integridad. En el evento que los acuerdos de intercambio de información requieran del desarrollo de servicio web (web service) o de cualquier otro medio tecnológico, el intercambio deberá realizarse con los controles criptográficos definidos en el artículo 8° de este decreto y será coordinado por la Oficina Gestión Tecnológica con los mecanismos establecidos para tal fin.

PARÁGRAFO. Como parte de sus términos y condiciones iniciales de trabajo, funciones u obligaciones, los servidores públicos o contratistas del Departamento del Cauca, sin importar su nivel jerárquico, firmarán un acuerdo o compromiso de confidencialidad y no divulgación que será elaborado por el área de contratación de la Gobernación del Departamento del Cauca con el apoyo del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces según el tipo de vinculación, en lo que respecta a la información de la entidad. Dicho documento original será conservado y archivado en forma segura en la historia laboral de los servidores públicos y en la carpeta de los procesos contractuales para el caso de los contratistas.

En el caso de persona jurídica proveedora de servicios para la gobernación del Departamento del Cauca, en la respectiva carpeta del contrato deberá reposar el acuerdo o compromiso de confidencialidad y no divulgación debidamente suscrita por el representante legal de dicha persona.

11. **Política de seguridad para la adquisición, desarrollo y mantenimiento de sistemas:** La Oficina de Gestión Tecnológica velará porque el desarrollo interno y externo de los sistemas de información, cumplan con los requerimientos de seguridad adecuados para la protección de la información digital de la entidad, para lo cual establecerá una metodología que detalle los requerimientos de seguridad para el desarrollo, pruebas, puesta en producción y mantenimiento de los sistemas de información.

En el marco del Plan Estratégico de Tecnologías de la Información (PETI), la Oficina de Gestión Tecnológica, es la única dependencia de la entidad con la capacidad de adquirir,

desarrollar e implementar soluciones tecnológicas para la Gobernación del Departamento del Cauca, así como de avalar la adquisición y recepción de software de cualquier tipo en el marco de convenios y contratos con terceros, conforme a los requerimientos de las dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en la Gobernación del Departamento del Cauca.

En consecuencia, cualquier software que opere en la Gobernación del Departamento del Cauca deberá contar con la autorización de la Oficina de Gestión Tecnológica y deberá reportarse y entregarse cumpliendo con los lineamientos técnicos y presupuestales de dicha oficina, con el fin de salvaguardar la información, brindar el soporte y demás procesos técnicos que permitan su recuperación en caso de algún incidente o siniestro.

PARÁGRAFO. En caso de que alguna dependencia adquiera, desarrolle o actualice sistemas de información dentro del ejercicio misional u operacional la Gobernación del Departamento del Cauca, deberá cumplir con lo establecido en la presente política. Para los desarrollos de software contratados por el Departamento del Cauca y en lo referente a derechos de autor y propiedad intelectual, se ejecutarán de conformidad con la Guia de Propiedad Intelectual en la Contratación Pública expedida por la Agencia Nacional de Contratación Pública - Colombia Compra Eficiente.

12. **Política de seguridad para relación con proveedores:** La Gobernación del Departamento del Cauca a través del Grupo Interno de Trabajo de Contratación, establecerá, en el manual de contratación, las disposiciones necesarias para asegurar que la información que se genere, custodie, procese, comparta, utilice, recolecte, intercambie o a la que se tenga acceso con ocasión del contrato, se utilice dentro del marco de la seguridad y privacidad de la información por parte de los proveedores. En el mismo sentido y a través del seguimiento a la ejecución, se garantizará que los supervisores en conjunto con la Oficina de Control Interno como sujeto de inspección, sean los responsables de aplicar las políticas y procedimientos de seguridad de la información durante la ejecución de los contratos, estos lineamientos deberán ser comunicados a los proveedores con el apoyo de la Oficina Asesora de Prensa.

PARÁGRAFO. Tratándose de relaciones contractuales de la Gobernación del Departamento del Cauca, estas disposiciones deberán ser incorporadas en los términos, minutas o acuerdos con los que se relacione estos, a efectos de garantizar su implementación.

13. **Política de gestión de incidentes de seguridad de la información:** La Gobernación del Departamento del Cauca, a través del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, promoverá entre los servidores públicos y contratistas de la entidad, el reporte y seguimiento de incidentes relacionados con la seguridad de la información y sus medios. Así mismo, asignará responsables para el tratamiento de

estos, quienes investigarán y solucionarán los incidentes reportados, de acuerdo con su sana crítica.

El Representante legal será el autorizado para reportar incidentes de seguridad ante las autoridades de defensa nacional, policía, fiscalía y de control; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas, medios de comunicación o la ciudadanía. La delegación de esta potestad podrá ser formal, por medio de acto administrativo.

14. **Política de la continuidad de la operación de los servicios:** La Gobernación del Departamento del Cauca, dispondrá los planes necesarios para la continuidad de la operación de los servicios, los cuales serán operados por los líderes de los procesos. El Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, la Oficina Asesora de Planeación o Gestión Organizacional y la Oficina de Gestión Tecnológica liderarán conjuntamente la Continuidad de la Operación de los Servicios.

PARÁGRAFO. El Plan de Continuidad de los Servicios de la Gobernación del Departamento del Cauca, contendrá el Plan de Continuidad de Tecnologías y los Planes de Emergencia y Contingencia, así como cualquier estrategia orientada a la continuidad de la prestación del servicio de la Gobernación del Departamento del Cauca.

15. **Política de cumplimiento:** La Gobernación del Departamento del Cauca, a través del Oficial de Seguridad y Privacidad de la Información o quien haga sus veces, velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la seguridad y privacidad de la información, de acuerdo con lo establecido por el gobierno nacional, entre ellos los referentes a derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional, para lo cual dispondrá una Matriz de Requisitos Legales para su control y seguimiento.

16. **Política de seguridad de la información en la gestión de proyectos:** La Oficina de Planeación, deberá incluir los requerimientos y consideraciones en materia de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios en la metodología de gestión de proyectos de la entidad, garantizando que se implementen en las fases iniciales de los proyectos, en el mismo sentido, la Oficina de Control Interno deberá incluir dentro de su plan de auditorías la revisión de su cumplimiento e implementación.

PARÁGRAFO. El grupo de trabajo de Contratación debe velar que, en todos los estudios previos de los proyectos o contratos a celebrar la Gobernación del Cauca, se incluyan los requerimientos y consideraciones referentes a Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los servicios que se están contratando.

RESPONSABILIDADES DE LOS COLABORADORES FRENTE AL USO DE LOS SERVICIOS TECNOLÓGICOS

17. Política de seguridad digital: Todos los servidores públicos o contratistas que hagan uso de los recursos tecnológicos de La Gobernación del Departamento del Cauca tienen la responsabilidad de cumplir cabalmente las políticas establecidas para su uso aceptable; entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación de los servicios y, por ende, el cumplimento de la misión institucional. Para ello, deben acatar las siguientes disposiciones:

A) Del uso del correo electrónico. El correo electrónico institucional es una herramienta de apoyo a la ejecución de funciones y obligaciones de los servidores públicos y contratistas la gobernación del Departamento del Cauca cuyo uso se facilitará en los siguientes términos:

- El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la entidad es el asignado por la Oficina de Gestión Tecnológica, que cuenta con el dominio @cauca.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.
- El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional, en consecuencia, no puede ser utilizado con fines personales, económicos, comerciales o cualquier otro ajeno a los propósitos de la entidad.
- En cumplimiento de la iniciativa institucional del uso aceptable del papel y la eficiencia administrativa, se debe preferir el uso del correo electrónico al envío de documentos físicos, siempre que la ley lo permita.
- Los mensajes de correo están respaldados por la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones), la cual establece la validez de los mensajes de datos.
- La Oficina de Gestión Tecnológica implementará herramientas tecnológicas que prevengan la pérdida o fuga de información de carácter reservada o clasificada, de conformidad con la Ley 1712 de 2014.
- Se prohíbe el envio de correos masivos (más de 30 destinatarios) internos o externos, con excepción de los enviados por los despachos de la Gobernación del Departamento del Cauca, de la Secretaria General, Oficina Asesora de Prensa, Oficina Asesora de Planeación, Grupo de Gestión Organizacional, Grupo Archivo General, Dirección de Gobierno Digital, Área de Gestión del Talento Humano, así como de Grupo de Gestión Tecnológica y Tics, solamente en caso de ventana de mantenimientos de los servicios de TI. Los correos masivos deben cumplir con las características de comunicación e imagen corporativa.

	- Todo mensaje de correo electrónico enviado por la gobernación del Departamento del Cauca mediante plataformas externas deberá hacerse con la cuenta de la entidad y utilizando el dominio @cauca.gov.co, con el fin de que no sean catalogados como spam o suplantación de correo. - Para apoyar la gestión de correo electrónico de directivos, el titular debe solicitar a la mesa de servicios la delegación del buzón correspondiente, relacionando los colaboradores que podrán escribir o responder en nombre del titular, con el fin de mitigar la suplantación. - Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser inmediatamente reportado a la Oficina de Tecnologías de la Información a través de la Mesa de Servicios como incidente de seguridad según el procedimiento establecido, y deberán acatarse las indicaciones recibidas para su tratamiento, lo anterior, debido a que puede contener virus, en especial si contiene archivos adjuntos con extensiones.exe,.bat, .prg,.bak,.pif, o explícitas referencias no relacionadas con la misión de la entidad (como por ejemplo: contenidos eróticos, alusiones a personajes famosos). Está expresamente prohibido el envío y reenvío de mensajes en cadena. - La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o cualquier otra ajena a los fines de la entidad. - Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y que atenten contra la integridad moral de las personas o instituciones. - Está expresamente prohibido distribuir información oficial de carácter clasificada o reservada de la gobernación del Departamento del Cauca a otras entidades o ciudadanos sin la debida autorización del despacho de la Gobernación del Cauca, secretarios (as), de la Secretaría General, de la Oficina Asesora de Prensa, de la Oficina Asesora de Planeación, previa revisión de la Oficina Asesora de Prensa en caso de comunicados y Oficina Asesora de Planeación en caso de cifras oficiales. - El cifrado de los mensajes de correo electrónico institucional será necesario siempre que la información transmitida esté catalogada como clasificada o reservada en el inventario de activos de información o en el marco de la ley. - El correo electrónico institucional en sus mensajes debe contener una sentencia de confidencialidad, que será diseñada por la Oficina de Gestión Tecnológica con el apoyo de la Oficina Asesora de Prensa y avalada por la Oficina Asesora Jurídica, dicha sentencia debe reflejarse en todos los buzones con dominio @cauca.gov.co. - Está expresamente prohibido distribuir, copiar o reenviar información de la Gobernación del Departamento del Cauca a través de correos personales o sitios web diferentes a los autorizados en el marco de las funciones u obligaciones contractuales.

- Cuando un servidor público o contratista cesa en sus funciones o culmina la ejecución de contrato con la gobernación del Departamento del Cauca, no se le entregará copia de los buzones de correo institucionales a su cargo, salvo autorización expresa de Secretaría General, por orden judicial, por solicitud de la Oficina de Control Interno o Control Disciplinario como parte de un proceso de investigación.

La Gobernación del Departamento del Cauca, se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucional de todos sus servidores públicos o contratistas. Además, podrá realizar copias de seguridad del correo electrónico en cualquier momento sin previo aviso y limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información de la entidad o de terceros operados en la misma, previa solicitud expresa del nominador, ordenador del gasto, supervisor del contrato, jefe inmediato, secretario, Líder de oficina, jefe de Control Disciplinario o jefe del Grupo de Talento Humano a la Oficina de Gestión Tecnológica. Para ello, al inicio de la relación laboral o contractual se deberá comunicar a los funcionarios y contratistas que la gobernación del Departamento del Cauca realiza el referido monitoreo.

B) **Del uso de Internet:** La Oficina de Tecnologías de la Información, en conjunto con el Oficial de la Seguridad de la Información o quien haga sus veces, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía y funciones. Será responsabilidad de los colaboradores las siguientes, entre otras:

- Los servicios a los que un determinado usuario pueda acceder en Internet dependerán del rol o funciones que desempeña en la gobernación del Departamento del Cauca y para las cuales esté formal y expresamente autorizado por su jefe o supervisor y solo se utilizará para fines laborales.
- Abstenerse de enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.
- Abstenerse de acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por la política de navegación de la gobernación del Departamento del Cauca.
- Abstenerse de enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.
- Abstenerse de propagar intencionalmente virus o cualquier tipo de código malicioso.

La Gobernación del Departamento del Cauca, se reserva el derecho de monitorear los accesos y el uso del servicio de Internet, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro uso ajeno a los fines de la entidad.

C) Del uso de los recursos tecnológicos: Los recursos tecnológicos de la Gobernación del Departamento del Cauca son herramientas de apoyo a las labores y responsabilidades de los servidores públicos y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

- Los bienes de cómputo que provea la entidad se emplearán de manera exclusiva y bajo la completa responsabilidad del servidor público o contratista al cual han sido asignados, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas. Por tanto, no pueden ser utilizados con fines personales o por terceros no autorizados por la Oficina de Gestión Tecnológica, salvo que medie solicitud formal de los secretarios, jefes de oficina o coordinadores de grupos.
- Sólo está permitido el uso de software licenciado por la entidad y aquel que, sin requerir licencia, sea expresamente autorizado por la Oficina de Gestión Tecnológica.
- En caso de que el servidor público o contratista deba hacer uso de equipos ajenos a la Gobernación del Departamento del Cauca, éstos deberán cumplir con la legalidad del Software instalado, sistema operativo y antivirus licenciado, actualizado y solo podrá conectarse a la red de la Gobernación del Departamento del Cauca una vez esté avalado por la Oficina de Tecnologías de la Información.
- Los servidores públicos y contratistas deberán realizar y mantener las copias de seguridad de su información y entregarla a la entidad al finalizar la vinculación.
- Está expresamente prohibido el almacenamiento en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, archivos de vídeo, música y fotos que no sean de carácter institucional o que atenten contra los derechos de autor o propiedad intelectual de los mismos.
- Los servidores públicos y contratistas deberán utilizar las herramientas tecnológicas que proporcione la Oficina de Gestión Tecnológica para gestionar la información digital de la gobernación del Departamento del Cauca.
- No está permitido ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos o información física que pueda estar expuesta a daño parcial o total y, por ende, a la pérdida de la integridad de ésta.
- No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, salvo en aquellos casos autorizados.
- Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar o reparar sus componentes, son las designadas para tal labor por la Oficina de Gestión Tecnológica.
- La Oficina de Gestión Tecnológica realizará control y monitoreo sobre los dispositivos de almacenamiento externos como USB, CD-ROM, DVD, Discos Duros

externos, entre otros, con el fin de prevenir o detectar fuga de información clasificada y reservada.

- La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la Oficina de Gestión Tecnológica, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes de la entidad.

- La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, deberá ser informada de inmediato a la Oficina de gestión Tecnológica por el servidor público o contratista a quien se le hubiere asignado; en caso de que el equipo de cómputo sea propiedad la gobernación del Departamento del Cauca, deberá reportarse al supervisor, jefe de oficina o secretaría siguiendo los procedimientos establecidos para este tipo de siniestros, sin perjuicio de las acciones penales y disciplinarias que requiera adelantar según sea el caso.
- La pérdida de información deberá ser informada con detalle a la Oficina de Gestión Tecnológica, a través de un correo, como incidente de seguridad.
- Todo incidente de seguridad que comprometa la confidencialidad, integridad o disponibilidad de la información física o digital deberá ser reportado a la mayor brevedad a la Oficina de Tecnologías de la Información.
- La Oficina de Gestión Tecnológica es la única dependencia autorizada para la administración del software de la Gobernación del Departamento del Cauca, el cual no deberá ser copiado, suministrado a terceros ni utilizado para fines personales.
- Todo acceso a la red de la entidad, mediante elementos o recursos tecnológicos no institucionales, deberá ser informado, autorizado y controlado por la Oficina de Gestión Tecnológica.
- La conexión a la red wifi institucional para servidores públicos y contratistas deberá ser administrada desde la Oficina de gestión Tecnológica mediante un SSID (Service Set Identifier) único; la autenticación deberá ser con usuario y contraseña de directorio activo.
- La conexión a la red institucional para visitantes deberá tener un SSID y contraseñas administradas por la Oficina de Gestión Tecnológica, las contraseñas deberán cambiar los lunes de cada semana y solo estarán disponibles en el horario laboral definido.
- El acceso a la red inalámbrica para servidores públicos y contratistas estará disponible para sus equipos personales, teniendo en cuenta las capacidades técnicas, contractuales y lineamientos de seguridad establecidos por la gobernación del Departamento del Cauca.
- Los equipos deben quedar apagados cada vez que el servidor público o contratista no se encuentre en la oficina o durante la noche, esto, con el fin de proteger la

seguridad y distribuir bien los recursos de la entidad, siempre y cuando no vaya a realizar actividades vía remota.

- Todo dispositivo móvil personal que requiera acceder a los servicios tecnológicos de la entidad debe acogerse a las políticas de "Trae tu propio dispositivo".
- Las herramientas corporativas instaladas en los dispositivos móviles personales serán gestionadas por la Oficina de Gestión Tecnológica con el fin de proteger la confidencialidad, integridad y disponibilidad de la información de la entidad, garantizando el cumplimiento del artículo 9 del presente decreto.

D) Del uso de los sistemas o herramientas de información: Todos los servidores públicos y contratistas de la Gobernación del Departamento del Cauca son responsables de la protección de la información a la que acceden y procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido, para lo cual se dictan los siguientes lineamientos:

- Las credenciales de acceso a la red y a los recursos informáticos (Usuario y Clave) son de carácter estrictamente personal e intransferible; los servidores públicos y contratistas no deben revelarse a terceros, ni utilizar claves ajenas.
- Todo servidor público y contratista es responsable del cambio periódico de su clave de acceso a los sistemas de información o recursos informáticos.
- Todo servidor público y contratista es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.
- En ausencia del servidor público o contratista, el acceso a la estación de trabajo le será bloqueada con una solicitud a la Oficina de Gestión Tecnológica con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. El Área de Gestión del Talento Humano debe reportar de inmediato, cualquier tipo de novedad de servidores públicos, a su vez los supervisores de contrato deben reportar oportunamente todas las novedades del contratista.
- Cuando un servidor público o contratista cesa sus funciones o culmina la ejecución del contrato con la Gobernación del Departamento del Cauca, todos los privilegios sobre los recursos informáticos otorgados le serán suspendidos inmediatamente; la información que estos ostenten será almacenada en los repositorios de la entidad.
- Cuando un servidor público o contratista cesa sus funciones o culmina la ejecución de contrato con la Gobernación del Departamento del Cauca, el jefe inmediato o supervisor es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual, de acuerdo con la normativa vigente.
- Cuando un servidor público o contratista cesa sus funciones o culmina la ejecución del contrato con la Gobernación del Departamentos del Cauca deberá tramitar a paz y salvo, de acuerdo con el procedimiento establecido por la entidad.

	- Todos los servidores públicos y contratistas de la entidad deben dar estricto cumplimiento a lo estipulado en la Ley 23 de 1982 "Sobre derechos de autor", la Decisión 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que adicione, modifique o reglamente la materia. **ARTÍCULO VIGÉSIMO CUARTO:** lineamientos de las políticas de seguridad de la información. Todas las políticas identificadas en este documento se deberán desarrollar de manera detallada y clara en la Declaración de Aplicabilidad y en el Manual de Políticas de Seguridad de la Información.

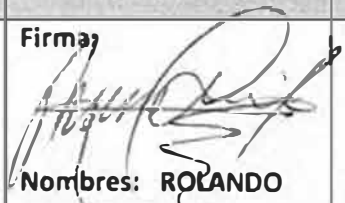
7. Estrategias para combatir el riesgo - Tratamiento de los riesgos	**Evitar el riesgo:** se toman medidas encaminadas a evitar la materialización del riesgo.
	Reducir el riesgo: Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante Transferencia o Mitigación de este. **Transferir:** Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional. **Mitigar:** Después de realizar un análisis y considerar los niveles de riesgo, se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.
	Aceptar el riesgo: Después de realizar un análisis y considerar los niveles de riesgo, se determina asumir el mismo, conociendo los efectos de su posible materialización
	Evitar el riesgo: Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo

8. Criterios para definir el nivel de Probabilidad	**Frecuencia de la Actividad**		**Probabilidad**
	Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
	Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
	Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
	Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
	Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

	VALORES CALIFICACIÓN DE IMPACTO PARA RIESGO DE GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN		
9. Niveles o criterios para calificar el impacto	**DESCRIPTOR**	**AFECTACIÓN ECONÓMICA**	**REPUTACIONAL**
	LEVE 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
	MENOR 40%	Entre 10 y 50 SMLMV.	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y / o de proveedores.
	MODERADO 60%	Entre 50 y 100 SMLMV.	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
	MAYOR 80%	Entre 100 y 500 SMLMV.	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
	CATASTRÓFICO 100%	Mayor a 500 SMLMV.	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

	RESPONSABLES	
9. Monitoreo, revisión y seguimiento	**Línea estratégica**	**Comité Institucional de Gestión y Desempeño.** o Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información. o Recomendaciones de mejoras a la política de operaciones para la administración del riesgo. **Comité institucional de Coordinación de Control Interno.** o Revisar la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios. o Aprobación de la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y de los Servicios
	1ra. Línea de defensa	**Responsables de Procesos – Responsables de Proyectos Planes y Programas.** o Asegurar que al interior de cada proceso y procedimientos se tenga el conocimiento de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios, reportando a la segunda línea sus avances y dificultades. o Delegar, por parte del responsable del proceso, el profesional que se encargará de la aplicación y socialización de la política.

		o Desarrollar ejercicios para establecer la confidencialidad, disponibilidad y privacidad de la información en todos sus procesos y procedimientos. o Revisar las acciones y planes de mejoramiento en la Política para llevar los procesos de manera segura y confiable. **Los responsables del proceso deben:** o Registrar los avances y controles de los resultados de la Política y evidenciar, para analizar y realizar acciones de mejora. o Evaluar con el equipo de trabajo la responsabilidad y resultados de la Política General de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de los Servicios. o Comunicar al equipo de trabajo resultados y la gestión de la política. o Asegurar que se documente las acciones realizadas por la política en el plan de mejoramiento.
	2da. Línea de defensa	**Responsable: Gestión Tecnológica y TIC** o Socializar la implementación de la Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los Servicios con el apoyo del Grupo de Gestión Organizacional y Control Interno. o Supervisar los controles de la primera línea de defensa. o Acompañar y orientar a todos los líderes de procesos para el conocimiento y aplicación de la Política. o Supervisar la adopción de las buenas prácticas para la implementación de la Política en los procedimientos y procesos de la Gobernación del Cauca. o Apoyar cada caso o identificación de riesgos que se presenten en los procesos y procedimientos de la entidad.
	3ra. Línea de defensa	**Responsable: Oficina de Control Interno.** o Supervisar que la primera línea identifique, analice, valore e implemente la Política garantizando los tres pilares de la seguridad de la Información (confidencialidad, integridad y disponibilidad). o Llevar a cabo un seguimiento a la Política con el Plan Anual de Auditoría y reportar los resultados. o Recomendar mejoras a la Política General de Seguridad de la Información, Seguridad Digital y Continuidad de los Servicios.

CONTROL DE CAMBIOS AL DOCUMENTO			
Versión / Fecha dd/mm/aaaa	**Descripción de Cambios**		**Responsable del Cambio**
Versión 01 Fecha: 26/12/2023	No aplica para la primera versión		N.A.
ELABORADO POR:	**APROBADO POR:**	**REVISADO POR:**	**CODIFICADO POR:**
Firma:  **Nombres: DIEGO ARMANDO RUALES CARVAJAL** **Cargos:** Profesional equipo de Apoyo Gestión Tecnológica **Fecha:** 10/09/2022	**Firma:** **Nombres: Comité Institucional de Gestión y Desempeño** **Cargo:** Acta # 5 de 2022 **Fecha:** 4/10/2022	**Firma:**  **Nombres: ROLANDO DANILO VELASCO MORALES** **Cargos:** Profesional Universitario Gestión Tecnológica **Fecha:** 20/09/2022	**Firma:** **Nombres: YOLIMA RECALDE CASTRO** **Cargos:** Tecnóloga equipo de Apoyo Gestión Organizacional **Fecha:** 30/09/2022
Firma: **Nombres:** N.A. **Cargo:**	**Firma:** **Nombres:** N.A. **Cargo:**	**Firma:**  **Nombres: SANDRA XIMENA ANTE M.** **Cargos:** Profesional Universitario Gestión Organizacional **Fecha:** 20/09/2022	**Firma:** **Nombres:** N.A. **Cargo:**
Firma: **Nombres:** N.A. **Cargo:**	**Firma:** **Nombres:** N.A. **Cargo:**	**Firma:**  **Nombres: SANDRA XIMENA MONTILLA** **Cargos:** Profesional Universitario Secretaría de Salud **Fecha:** 20/09/2022	**Firma:** **Nombres:** N.A. **Cargo:**

Firma:	Firma:	Firma:	Firma:
Nombres: N.A. Cargo:	Nombres: N.A. Cargo:	Nombres: MERY JHOHANNA CHAMORRO Cargos: Profesional Universitaria Secretaria de Educación Fecha: 15/09/2022	Nombres: N.A. Cargo: