POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Departamento del Valle del Cauca

Gobernación

CODIGO: PO-M11-P1-03

Versión: 02

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

Tabla de contenido

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

1. OBJETIVO

Establecer lineamientos para el manejo adecuado de los activos de la información a través de las herramientas de gestión de seguridad de la información, garantizando la confidencialidad, integridad y disponibilidad de los datos en la Gobernación del Valle del Cauca, enmarcando en la buena gestión para la continuidad de las actividades administrativas, operativas y/o logísticas, teniendo en cuenta los procesos, programas, proyectos, objetivos de negocio, requisitos legales vigentes y su aplicación para los funcionarios, contratistas y terceros involucrados con la entidad que tengan cualquier tipo de acceso a la información de la entidad, fortaleciendo así la gestión para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) y la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) de tal manera que permita mitigar el impacto de los riesgos generados en la operación de los procesos.

2. ALCANCE

La Política de Seguridad de la Información inicia con el ciclo de vida de los activos de información definiendo los lineamientos, controles y directrices para el Sistema de Gestión de Seguridad de la Información (SGSI) de la Gobernación del Valle del Cauca, incluye a los funcionarios, contratistas y terceros involucrados con la entidad que accedan a los sistemas de información y finaliza con la gestión de la mejora continua para garantizar controles que permitan lograr niveles adecuados de seguridad para salvaguardar la confidencialidad, integridad y disponibilidad de la información.

3. RESPONSABLES

Los funcionarios, contratistas y terceros involucrados con la entidad a la Gobernación del Valle del Cauca son responsables del cumplimiento de la Política de Seguridad de la Información definida en este documento, con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información en cada una de las actividades realizadas en los planes, programas y/o proyectos que permita el adecuado uso de los activos de información.

4. DEFINICIONES

Activo de información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, entre otros) que tenga valor para la organización.

Activo de información digital: Cualquier información en formato electrónico que tenga valor para la Gobernación, incluyendo datos personales, información financiera, propiedad intelectual, registros públicos, software, hardware, servicios en la nube, etc.

Amenaza de seguridad: Evento o acción que podría comprometer la seguridad de los activos de información digital, como ataques cibernéticos (malware, phishing, ransomware,

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

denegación de servicio), errores humanos, fallos de hardware o software, desastres naturales, etc.

Autenticación: Proceso de verificación de la identidad de un usuario, dispositivo o sistema antes de permitirle acceder a recursos digitales protegidos.

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

Control de acceso: Conjunto de medidas y procedimientos que regulan quién puede acceder a recursos digitales, qué acciones pueden realizar y bajo qué condiciones; garantizando la confidencialidad, integridad y disponibilidad de la información.

Control de seguridad: Medida implementada para reducir el riesgo de una amenaza de seguridad digital, como firewalls, antivirus, contraseñas seguras, cifrado, autenticación de dos factores, copias de seguridad, actualizaciones de software, etc.

Disponibilidad: Propiedad de la información que asegura su acceso y utilización oportuna cuando es requerida, garantizando así el funcionamiento ininterrumpido de las operaciones y servicios que dependen de ella..

Gestión de riesgos: Proceso sistemático de identificación, análisis, evaluación y tratamiento de los riesgos que amenazan la seguridad de la información y los sistemas, con el objetivo de minimizar su impacto y probabilidad de ocurrencia.

Incidente de seguridad de la información: Evento o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información pública: Toda información en posesión, bajo control o custodia de un sujeto obligado (entidades públicas) se presume pública, por lo tanto, cualquier persona tiene derecho a acceder a ella.

Información pública clasificada: Es aquella información pública que, por disposición expresa de la ley, requiere un tratamiento especial para su divulgación, ya sea por razones de seguridad nacional, protección de derechos fundamentales o por afectar el debido proceso en actuaciones administrativas, entre otros motivos.

Información pública reservada: Es aquella información que no puede ser divulgada porque su publicidad puede causar daño a intereses públicos, como la seguridad nacional, las relaciones internacionales o la defensa nacional. Solo la Constitución o la ley pueden definir qué información es reservada.

Integridad: Propiedad de la información que garantiza su exactitud, consistencia y fiabilidad a lo largo del tiempo, asegurando que no ha sido modificada, alterada o destruida sin autorización.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

Mejora continua: Proceso cíclico de revisión, análisis y optimización constante de las medidas de seguridad digital, adaptándose a las nuevas amenazas y vulnerabilidades para garantizar la protección de la información y los sistemas.

No repudio: Garantía de que el autor de una acción o comunicación digital no puede negar su participación, ya que existen pruebas irrefutables de su origen y/o recepción.

Riesgo de seguridad: Probabilidad de que una amenaza explote una vulnerabilidad y cause daño a los activos de información digital.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de gestión de seguridad de la información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

Vulnerabilidad: Debilidad en un sistema, red, aplicación, proceso o comportamiento humano que puede ser explotada por una amenaza.

5. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 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 del Cauca, mediante la adopción e implementación de un Modelo de Seguridad y Privacidad de la Información enmarcado en un Sistema de Gestión de Seguridad de la Información, pretende 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 un Sistema de Gestión de Seguridad de la Información para proteger sus activos de información, comprometiéndose a:

- Gestionar los riesgos de los activos de información, teniendo en cuenta el nivel de tolerancia al riesgo de la entidad.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

- Implementar una gestión integral de riesgos basada en controles físicos y digitales orientados a la prevención de incidentes.
- Aplicar políticas de seguridad de alto nivel y políticas complementarias, de acuerdo con lo establecido en la norma ISO/IEC 27001, para asegurar la confidencialidad, integridad y disponibilidad de la información de la entidad.
- Fomentar la cultura y la toma de conciencia en funcionarios, contratistas y terceros involucrados con la entidad sobre la importancia de la seguridad de la información.
- Definir, compartir, publicar y aceptar las responsabilidades frente a la seguridad de la información por parte de cada funcionario, contratista y tercero.
- Proteger la información generada, procesada o resguardada por los procesos de la entidad, su infraestructura tecnológica y los activos de información frente a riesgos derivados de accesos otorgados a funcionarios, contratistas y terceros involucrados con la entidad, o como resultado de servicios internos en outsourcing.
- Mitigar los incidentes de seguridad y privacidad de la información de manera efectiva, eficaz y eficiente, minimizando los impactos financieros, operativos o legales derivados del uso incorrecto de la información.
- Aplicar controles adecuados según la clasificación de la información en propiedad o en custodia, protegiendo la información frente a amenazas internas del personal de la Gobernación del Valle del Cauca.
- Generar conciencia organizacional para el cambio requerido en la apropiación de la seguridad y privacidad de la información.
- Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soportan los procesos críticos.
- Controlar la operación de los procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Implementar controles de acceso a la información, sistemas y recursos de red.
- Garantizar que la seguridad forme parte integral del ciclo de vida de los sistemas de información.
- Mejorar de manera efectiva el modelo de seguridad a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información.
- Asegurar la disponibilidad de los procesos de negocio y la continuidad de la operación, con base en el impacto que puedan generar los eventos.
- Cumplir con 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 de los responsables de personal.

Este apartado define las acciones que deben realizar los responsables de personal, en la gestión de accesos y recursos, cuando un funcionario se ausenta o es retirado, ya sea voluntariamente o involuntariamente, por medio de las siguientes consideraciones:

A. Cuando un funcionario se ausente de su lugar de trabajo, para desarrollar actividades personales, su jefe inmediato deberá:
   - Determinar si los accesos a los recursos físicos y a la información deben ser suspendidos.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

- Notificar la fecha en que el acceso debe ser suspendido, de ser necesario.
- Recoger los equipos de seguridad como por ejemplo llaves, claves, computadoras, etc.
- Suspender inmediatamente el acceso a los recursos físicos y a la información cuando un empleado se encuentre en una situación que le impida cumplir con sus funciones (licencia, permiso sindical, suspensión, encargo, etc.), por solicitud de su jefe inmediato, si así se requiere.

B. Cuando un empleado es retirado (voluntaria o involuntariamente), su jefe inmediato es responsable de:
   - Solicitar la revocación de las autorizaciones.
   - Revocar o restringir los privilegios de acceso antes de notificarle la terminación del contrato, si es apropiado.
   - Recoger los equipos, los dispositivos físicos y solicitar la revocación de las autorizaciones a los sistemas de información.

5.3. Políticas específicas de seguridad de la información

Las Políticas Específicas de Seguridad de la Información de la Gobernación del Valle del Cauca, son un conjunto de directrices y normas diseñadas para salvaguardar la confidencialidad, integridad y disponibilidad de la información en la entidad. Estas políticas establecen un marco normativo robusto que aborda de manera exhaustiva las necesidades particulares de la Gobernación, garantizando la protección efectiva de los datos; Incluyen lineamientos sobre control de acceso, gestión de incidentes y protección de datos personales aplicables a todos los funcionarios, contratistas y terceros involucrados con la entidad. Su definición y aplicación son esenciales para mitigar riesgos, asegurar la continuidad de las operaciones y promover una cultura de seguridad digital dentro de la Gobernación, en consonancia con el Plan de Seguridad y Privacidad de la Información (PSPI) y las normativas vigentes. La implementación de estas políticas también permite realizar ajustes para una mejora continua en la gestión de la seguridad de la información.

5.3.1. Política de gestión de contraseñas.

La Política de Gestión de Contraseña establece directrices claras y efectivas para asegurar el uso responsable de las contraseñas dentro de la Gobernación del Valle del Cauca, protegiendo así la confidencialidad e integridad de nuestro sistema de información. A través de esta política, se define cómo deben generarse, utilizarse y gestionar las contraseñas, así como, las responsabilidades de los usuarios para mantener un entorno seguro y prevenir accesos no autorizados. Adherirse a estas directrices garantiza la protección adecuada de la información y el cumplimiento de los estándares de seguridad.

Los usuarios deberán cumplir con las siguientes indicaciones para la generación y uso de contraseñas de acceso. Asimismo, serán responsables de cualquier acción realizada con las credenciales asignadas:

A. Las contraseñas son personales e intransferibles; en ninguna circunstancia deben compartirse con otros usuarios.
B. Las contraseñas deberán mantenerse confidenciales.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

C. Las contraseñas deberán ser memorizadas por los usuarios y no registrarse en ningún soporte físico o digital.
D. Todo el personal, incluidos los contratistas de la Gobernación del Valle del Cauca deberán cambiar de inmediato la contraseña inicial otorgada por los administradores de sistemas de información o de la Secretaría de las TIC. Este cambio es crucial para evitar accesos no autorizados y asegurar la trazabilidad y gestión de identidades de los usuarios. Esto abarca a superadministradores, superusuarios y cuentas privilegiadas que administran sistemas de información, bases de datos, plataformas de seguridad e infraestructura tecnológica.
E. Los usuarios administradores de cuentas con acceso privilegiado a sistemas de información, bases de datos, plataformas de seguridad e infraestructura tecnológica, deberán aceptar formalmente la responsabilidad de gestionar y custodiar sus cuentas asignadas.
F. Los funcionarios, contratistas y terceros involucrados con la entidad deberán ingresar su usuario y contraseña cada vez que accedan a las diferentes aplicaciones de la Gobernación del Valle del Cauca. Además, las contraseñas no deben guardarse automáticamente durante el inicio de sesión de las aplicaciones. Al finalizar la jornada, es importante cerrar todas las sesiones abiertas antes de apagar el equipo.
G. Las contraseñas de acceso deben adherirse a los estándares de seguridad establecidos por la Gobernación del Valle del Cauca para garantizar una protección adecuada.
H. El estándar para la generación de contraseñas seguras incluye las siguientes consideraciones:
    1. Las contraseñas deberán ser independientes del nombre de la cuenta o del usuario y no pueden contener ninguna parte de ellas, sin importar la forma de escritura.
    2. Longitud mínima de 8 caracteres.
    3. La contraseña deberá incluir caracteres de al menos 3 de los siguientes grupos: letras mayúsculas (A-Z), letras minúsculas (a-z), dígitos (0-9) y caracteres especiales (~! @ # $% ^ & * _- + = `| \ () {} [] :;" '<>,.? /). Tenga en cuenta que los símbolos de moneda como el euro o la libra esterlina no se consideran caracteres especiales según esta política.
    4. Las contraseñas se deben cambiar cada 90 días.
    5. Se debe evitar el uso de las contraseñas para múltiples cuentas o sistemas.

J. Todo el personal tiene la obligación de notificar cualquier indicio de uso no autorizado de credenciales de acceso o identificación de usuarios, lo cual debe ser considerado como un incidente de seguridad y reportado de inmediato a las autoridades pertinentes.
K. Es obligatorio que los sistemas de información soliciten a los usuarios cambiar su contraseña cada 120 días.

5.3.2. Política de capacitación y sensibilización en seguridad de la información.

La Política de Capacitación y Sensibilización en Seguridad de la Información de la Gobernación del Valle del Cauca tiene como objetivo que todos los funcionarios, contratistas y terceros involucrados con la entidad comprendan la importancia de proteger la información institucional. Este programa anual ofrece formación continua y sesiones de sensibilización diseñadas para fortalecer las prácticas de seguridad y proteger la infraestructura tecnológica. A través de capacitaciones regulares, adaptadas a las

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

necesidades específicas de cada área y personal, se promoverá una cultura de seguridad que asegure el cumplimiento de las mejores prácticas, contribuyendo a un entorno institucional más seguro y resiliente.

A. La implementación de un programa anual de concientización y sensibilización es esencial para garantizar que funcionarios, contratistas y terceros involucrados con la entidad que interactúen con la información institucional comprendan la importancia de protegerla. Este programa servirá para fomentar prácticas seguras y fortalecer la seguridad de la información y la infraestructura tecnológica de la Gobernación del Valle del Cauca.
B. Todos los funcionarios, contratistas y terceros involucrados con la entidad de la Gobernación del Valle del Cauca deben recibir información de la Política de Seguridad de la Información de la entidad y los aspectos necesarios para desempeñar las funciones asignadas de manera adecuada. Esta orientación deberá proporcionarse en los procesos de inducción y reinducción, o también cuando se actualiza o modifica dicha política.
C. Los funcionarios, contratistas y terceros involucrados con la entidad de la Gobernación del Valle del Cauca deben mejorar continuamente sus habilidades y competencias en seguridad de la información.
   Para lograrlo, se implementarán programas de capacitación y sesiones de socialización diseñadas para mantener a todos actualizados sobre las mejores prácticas y procedimientos de seguridad.
D. La Gobernación del Valle del Cauca deberá disponer de los recursos necesarios para promover actividades que fomenten la sensibilización sobre los procedimientos encargados de gestionar la Seguridad de la Información.
E. Las actividades de sensibilización de los procedimientos encargados de gestionar la Seguridad de la Información, se diseñarán teniendo en cuenta las responsabilidades, conocimientos y necesidades específicas de cada área y del personal al que van dirigidas.

5.3.3. Política de relación con proveedores.

Este grupo de políticas específicas tiene como objetivo regular y supervisar las interacciones con proveedores, asegurando que éstos manejen la información sensible de manera segura y conforme a las normativas vigentes. A través de la implementación de acuerdos de confidencialidad, evaluaciones de riesgos y controles de acceso, se busca proteger la integridad, confidencialidad y disponibilidad de los datos, minimizando los riesgos asociados a la cadena de suministro y fortaleciendo la postura de seguridad de la organización.

5.3.3.1. Planificación de las relaciones con proveedores y cadena de suministro de TI.

Esta política contempla la etapa de planificación en la adquisición de productos o servicios de tecnologías de la información

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

A. Es fundamental tener en cuenta los requisitos legales y regulatorios aplicables al producto o servicio que se planea adquirir para garantizar que se obtengan todos los permisos y licencias formales necesarios antes de iniciar la relación con el proveedor.
B. Evaluar y determinar el nivel aceptable de riesgos en la relación con un potencial proveedor para garantizar la seguridad y eficiencia operativa. Esta evaluación permite a la Secretaría de las TIC establecer si los riesgos asociados al proveedor son manejables y conformes a las políticas y procedimientos de la entidad.
C. Identificar y evaluar diversas opciones para el tratamiento de los riesgos previamente identificados y evaluados, con el fin de determinar las estrategias más efectivas para mitigar, transferir, aceptar o evitar dichos riesgos.
D. Incluir en los contratos con proveedores una cláusula que estipula que toda la información generada como resultado de la ejecución del contrato será de propiedad exclusiva de la Gobernación del Valle del Cauca. Esta disposición garantizará que la entidad mantenga el control total sobre los datos y recursos generados, fortaleciendo así la protección de la información institucional.

5.3.3.2. Selección de proveedores.

Definir e implementar criterios de selección de proveedores que contenga especificaciones del producto o servicio que se puede contratar y en el marco de criterios de selección de proveedores definidos. Los criterios de selección de proveedores cubrirán lo siguiente:

A. La aceptación por parte del proveedor de los requisitos de seguridad de la información especificados en el pliego de condiciones será un requisito obligatorio para su cumplimiento.
B. Aceptación transitoria cuando el producto o servicio a contratar haya sido previamente explotado o fabricado por la Entidad o por otro proveedor.
C. Aceptación de terminación para mantener la seguridad de la información en caso de terminación del contrato de relación con el proveedor.

5.3.3.3. Negociación de acuerdos con proveedores.

Esta política contempla las negociaciones y la gestión de acuerdos con proveedores de TI para mantener la integridad y la confidencialidad.

A. Facilitar la transición del producto o servicio según el plan acordado y notificar de manera oportuna a la otra parte sobre cualquier evento inesperado que surja durante esta actividad.
B. Gestionar los eventos e incidentes de seguridad de la información de acuerdo con las actividades acordadas.
C. Capacitar periódicamente al personal que pueda estar involucrado en la ejecución del plan de actividades

5.3.3.4. Gestión de relaciones con proveedores.

Establecer las actividades que deben ser tenidas en cuenta por la Entidad, para la gestión de la prestación de los servicios o productos contratados, verificación de las responsabilidades y controles aplicables para dar alcance al objeto contractual, por lo cual se recomienda:

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

- Garantizar la vigencia de los documentos y pólizas durante el período de ejecución es crucial, con la responsabilidad de monitorear y actualizar las condiciones contractuales según sea necesario, especialmente en casos de prórroga.
- Realizar revisiones periódicas de los documentos, planes y procedimientos entregados por los proveedores, como aspecto fundamental para la Secretaría de las TIC. Estas revisiones permiten evaluar la funcionalidad y determinar si es necesario actualizar o mejorar los documentos para alinearse eficazmente con los procesos y políticas vigentes de la organización.

5.3.3.5. Proceso de terminación de la relación con el proveedor.

Define las actividades necesarias para la gestión efectiva a la finalización contractual con proveedores.

A. Solicitar al proveedor la documentación técnica detallada, bitácoras de procedimientos actualizadas y cualquier otro registro relevante que documente de manera integral las actividades llevadas a cabo durante la ejecución contractual.
   De acuerdo con el servicio deberán ser requeridos en la entrega como mínimo:
   - Documentación técnica del diseño y de la operación.
   - Archivos de Imágenes de máquinas virtuales.
   - Archivos de bases de datos.
   - Archivos de bases de datos de administración de configuraciones (CMDB).
   - Archivos que se encuentren dispuestos en los servicios de almacenamiento contratado.
   - Toda aquella documentación sobre topologías, estructuras físicas o lógicas
B. Solicitar el apoyo del proveedor durante el proceso de cierre contractual para coordinar los despliegues técnicos y operativos necesarios. Esto incluye verificar, probar, trasladar y ejecutar la entrega o migración de productos o servicios relacionados con la seguridad de la información, asegurando así un proceso eficiente y bien coordinado.
C. Acta de finalización del proceso contractual, avalada y firmada por el supervisor, donde se certifique oficialmente el cierre del contrato.
D. Asegurar la verificación del cambio de credenciales de acceso, la eliminación de usuarios y el cierre de conexiones remotas con el proveedor saliente para garantizar la seguridad y la integridad de los sistemas.

5.3.3.6. Acuerdos de confidencialidad.

Todos los funcionarios deberán suscribir acuerdos de confidencialidad conforme al Código Disciplinario vigente y las demás normas que regulen el empleo público, la carrera administrativa y la gerencia pública, mientras que los contratistas lo harán según la cláusula de confidencialidad incluida en sus contratos respectivos. Estos acuerdos establecerán términos legalmente ejecutables que delimitan las responsabilidades y acciones de los firmantes para evitar la divulgación no autorizada de información.

5.3.3.7. Seguridad de la información para la colaboración con contratistas.

La política de gestión de medios extraíbles establece directrices para el uso, control y protección de dispositivos de almacenamiento personal en la infraestructura tecnológica de la Gobernación del Valle del Cauca, su propósito es asegurar que los medios extraíbles que

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

contengan información institucional sean gestionados de manera segura, garantizando su adecuada identificación, protección, y eliminación para mitigar riesgos de seguridad. Esta política define las responsabilidades y procedimientos necesarios para la autorización, manejo y destrucción segura de estos dispositivos, con el objetivo de proteger la integridad de la información y prevenir accesos no autorizados.

A. En todos los contratos relacionados con la prestación de servicios personales bajo cualquier modalidad jurídica, tales como contratos laborales, contratos de prestación de servicios, acuerdos de consultoría, contratos administrativos y convenios interinstitucionales, que se lleven a cabo dentro de las instalaciones de la Gobernación del Valle del Cauca, se establecerán estrictos controles de seguridad y compromisos de confidencialidad. Estos requisitos aseguran que los permisos concedidos sean los mínimos necesarios.
B. El acceso de terceros a información confidencial, áreas de procesamiento de datos o servicios críticos se permitirá únicamente después de implementar los controles adecuados y de firmar contratos o acuerdos que definan claramente las condiciones de conexión o acceso. Estos requisitos deben cumplirse antes de otorgar acceso para garantizar la seguridad y protección de los datos y servicios críticos.
C. El acceso de terceros a la información o cualquier elemento de la infraestructura tecnológica de la Entidad debe ser solicitado por el supervisor o responsable del tercero al responsable del activo correspondiente, por los medios institucionales autorizados. El responsable, junto con la Secretaría de las TIC, evaluará y autorizará el acceso y uso de la información.
D. Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y ambientes de computadores deben incluir los siguientes aspectos fundamentales:
    1. **Cumplimiento de los requisitos legales aplicables.** Es fundamental asegurar que todas las actividades de tercerización cumplan con las leyes y regulaciones pertinentes y vigentes.
    2. **Responsabilidades claras y comunicación efectiva.** Todos los involucrados, incluidos los contratistas, deberán comprender claramente sus responsabilidades en materia de seguridad.
    3. **Integridad y confidencialidad de los activos.** Se deberán establecer mecanismos sólidos para mantener y verificar la integridad y confidencialidad de los datos y recursos de la organización.
    4. **Controles de acceso robustos.** Es esencial implementar controles físicos y lógicos efectivos para restringir el acceso a la información sensible.
    5. **Continuidad del servicio.** Se deberán definir protocolos claros para garantizar la disponibilidad de los servicios incluso en situaciones de desastre.
    6. **Seguridad física del equipamiento.** Asignar niveles adecuados de seguridad física al equipamiento tercerizado para protegerlo de amenazas.
    7. **Derecho a la auditoría.** La capacidad de realizar auditorías por parte de la Secretaría de las TIC a los proveedores de servicio para garantizar la transparencia y el cumplimiento de los acuerdos pactados a través de los contratos.

5.3.4. Política de gestión de medios extraíbles.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

La política de gestión de medios extraíbles establece directrices para el uso seguro y controlado de dispositivos de almacenamiento como unidades USB, discos duros y CDs dentro de la Gobernación del Valle del Cauca. Su objetivo es proteger la infraestructura tecnológica y la información institucional mediante restricciones en el uso de dispositivos no institucionales, asegurar una adecuada clasificación y control de los medios removibles, y garantizar la protección de datos sensibles a través de procedimientos de baja y reutilización rigurosos. La Secretaría de las TIC supervisa y autoriza el uso de estos medios para asegurar el cumplimiento efectivo de esta política.

A. La conexión a la infraestructura tecnológica de la Gobernación del Valle del Cauca está estrictamente restringida, lo que incluye cualquier dispositivo de almacenamiento personal como unidades USB, discos duros externos, CDs, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, módems y otros dispositivos no institucionales.
B. Los medios de almacenamiento removibles, como cintas, discos duros extraíbles, CDs, DVDs, medios impresos y dispositivos USB, que contengan información institucional, deben ser adecuadamente controlados y protegidos físicamente.
C. La Secretaría de las TIC será responsable de determinar los medios removibles de almacenamiento que podrán ser utilizados por el personal autorizado en la infraestructura tecnológica de la Entidad, en caso de ser necesario para el cumplimiento efectivo de sus funciones.
D. Cada medio removible de almacenamiento deberá estar debidamente identificado según el tipo de información que contenga, garantizando una clasificación adecuada y facilitando así su manejo y gestión dentro de la entidad.
E. Para los procesos de baja, reutilización o gestión de garantías de dispositivos que incluyan medios de almacenamiento, se debe cumplir, según corresponda, con la destrucción física del dispositivo o con un borrado seguro de los datos almacenados en él, asegurando así la protección de la información sensible y la mitigación de riesgos de seguridad.
F. El tránsito o préstamo de medios removibles debe contar con la autorización del responsable del activo de información. Asimismo, en los procesos de baja, reutilización o gestión de garantías de dispositivos que albergan medios de almacenamiento, se debe proceder, según sea pertinente, con la destrucción física del dispositivo o con un borrado seguro de los datos almacenados en él, asegurando la protección de la información y la mitigación de riesgos de seguridad.

5.3.5. Política de protección de los derechos de propiedad intelectual.

La Política de Protección de los Derechos de Propiedad Intelectual tiene como objetivo salvaguardar los derechos de autor y propiedad intelectual en todas las actividades de la Gobernación del Valle del Cauca. Esta política prohíbe el uso no autorizado de contenido protegido, establece condiciones para el uso de información pública, y asegura el cumplimiento de la legislación vigente en la adquisición y desarrollo de software. Nuestro compromiso es respetar y proteger los derechos legales relacionados con todas las obras y recursos utilizados.

A. No se permite el almacenamiento, descarga desde Internet, intercambio, uso, copia, reproducción y/o instalación de cualquier contenido no autorizado, incluyendo software, música, videos, documentos, textos, fotografías, gráficos y otras obras protegidas por

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

derechos de propiedad intelectual, que carezcan de la debida licencia o autorización legal.

B. Se permite el uso de documentos, cifras y/o textos de carácter público siempre y cuando se cite al autor de estos con el fin de preservar los derechos morales e intelectuales de las obras o referencias citadas.
C. Los procesos de adquisición de aplicaciones y paquetes de software deben estar en total conformidad con los requerimientos y obligaciones establecidos por las leyes de propiedad intelectual y los derechos de autor, asegurando así el respeto y cumplimiento de los derechos legales asociados a dichas adquisiciones.
D. Establecer que el desarrollo de software a la medida, adquirido a terceras partes o realizado por funcionarios de la Entidad, sea de uso exclusivo de la Gobernación del Valle del Cauca. Además, incluir en los contratos correspondientes una cesión de derechos patrimoniales que garantice que todos los derechos económicos sobre el software, incluyendo su explotación, modificación y distribución, sean transferidos a la Gobernación. Esto asegura que la entidad mantenga el control total y exclusivo sobre el uso y explotación del software desarrollado.

5.3.6. Política de bloqueo de sesión, escritorio y pantalla limpia.

Esta política establece directrices esenciales para garantizar la seguridad de la información en el entorno de trabajo. Su objetivo es proteger los datos críticos y sensibles de accesos no autorizados mediante el bloqueo adecuado de estaciones de trabajo, la gestión segura de documentos y el cumplimiento de prácticas estandarizadas para la protección de la información. Asegurar el cumplimiento de estas normas minimiza los riesgos asociados a la exposición y pérdida de información, y promueve un entorno seguro y responsable para todos los usuarios.

A. Cuando los sitios de trabajo se encuentren desatendidos o en horas no hábiles, las y los usuarios deben dejar bajo llave los medios que contengan información crítica protegida.
B. Es responsabilidad de cada usuario bloquear su estación de trabajo al ausentarse de su puesto, y el acceso posterior sólo estará permitido mediante el uso de la contraseña asignada a cada usuario.
C. Las estaciones de trabajo deberán emplear exclusivamente el papel tapiz y el protector de pantalla predeterminados por la Gobernación del Valle del Cauca. Estos se activarán automáticamente después de un período de inactividad establecido por el responsable de Seguridad de la Información y solo podrán desbloquearse mediante la contraseña del usuario correspondiente.
D. Los usuarios deben recoger de inmediato cualquier documento con información sensible que envíen a las impresoras o dispositivos de copiado. Esto asegura que la información confidencial no quede expuesta y reduce el riesgo de acceso no autorizado.
E. Es fundamental abstenerse de reutilizar papel que contenga información confidencial.
F. Los usuarios no deben almacenar documentos digitales ni accesos directos a sistemas de información sensibles en el escritorio de sus estaciones de trabajo. Es crucial que toda información sensible esté guardada en ubicaciones seguras, como carpetas protegidas con contraseñas o sistemas de almacenamiento cifrados, para prevenir accesos no autorizados y garantizar la seguridad de los datos.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

G. Los usuarios son responsables de la custodia y del uso adecuado de los activos de información asignados. Por consiguiente, se requiere su presencia en el lugar de trabajo durante cualquier proceso de mantenimiento o actualización de dichos activos.
H. Todos los funcionarios, contratistas y terceros involucrados con la entidad tienen la responsabilidad de eliminar cualquier información sensible que haya sido escrita en los tableros o pizarras al concluir las reuniones de trabajo. Además, deben asegurarse de que no queden documentos o notas escritas sobre las mesas con información sensible.
I. Durante su ausencia del puesto de trabajo, los funcionarios, contratistas y terceros involucrados con la entidad, no deben dejar sobre el escritorio ningún documento físico u otros elementos que contengan información confidencial de la entidad. Es necesario guardar dicha información en un lugar seguro para evitar su pérdida, daño, copia o acceso por parte de personas no autorizadas.
J. Es responsabilidad de los funcionarios, contratistas y terceros involucrados con la entidad custodiar los expedientes físicos que soliciten al área de archivo o los expedientes digitales del repositorio general de la Gobernación del Valle del Cauca para el cumplimiento de sus respectivas funciones u obligaciones, darles un uso responsable con todas las medidas de seguridad y retornarlos al área de archivo en las condiciones originales que fueron suministrados.

5.3.7. Política de registros de procedimientos operativos.

Los procedimientos operativos son directrices documentadas que guían el manejo y la gestión de los activos de información en la entidad. Su propósito es asegurar que todas las actividades se realicen de manera coherente, eficiente y conforme a los estándares de seguridad establecidos. Estos procedimientos proporcionan instrucciones claras para la ejecución de tareas, el manejo de errores y la recuperación de sistemas, garantizando así la integridad y disponibilidad de la información. Las solicitudes para la elaboración, modificación o publicación de estos documentos deben ser autorizadas por la Secretaría de las TIC, en conjunto con la Secretaría General, compartiendo así las responsabilidades en el proceso de publicación y asegurando el cumplimiento de las normativas vigentes**.**

A. Toda actividad realizada sobre los activos de información de la entidad debe estar respaldada por instrucciones operativas documentadas. Estos documentos deben estar siempre disponibles para todos los usuarios que los necesiten en el desempeño de sus funciones, asegurando así la correcta ejecución de las tareas y el cumplimiento de los estándares establecidos.
B. Todas las solicitudes relacionadas con la elaboración, publicación y modificación de documentos de Seguridad de la Información deben ser autorizadas por la Secretaría de las TIC, en conjunto con la Secretaría General, compartiendo así las responsabilidades en el proceso de publicación. Este proceso se llevará a cabo de acuerdo con las instrucciones establecidas, garantizando así que todas las acciones cumplan con las normativas y estándares de seguridad vigentes.
C. Las instrucciones operativas deben incluir directrices claras para la gestión de errores durante la ejecución de las actividades. Esto abarca los contactos de soporte, las instrucciones para reinicio y recuperación de sistemas y aplicaciones, las pautas para el procesamiento y manejo seguro de la información, y las estrategias de respaldo de datos. Asimismo, se deben detallar otros aspectos relevantes necesarios para asegurar una operación segura, eficiente y continua.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

5.3.8. Política de control de cambios en operaciones.

La Política de Control de Cambios en Operaciones establece las instrucciones necesarias para gestionar, autorizar y controlar todas las modificaciones en los sistemas de información e infraestructura tecnológica. Su objetivo es asegurar que cada cambio sea implementado de manera planificada, documentada y controlada, garantizando la continuidad, seguridad y calidad de los servicios tecnológicos. Esta política promueve una gestión eficiente al reducir riesgos y minimizar impactos, facilitando una transición fluida y segura en las operaciones tecnológicas.

A. Cualquier modificación en los sistemas de información e infraestructura tecnológica debe ser rigurosamente controlada, gestionada y autorizada tanto por la Secretaría de las TIC como de la dependencia propietaria del sistema. Este proceso debe incluir una planificación detallada y la ejecución de pruebas exhaustivas para identificar posibles riesgos, tiempos de implementación e impactos potenciales que puedan afectar la operación del sistema. De esta manera, se asegura una gestión eficiente y segura de los cambios, minimizando cualquier interrupción o problemas que puedan surgir.
B. Todos los cambios realizados en los sistemas de información e infraestructura tecnológica deben ser precedidos por una definición clara de los requisitos, especificaciones y controles necesarios, según lo establecido en el Proceso M1-P3 “Administrador de MIPG - Matriz de Planificación de Cambios”. Este proceso garantiza que cualquier modificación sea planificada, evaluada y aprobada adecuadamente, asegurando así la integridad, seguridad y eficiencia de la infraestructura tecnológica.
C. Cualquier modificación en los sistemas de información e infraestructura tecnológica debe estar plenamente justificada y documentada.
D. Las modificaciones deben ser sugeridas e implementadas de manera que no afecten la calidad de los servicios de información y tecnología de comunicaciones de la Gobernación del Valle del Cauca. Es esencial garantizar que cualquier cambio propuesto mantenga o mejore el nivel actual de servicio, asegurando así la continuidad y eficiencia en todas las operaciones tecnológicas.
E. Los cambios de emergencia deben documentarse formalmente y ser comunicados al Comité Institucional de Gestión y Desempeño, o quien haga sus veces, para su formalización. Este proceso garantiza que todos los ajustes realizados en situaciones de emergencia sean transparentes y estén debidamente registrados, lo que facilita su revisión y seguimiento por parte del comité, asegurando la continuidad y la integridad de las operaciones
F. Todos los cambios deben ir acompañados de un análisis exhaustivo de los riesgos tanto de su implementación como de su no implementación. Este análisis debe identificar y evaluar las posibles consecuencias y desafíos asociados con la adopción de los cambios, así como, las implicaciones de mantener el estado actual sin realizar modificaciones. Al considerar ambos escenarios, se pueden tomar decisiones informadas que maximicen los beneficios y minimicen los riesgos, asegurando así una transición suave y efectiva hacia los cambios propuestos.
G. Antes de ejecutar cualquier cambio, es esencial someterlo a un mecanismo de prueba rigurosa. Este proceso de prueba debe verificar que la planificación esté completa y adecuada, asegurando que todos los posibles impactos y riesgos han sido considerados.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

Así, se garantiza que la implementación se llevará a cabo sin contratiempos, minimizando errores y asegurando una transición progresiva y efectiva.

H. Solo se ejecutan los cambios que han sido debidamente aprobados y autorizados por el Comité Institucional de Gestión y Desempeño, cuando así se requiera. Este proceso garantiza que todas las modificaciones se realicen con la debida supervisión y conformidad con las políticas establecidas, asegurando así la integridad y eficacia de las operaciones de la institución.

I. Todos los cambios deben ser formalmente registrados, clasificados y documentados conforme a las instrucciones establecidas por la Secretaría de las TIC. Este proceso asegura que cada modificación sea adecuadamente rastreada y gestionada, garantizando la transparencia y la coherencia en la implementación de ajustes y mejoras. Al seguir estas instrucciones, se facilita la supervisión y el control, promoviendo una gestión eficiente y responsable de los cambios realizados.

J. Es esencial que todos los cambios implementados incluyan una serie de actividades de marcha atrás o “rollback” para garantizar la capacidad de revertir el cambio en caso de que surjan problemas o fallos. Este plan debe estar claramente documentado y probado con antelación, asegurando que cualquier alteración pueda deshacerse de manera rápida y segura, minimizando el impacto en las operaciones y manteniendo la continuidad del servicio. De este modo, se asegura que, ante cualquier eventualidad, la entidad pueda retomar el estado operativo previo sin complicaciones ni pérdidas significativas.

K. Cada vez que se realicen cambios en la infraestructura de información y tecnología de comunicaciones de la entidad, es esencial evaluar la necesidad de actualizar los planes de contingencia y continuidad de negocio. Esta verificación asegura que las nuevas configuraciones y modificaciones no comprometan la capacidad de la institución para responder eficazmente a incidentes imprevistos y garantizar la continuidad operativa. Mantener estos planes actualizados es crucial para minimizar riesgos y proteger los intereses y operaciones esenciales de la organización.

L. Elaborar la hoja de vida de los Sistemas de Información (SI) y el formato de requerimientos será necesario cada vez que se realicen cambios en los sistemas de información. Esto permitirá un registro detallado de las modificaciones implementadas, facilitando la gestión, seguimiento y documentación de los cambios realizados. De esta manera, se asegura que cualquier cambio quede debidamente registrado y que los requisitos asociados a las modificaciones sean claros y fácilmente accesibles para futuras referencias

5.3.9. Política de gestión de la capacidad.

La Política de Gestión de la Capacidad de la Gobernación del Valle del Cauca establece un proceso sistemático para el monitoreo y evaluación continua del rendimiento y capacidad de la infraestructura tecnológica. Su objetivo es garantizar la eficiencia en el uso de los recursos y anticipar el crecimiento necesario para mantener la integridad y disponibilidad de los sistemas. Mediante la medición regular de variables críticas, esta política permite prever necesidades futuras y planificar la adquisición de recursos para soportar la demanda, asegurando una infraestructura tecnológica robusta y adaptable

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

A. La Gobernación del Valle del Cauca mantendrá un proceso continuo de monitoreo, análisis y evaluación del rendimiento y capacidad de su infraestructura tecnológica de procesamiento de información. Este proceso permitirá identificar y controlar el consumo de recursos, prever su crecimiento de forma planificada y asegurar la integridad del procesamiento. Periódicamente, se medirán las variables críticas de operación para verificar el estado y uso de los recursos, lo que facilitará la definición de proyecciones de crecimiento que garanticen la disponibilidad y eficiencia de la infraestructura

B. Los resultados de dichas mediciones serán analizados y presentados a la Alta Dirección y en caso de ser necesaria la adquisición de nuevos recursos o elementos para soportar la demanda, se proceda a planificar la consecución de dichos elementos.

5.3.10. Política de continuidad del negocio.

La Política de Continuidad del Negocio define las directrices para asegurar la protección y recuperación efectiva de la información en caso de incidentes. Esta política establece que la seguridad de la información debe ser garantizada en cada fase de las estrategias de continuidad, desde su diseño hasta su ejecución. Además, promueve una evaluación constante de riesgos y la implementación de medidas preventivas, así como, la realización de ejercicios de recuperación periódicos para mantener la efectividad de los planes. La política también enfatiza la importancia de contar con redundancia en los sistemas críticos para asegurar la disponibilidad continua de los servicios esenciales.

A. La Secretaría de las TIC debe garantizar la seguridad de la información en todas las fases de sus estrategias de continuidad y retorno a la normalidad. Esto incluye desde el diseño inicial, pasando por la implementación, hasta la activación de dichas estrategias. Asegurarse de que los datos están protegidos en cada etapa, es fundamental para mantener la integridad, confidencialidad y disponibilidad de la información, permitiendo así una recuperación efectiva y segura ante cualquier eventualidad.
B. La Secretaría de las TIC debe llevar a cabo un análisis y evaluación exhaustiva de los riesgos asociados con la seguridad de la información y la ciberseguridad. Este proceso es crucial para identificar vulnerabilidades en los activos de información que podrían provocar interrupciones en la operación de los procesos críticos de la entidad. Mediante la implementación de medidas preventivas y correctivas, se busca garantizar la continuidad y resiliencia de las funciones esenciales de la organización, asegurando así la protección e integridad de la información.
C. Es esencial realizar ejercicios de recuperación de datos regularmente para mantener los planes actualizados, fortalecer la confianza de la dirección en estos y asegurar que los colaboradores estén bien familiarizados con sus responsabilidades en caso de incidentes de interrupción o contingencias. Estos ejercicios no solo validan la efectividad de los planes, sino que también mejoran la preparación del personal y garantizan una respuesta coordinada y eficaz ante cualquier eventualidad.
D. Es responsabilidad de la Secretaría de las TIC asegurar que los sistemas de procesamiento de información críticos dispongan de redundancia adecuada para cumplir con los requisitos de disponibilidad establecidos en el Sistema de Gestión de Continuidad del Negocio de la Entidad. Esta medida garantiza que, en caso de fallos o interrupciones inesperadas, los servicios esenciales puedan mantenerse operativos sin

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

afectar la continuidad de las operaciones. La implementación de estrategias de redundancia contribuye significativamente a la resiliencia del sistema y a la capacidad de respuesta ante posibles contingencias, asegurando así la prestación eficiente y continua de los servicios críticos para la comunidad.

5.3.11. Política de sanciones previstas por incumplimiento.

Las políticas de seguridad establecidas buscan proteger la integridad y el correcto funcionamiento de la Gobernación del Valle del Cauca. En caso de incumplimiento, se evaluarán las acciones correctivas necesarias de acuerdo con las normativas vigentes, y, si corresponde, se informará a las autoridades competentes para que estas puedan tomar las medidas correspondientes. Las posibles sanciones, si aplican, serán formalizadas mediante actos administrativos, respetando los derechos de los involucrados y en conformidad con el marco legal. De esta manera, se garantiza una respuesta justa y legal ante cualquier violación, protegiendo nuestros recursos e intereses institucionales.

A. Cualquier violación de las políticas de seguridad establecidas será objeto de sanción administrativa, conforme a las normativas vigentes que regulan al personal de la Gobernación del Valle del Cauca. En caso de ser necesario, se procederá a tomar las acciones correspondientes ante las autoridades competentes, garantizando así el cumplimiento de las disposiciones y la protección de la integridad institucional.
B. Las sanciones deben ser impuestas a través de actos administrativos que cumplan con todas las formalidades establecidas por la Constitución, la ley de procedimientos administrativos y las normativas específicas aplicables. Este proceso garantiza el respeto a los derechos y garantías de los involucrados, asegurando que las sanciones se apliquen de manera justa y legal.
C. Además de enfrentar sanciones disciplinarias o administrativas, la persona que incumple sus obligaciones puede incurrir también en responsabilidad civil o patrimonial si causa un daño que requiere indemnización. Así mismo, puede ser responsable penalmente si su conducta se considera delictiva según el código penal y las leyes especiales aplicables.

5.3.12. Política de seguridad de espacios físicos y ambientales.

La Política de Seguridad de Espacios Físicos y Ambientales establece las directrices para proteger las áreas críticas dentro de la Oficina de Tecnologías de la Información y las Comunicaciones. Su objetivo principal es garantizar que las zonas sensibles, como servidores y equipos clave, estén protegidas mediante controles de acceso físico rigurosos. Estas áreas estarán claramente marcadas y su acceso estará restringido a personal autorizado exclusivamente. La política asegura que se realice una evaluación exhaustiva de riesgos, como incendios y desastres naturales, para proteger tanto a las personas como a los activos de información. En esencia, esta política busca crear un entorno seguro y conforme a las normativas vigentes, minimizando riesgos y promoviendo la integridad de las operaciones tecnológicas.

A. Las áreas seguras estarán protegidas mediante controles de acceso físico, establecidos por la Oficina de Tecnologías de la Información y las Comunicaciones. Solo el personal autorizado tendrá acceso a estas zonas, las cuales estarán claramente señalizadas con

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

avisos que indiquen "SOLO PERSONAL AUTORIZADO, ZONA RESTRINGIDA o similares". Estos controles aseguran que únicamente las personas con los permisos adecuados puedan ingresar, garantizando así la seguridad y protección de los recursos y la información contenidos en dichas áreas.

B. Para seleccionar las áreas críticas, candidatas a ser aseguradas y restringidas, se evaluarán los riesgos potenciales de incendio, inundación, explosión, afectación por disturbios civiles y otras formas de desastres naturales o provocados por el hombre. Además, se considerarán las normativas y estándares vigentes en materia de salud y seguridad de las instalaciones. Esta evaluación integral asegurará que las áreas designadas sean adecuadas y cumplan con los requisitos necesarios para garantizar la protección y seguridad de las personas y los activos de información.
C. Las plataformas tecnológicas se alojarán, protegerán y administrarán estratégicamente para minimizar los riesgos derivados de amenazas y peligros ambientales, así como, para prevenir el acceso no autorizado. Esta medida garantiza tanto la seguridad física como la integridad de los datos, promoviendo un entorno seguro y confiable para la operación tecnológica.

5.3.13. Manejo de información confidencial.

La gestión de información confidencial es crucial para garantizar la seguridad y privacidad de los datos sensibles. Estas directrices establecen procedimientos para proteger la información contra accesos no autorizados, asegurar su adecuada clasificación y divulgación, y garantizar que todos los documentos y copias de respaldo se manejen con el máximo cuidado. La implementación efectiva de estas prácticas asegura que la información confidencial se mantenga segura y accesible únicamente para aquellos con la debida autorización.

A. No debe exponerse a manipulación o uso de personal no autorizado.
B. Debe contener los datos del responsable o su respectiva fuente en la primera página o cubierta.
C. Debe ser apropiadamente autorizada para su divulgación de acuerdo con los estándares de clasificación de la información por parte de los responsables.
D. Su divulgación, por cualquier medio, verbal, escrita, telefónica o electrónica, debe ser efectuada sobre la base de la necesidad de conocerla con la debida justificación del solicitante y la autorización de quien la custodia.
E. Las reuniones relacionadas con el manejo de información confidencial deben llevarse a cabo en áreas de oficinas cerradas.
F. No debe ser accedida o enviada a través de cualquier tecnología de fácil acceso, tales como teléfonos celulares o medios inalámbricos inseguros.
G. Para propósitos de seguridad, toda la información debe ser etiquetada con la clasificación respectiva.
H. El etiquetado debe ser legible y poderse entender a simple vista.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

I. Por ningún motivo se debe divulgar verbalmente información clasificada, restringida o confidencial.

J. El acceso de información de uso interno debe estar limitado a funcionarios, contratistas y terceros involucrados con la entidad si es necesario para cumplir con sus funciones.

K. Documentos que contengan información confidencial deben ser alojados en un área segura o con la supervisión adecuada.

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

M. Los mecanismos de entrega utilizados para información restringida deben contemplar confirmación de recibo. Lo anterior se aplica tanto a los originales como a todas las copias de la información.

N. El acceso a información confidencial que se encuentre almacenada debe ser adecuadamente controlado. Esto incluye información confidencial almacenada externamente o copias de respaldo.

O. 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.

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

Q. 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.

5.3.14. Política de control de acceso y gestión de privilegios.

La Política de Control de Acceso y Gestión de Privilegios establece un marco formal para la creación, asignación y gestión de cuentas de usuario dentro de la entidad. Su objetivo es asegurar que solo los usuarios autorizados accedan a los sistemas y recursos informáticos, mediante procedimientos rigurosos de aprobación y documentación. La política garantiza la definición clara de roles y responsabilidades, la segregación de funciones, y el uso de contraseñas seguras, con el fin de proteger la infraestructura tecnológica y mantener la integridad y seguridad de la información. Además, se establecen medidas para la gestión de accesos remotos y redes inalámbricas, asegurando un entorno de trabajo seguro y eficiente.

A. La entidad debe adherirse a un procedimiento formalmente establecido para la creación y aprobación de cuentas de usuarios. Este procedimiento debe garantizar que todas las solicitudes de nuevas cuentas sean revisadas y aprobadas adecuadamente, asegurando que solo los usuarios autorizados obtengan acceso a los sistemas y recursos informáticos solicitados.

B. Los sistemas de información deben contar con una documentación clara y detallada sobre la gestión de roles y privilegios de servicios.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

C. Todas las personas con acceso a la infraestructura tecnológica o a los sistemas de información deben tener una definición clara de sus roles y responsabilidades. Esto es fundamental para reducir y evitar el uso no autorizado o la modificación no intencional de los activos de información.
D. La segregación de funciones en la infraestructura tecnológica de la entidad y sus sistemas de información, deberá ser revisada periódicamente por sus respectivos administradores. Esta revisión tiene como objetivo mantener la información actualizada y en consonancia con la realidad y necesidades específicas de cada una de las dependencias de la entidad.
E. Toda persona, sistema de información o componente de procesamiento de datos que necesiten acceder a un recurso informático de la Entidad, deberá contar con una cuenta única, de uso exclusivo e intransferible. Esta cuenta permitirá el acceso a la información según la necesidad de uso aprobada por el responsable de la información.
F. Cuando un miembro del personal, ya sea funcionario o contratista, necesite acceder a los sistemas de información de la Entidad, se le proporcionará un usuario y contraseña para su acceso, con los permisos de acceso de acuerdo a las funciones que vaya a realizar.
G. Las personas encargadas de la gestión de los datos almacenados en los sistemas de información, serán responsables de autorizar los privilegios asignados a las cuentas de usuario, teniendo en cuenta la necesidad de acceso a la información según las funciones específicas que desempeñará el usuario o el componente electrónico de procesamiento de información que utilizará la cuenta de acceso.
H. La asignación de cualquier cuenta de acceso a un sistema de información debe cumplir con los controles que garanticen la identificación de las personas encargadas de las actividades de solicitud, aprobación, creación, modificación, inactivación o eliminación autorizada de dicha cuenta. Además, se deben implementar medidas para mantener la veracidad y la trazabilidad de todas las actividades relacionadas con la asignación de cuentas de acceso.
I. Cada actividad llevada a cabo utilizando una cuenta de acceso debe ser registrada meticulosamente mediante controles apropiados para garantizar la trazabilidad de dichas acciones.
J. Cada cuenta de acceso requerirá obligatoriamente una contraseña como medida de autenticación segura, la cual debe cumplir con los estándares de complejidad establecidos en el presente documento.
K. Toda cuenta de acceso debe ser asignada formalmente a una persona quién responderá por su uso y acciones realizadas con la misma en el componente electrónico de procesamiento de información o con la información del componente de procesamiento de información.
L. Las cuentas de usuario de contratistas naturales y jurídicos dentro de la Entidad deben configurarse en los sistemas de información de manera que se desactiven automáticamente de acuerdo con los términos y fechas estipulados en el acuerdo contractual con la institución. Por otro lado, en el caso del funcionario, el Departamento Administrativo de Desarrollo Institucional tiene la responsabilidad de notificar a la Secretaría de las TIC sobre los empleados que se retiren de la Entidad, para que esta última proceda a desactivar sus cuentas de usuario.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

M. En cuanto a los dispositivos que forman parte activa de la plataforma tecnológica, las personas responsables de su administración deben cambiar todas las credenciales y usuarios que traen por defecto dichos dispositivos, ya que estos son ampliamente conocidos. Una vez configurado y puesto en funcionamiento el dispositivo, se debe establecer una periodicidad para cambiar las contraseñas creadas.
N. Para solicitar creación y/o permisos de usuario en aplicaciones, se debe enviar una solicitud a la mesa de ayuda servicios TI de la Entidad a través de los medios definidos por la secretaría de las TIC para ello. Una vez recibida la solicitud, el permiso será evaluado y aprobado por el jefe de área de servicios tecnológicos. Después de que se haya ejecutado la actividad y se hayan otorgado los permisos, el requerimiento será reasignado a la persona titular de la cuenta a la que se le han concedido los permisos. Además, la herramienta de gestión correspondiente deberá enviar notificaciones de cierre al correo del titular de la cuenta con permisos y a su superior jerárquico autorizado.
O. El acceso como administrador en los equipos de cómputo está reservado únicamente para el personal autorizado de la Entidad, en estricto cumplimiento de las políticas de seguridad de la información.
P. Todo usuario, interno o externo, que necesite acceder de forma remota a la red o a la infraestructura de procesamiento o seguridad informática de la Entidad, debe contar con la autorización correspondiente, la cual será otorgada previa evaluación y aprobación por parte de la Secretaría de las TIC.
Q. Todas las conexiones remotas deben ser cifradas y autenticadas para generar un tráfico seguro de información.
R. Los accesos a las redes inalámbricas de la entidad deben ser gestionados y autorizados por la Secretaría de las TIC, luego de verificar condiciones seguras de conexión y de establecer los mecanismos de control necesarios para salvaguardar la infraestructura de la entidad.
S. Asegurar que todos los accesos a los sistemas de información e infraestructura tecnológica se realicen con base en las políticas de roles y perfiles definidas por la entidad. Además, la asignación y modificación de accesos deberá cumplir con los formatos establecidos por la Secretaría de las TIC, garantizando que cada usuario tenga únicamente los permisos necesarios para sus funciones y que se mantenga la trazabilidad y control de los privilegios asignados.

5.3.15. Política de administración de registros (logs).

La política de administración de registros establece que todos los sistemas de información, dispositivos de procesamiento, y equipos de red y seguridad deben generar y mantener registros detallados de eventos. Estos logs son esenciales para la vigilancia continua, la detección de actividades no autorizadas y la protección de la infraestructura tecnológica de la Entidad. La retención de estos registros se ajustará a las necesidades específicas del sistema y a las normativas vigentes. Cualquier actividad sospechosa detectada a través de los logs debe ser reportada de inmediato a la Secretaría de las TIC y al operador tecnológico para su pronta resolución.

A. Generar registros de eventos (logs) en los sistemas de información que manejan datos críticos, así como en los dispositivos de procesamiento, red y seguridad informática. Estos registros deberán ser recolectados y analizados según las necesidades operativas

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

de la entidad, con el fin de detectar actividades no autorizadas en la información y en los dispositivos de procesamiento, red y seguridad de la infraestructura tecnológica de la Entidad. La periodicidad y el alcance del análisis se determinarán en función de los recursos y capacidades disponibles.

B. La duración de la retención de los registros estará determinada por las condiciones específicas de cada sistema de información, recurso informático o dispositivo de red, así como, por las leyes, normativas o regulaciones vigentes.
C. Cualquier evento identificado a través del monitoreo y la revisión de registros que comprometa la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica debe ser reportado inmediatamente a la Secretaría de las TIC, así como, al operador tecnológico, para ser resuelto con la mayor prontitud posible.

5.3.16. Política de gestión y supervisión de usuarios.

Esta política establece los lineamientos generales para la correcta gestión y supervisión de usuarios dentro de las instalaciones de la Gobernación del Valle del Cauca. Su objetivo es asegurar un control de acceso efectivo y la seguridad de las dependencias, garantizando que todos los funcionarios, contratistas y terceros involucrados con la entidad actúen conforme a las regulaciones establecidas. La implementación de estas normas contribuye a mantener un entorno seguro y ordenado, facilitando la identificación y supervisión del personal y visitantes.

A. Usar el carnet de identificación de manera visible es recomendado para todos los funcionarios, contratistas y terceros involucrados con la entidad mientras se encuentren dentro de las instalaciones de la Gobernación del Valle del Cauca, conforme a las directrices del Departamento Administrativo de Desarrollo Institucional (DADI). Este documento es personal e intransferible.
B. Verificar el uso correcto del carnet al ingresar a las instalaciones es responsabilidad del personal de vigilancia, gestionado por el Departamento Administrativo de Desarrollo Institucional (DADI) a través de la empresa de seguridad contratada.
C. Denunciar cualquier extravío del carnet ante las autoridades competentes y reportar el incidente a las áreas responsables dentro de la Gobernación, es obligación de los funcionarios, contratistas o terceros afectados.
D. Entregar el carnet de identificación al finalizar la vinculación laboral o contractual es necesario para todos los funcionarios y contratistas, siguiendo las directrices emitidas por el Departamento Administrativo de Desarrollo Institucional (DADI).
E. Asegurar que todas las puertas con sistemas de control de acceso permanezcan cerradas en todo momento es responsabilidad de todos los funcionarios, contratistas y terceros. No se deben dejar las puertas abiertas sin supervisión. El acceso al Datacenter estará restringido únicamente a personas autorizadas por la Secretaría de las TIC
F. Cumplir con las regulaciones de seguridad y los procedimientos de control de acceso establecidos por la empresa de seguridad contratada por el Departamento Administrativo de Desarrollo Institucional (DADI) es deber de todos los funcionarios, contratistas y terceros involucrados con la entidad.

5.3.17. Política de seguridad en áreas restringidas.

Las siguientes áreas deben ser consideradas cómo restringidas:

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

- Centro de Datos
- Salas de control y monitoreo
- Oficinas de Hacienda y Finanzas Públicas
- Oficinas legales
- Oficinas de alta gerencia
- Archivo, áreas de recepción y entrega de correspondencia.
- Cuartos de telecomunicaciones
- Cualquier área que albergue información sensible o crítica para la organización.

A. Estas zonas deberán estar equipadas con dispositivos de seguridad física y ambiental, así como, con controles de acceso adecuados para salvaguardar la información de la Gobernación del Valle del Cauca.
B. En los espacios que alberguen activos de información, es imperativo cumplir con los siguientes lineamientos como requisito mínimo:
   1. Está prohibido el acceso sin la autorización correspondiente. Cualquier individuo autorizado para entrar a las áreas debe registrar sus datos en la planilla designada tanto al ingresar como al salir de las mismas.
   2. Está prohibida la ingesta de alimentos o bebidas en estas áreas.
   3. Está prohibida la introducción de elementos inflamables a estas áreas.
   4. Para mantener la seguridad y confidencialidad de la entidad, es esencial controlar estrictamente el acceso de visitantes externos. Todo individuo que no sea miembro de la entidad debe estar acompañado por un funcionario durante toda la duración de su visita, garantizando así su supervisión y evitando cualquier acceso no autorizado a información sensible o áreas restringidas.
   5. Es fundamental abstenerse de guardar objetos o elementos que no estén relacionados con las funciones propias del área designada como restringida.
   6. Queda estrictamente prohibido tomar fotografías o grabaciones en las áreas restringidas sin obtener previamente la autorización correspondiente del área responsable de cada una de ellas.
   7. No se permitirá la entrada de equipos electrónicos ni de maletas o contenedores a estas áreas, a menos que se justifique su ingreso. En tal caso, se requerirá su registro tanto al entrar como al salir, con el fin de minimizar la posibilidad de ingreso de elementos no autorizados o la extracción de objetos no permitidos.
   8. Las áreas designadas como seguras deben tener condiciones ambientales óptimas que garanticen el correcto funcionamiento de los equipos y el estado de los medios que almacenan información crítica. Además, es imperativo contar con un sistema eficaz de detección y control de incendios. Es fundamental que la Gobernación del Valle del Cauca mantenga estas medidas de seguridad para salvaguardar la integridad de sus activos de información y proteger la información sensible de la entidad.
   9. El acceso al Data Center de la Gobernación del Valle del Cauca debe estar restringido y garantizar la seguridad de la información mediante un sistema de control de acceso. Para ello, se debe implementar un sistema biométrico de huella dactilar, tarjetas de proximidad o claves autorizadas para el ingreso del personal autorizado. Esta medida busca salvaguardar la integridad de los datos y garantizar que solo el personal

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

autorizado tenga acceso a las instalaciones del centro de datos, fortaleciendo así la seguridad de la información de la entidad gubernamental.

5.3.18. Política de seguridad y mantenimiento de equipos tecnológicos.

La Política de Seguridad y Mantenimiento de Equipos Tecnológicos de la Gobernación del Valle del Cauca establece directrices esenciales para la protección y conservación de los equipos tecnológicos. Su propósito es asegurar la integridad, disponibilidad y seguridad de la infraestructura tecnológica mediante la implementación de controles físicos y digitales, la responsabilidad de los usuarios, y el mantenimiento periódico de los equipos. Además, la política contempla la gestión de seguros para respaldar la continuidad operativa y la reposición de activos en caso de pérdida o daño. Esta política garantiza que los equipos tecnológicos sean utilizados y mantenidos adecuadamente para prevenir riesgos y asegurar el funcionamiento óptimo de los sistemas de información.

A. Los equipos que forman parte de la infraestructura tecnológica de la Gobernación del Valle del Cauca deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado. Es esencial que estos equipos estén bien posicionados y seguros para garantizar la integridad y disponibilidad de la información, así como, para evitar cualquier amenaza que pueda comprometer su funcionamiento o la seguridad de los datos almacenados en ellos.
B. La Entidad implementará los controles necesarios para asegurar que los equipos se mantengan alejados de lugares con riesgos potenciales, tales como incendios, explosivos, agua, polvo, vibraciones, interferencias electromagnéticas y actos de vandalismo, entre otros.
C. Todos los funcionarios y contratistas serán responsables del uso adecuado de los equipos de escritorio, portátiles y móviles que se les hayan asignado. Por lo tanto, estos equipos no deberán ser prestados a personas no autorizadas o ajenas a la Gobernación del Valle del Cauca.
D. Es fundamental garantizar que la infraestructura utilizada para el procesamiento de la información, las comunicaciones y la seguridad informática, reciba mantenimientos periódicos para evitar que se vean afectados por la obsolescencia. Por ello, la Gobernación del Valle del Cauca revisará constantemente la vida útil de cada uno de los recursos que componen dicha infraestructura, siguiendo las descripciones y recomendaciones de sus fabricantes.
E. Los equipos portátiles de la entidad deben tener un mecanismo de seguridad, tanto físico como digital, para protegerlos dentro y fuera de las instalaciones de la Gobernación del Valle del Cauca. El funcionario o contratista a quien se le asigne el equipo se hace responsable del cuidado e integridad física del mismo.
F. La Gobernación del Valle del Cauca debe gestionar pólizas o seguros que permitan la reposición de los activos de información necesarios para respaldar los planes de contingencia y garantizar la continuidad de los servicios.

5.3.19. Política de uso de dispositivos móviles.

Esta política establece directrices para el uso seguro de dispositivos móviles, incluyendo portátiles, teléfonos y tabletas, dentro de la entidad. Su objetivo es proteger la información institucional mediante controles de acceso, mecanismos de respaldo y medidas de

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

seguridad específicas. Se debe asegurar que todos los dispositivos cuenten con software antivirus, que las conexiones a la infraestructura tecnológica estén autorizadas y que se minimicen riesgos asociados al uso de redes públicas y almacenamiento de datos no autorizados. Estas medidas garantizan la integridad y seguridad de la información en todo momento.

A. Para el uso de dispositivos de computación móvil como equipos portátiles, teléfonos móviles, tabletas, entre otros, se deben implementar controles de acceso u otros mecanismos que se consideren necesarios y pertinentes para garantizar la Seguridad de la Información.
B. Los dispositivos móviles de la entidad deben contar con un software de antivirus instalado para garantizar la seguridad de los datos. Además, los dispositivos personales que utilicen servicios de la entidad deberán contar con sistemas operativos licenciados y un software antivirus proporcionado por los usuarios para cumplir con los estándares de seguridad requeridos.
C. La conexión de los dispositivos móviles a la infraestructura tecnológica institucional debe ser autorizada por la Secretaría de las TIC, tras verificar que cumplan con las condiciones de seguridad necesarias, estableciendo los mecanismos de control adecuados para proteger la infraestructura tecnológica de la entidad.
D. Los equipos portátiles deben configurarse para que, después de cinco (5) minutos de inactividad, pasen automáticamente al modo de suspensión. Esto activará el bloqueo de la pantalla, el cual requerirá que el usuario introduzca su contraseña para desbloquearla.
E. Para garantizar la seguridad de la información de la entidad, los funcionarios, contratistas y terceros involucrados con la entidad deben restringir el uso de redes inalámbricas públicas a situaciones estrictamente necesarias. Además, deben deshabilitar las conexiones Bluetooth e infrarrojas en los dispositivos móviles de la entidad mientras no sean necesarias. Estas medidas sólo deben autorizarse y utilizarse para actividades laborales específicas.
F. Los funcionarios, contratistas y terceros involucrados con la entidad deben evitar la conexión de los dispositivos móviles de la entidad, a través de sus diferentes puertos físicos, a cualquier red o equipo público, de hoteles o cafés internet, entre otros, para protegerlos de posibles infecciones de malware.
G. Los funcionarios, contratistas y terceros involucrados con la entidad no deben almacenar vídeos, fotografías o información personal en los dispositivos móviles asignados, de la entidad, a menos que sean requeridos para el ejercicio de las actividades asignadas, siguiendo todas las medidas de seguridad de la información.
H. El uso de los equipos de cómputo portátiles de la Gobernación del Valle del Cauca, fuera de las instalaciones de la entidad, únicamente se permitirá a usuarios autorizados, y dichos equipos deben contar con productos vigentes y actualizados de protección de punto final (antivirus y las que se consideren necesarias de forma adicional).

5.3.20. Política de teletrabajo y trabajo en casa.

Los funcionarios, contratistas y terceros involucrados con la entidad recibirán de sus respectivas dependencias en las que desempeñen sus actividades en la Gobernación del Valle, los equipos de cómputo o dispositivos a utilizar para conectarse a la infraestructura tecnológica de la Entidad, de forma concertada, con el fin de realizar sus labores funcionales

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

o contractuales, ya sea en el sitio de teletrabajo o trabajo en casa, tanto en Colombia como en el extranjero, según la modalidad de contratación. En cualquiera de los equipos de cómputo acordados entre las partes, los funcionarios, contratistas y terceros involucrados con la entidad deberán garantizar la seguridad física de dichos equipos en la residencia o lugar donde ejercerán sus funciones y obligaciones. Para ello, se deberán seguir las recomendaciones establecidas:

A. Gobernación del Valle del Cauca.

1. La Entidad debe implementar canales de comunicación seguros, como VPN con cifrado SSL/TLS, para garantizar que todos los funcionarios, contratistas y terceros involucrados con la entidad puedan establecer conexiones seguras durante el teletrabajo o trabajo en casa.
2. Implementar soluciones de almacenamiento, como Drive corporativo, para guardar los archivos de los funcionarios, contratistas y terceros involucrados con la entidad, en la nube.
3. Activar perfiles de navegación para los usuarios que utilicen VPN con cifrado SSL/TLS permitidos.
4. Realizar monitoreos permanentes a la infraestructura de los servicios utilizados por los teletrabajadores, con el fin de analizar posibles acciones no autorizadas.
5. Establecer conexiones VPN con cifrado SSL/TLS para garantizar un acceso seguro y protegido a los usuarios, desde los equipos de cómputo asignados por la entidad o desde sus equipos personales. Dentro de las medidas de seguridad de los equipos de cómputo se debe contar con protección de antivirus, actualización de parches de seguridad del sistema operativo entre otros controles. La implementación de estas medidas mitiga los riesgos potenciales asociados con las amenazas cibernéticas y las vulnerabilidades del sistema, asegurando que los usuarios puedan acceder de manera segura y protegida a los recursos de la red autorizados por la entidad.
6. Es fundamental implementar medidas de seguridad efectivas en caso de pérdida de dispositivos para garantizar la protección de la información de la entidad. Estas acciones son cruciales para mitigar riesgos y asegurar que los datos sensibles estén protegidos adecuadamente en todo momento.

B. Funcionarios, contratistas y terceros.

1. Se deben cambiar regularmente las claves de acceso al WiFi y evitar el uso de redes inalámbricas abiertas para reducir el riesgo de pérdida de información sensible durante la transmisión de datos.
2. Realizar copias de seguridad periódicas utilizando los medios de almacenamiento proporcionados por la entidad para asegurar la integridad y disponibilidad de los datos críticos.
3. Es fundamental evitar el envío de archivos que contengan información de la entidad a través de canales no oficiales como WhatsApp, Dropbox, WeTransfer o correos de dominio gratuito con el fin de mantener la seguridad de los datos, protegiendo la información sensible al transmitirse únicamente por medios autorizados y de confianza.
4. Es fundamental asegurarse de cerrar la sesión cuando el dispositivo no esté en uso, ya sea en entornos domésticos o en lugares públicos. Esta medida contribuye

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

significativamente a la seguridad al proteger los datos sensibles y evitar accesos no autorizados.

5. Es fundamental mantener actualizado el sistema operativo con los últimos parches de seguridad proporcionados por el fabricante, especialmente si se está utilizando un dispositivo personal para acceder a la conexión por VPN con cifrado SSL/TLS. Esta práctica ayuda a mitigar vulnerabilidades y protege la integridad de los datos durante la conexión remota, asegurando un entorno más confiable para el intercambio de información sensible.
6. Se debe implementar y mantener actualizado un software antivirus de un fabricante reconocido para prevenir infecciones de malware y software malicioso al conectarse a través de VPN con cifrado SSL/TLS. Este paso es fundamental para garantizar la seguridad de la red y proteger la integridad de los datos durante las sesiones de conexión remota.
7. Es fundamental contar con un entorno de trabajo seguro al teletrabajar, minimizando riesgos como la pérdida de información debido a posibles daños en los equipos, resultantes de la manipulación inapropiada de alimentos en su uso.
8. Es crucial evitar la instalación de programas o extensiones de navegadores provenientes de fuentes desconocidas, ya que estos suelen estar infectados con malware que puede comprometer la seguridad de los dispositivos y exponer información sensible.
9. Se prohíbe el uso de aplicaciones de escritorio remoto no autorizadas por la entidad, ya que estas pueden crear accesos no controlados que comprometan la seguridad de los datos y sistemas, poniendo en riesgo tanto el servicio como las credenciales de los usuarios. Esta medida refuerza las validaciones de seguridad mínimas requeridas al conectarse a través de VPN con cifrado SSL/TLS, como mantener un antivirus actualizado y aplicar parches de seguridad, creando así un entorno más protegido contra posibles amenazas.
10. Cuando se trabaja desde casa, es fundamental asegurar la protección de los datos y cumplir con las políticas de seguridad establecidas por la Secretaría de las TIC y la legislación vigente sobre protección de datos personales.
11. Las demás instrucciones dadas en este documento.

C. Es fundamental que los funcionarios, contratistas y terceros involucrados con la entidad cumplan con los lineamientos de seguridad establecidos por la Secretaría de las TIC. Esto asegura la protección contra posibles vulnerabilidades, intrusiones o ataques a la infraestructura tecnológica de la entidad, mientras desempeñan sus labores en modalidades de teletrabajo o trabajo desde casa. En consecuencia, es recomendable que los equipos personales dispongan de antivirus actualizados, así como de sistemas operativos debidamente licenciados y con las últimas actualizaciones de seguridad aplicadas.

D. Los funcionarios, contratistas y terceros involucrados con la entidad deben asegurarse de conectarse a internet mediante una red privada desde su lugar de residencia o ubicación remota, para garantizar una conectividad confiable desde su equipo o dispositivo personal, asegurando así el tráfico e integridad de los datos.

E. Es fundamental que tanto los funcionarios, contratistas y terceros involucrados con la entidad, implementen medidas de seguridad para proteger la información y prevenir accesos no autorizados a recursos o datos sensibles, especialmente cuando utilizan

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

equipos o dispositivos personales autorizados por la entidad. Estas medidas deben asegurar que el acceso esté permitido únicamente a los usuarios autorizados, minimizando así riesgos potenciales derivados del uso compartido de equipos o dispositivos.

F. Para los funcionarios, contratistas y terceros involucrados con la entidad que trabajan bajo la modalidad de teletrabajo y utilizan los equipos proporcionados por la entidad, es fundamental que estos dispositivos sean utilizados exclusivamente por el teletrabajador asignado. Al finalizar el objeto contractual o las actividades asignadas, el teletrabajador deberá devolver los equipos a la entidad, en buen estado, a excepción del desgaste normal por el uso habitual.
G. Mientras los funcionarios, contratistas y terceros involucrados con la entidad accedan a los recursos privados o confidenciales de la entidad a través de VPN con cifrado SSL/TLS, no deben utilizar simultáneamente el equipo o dispositivo para acceder a otros servicios o sitios web, como redes sociales o servicios de streaming de video. Estas actividades pueden saturar la red de la entidad y causar problemas de ciberseguridad. Si no se cumple con este lineamiento se expondrá a la restricción del acceso a la VPN.
H. Para los funcionarios, contratistas y terceros involucrados con la entidad que trabajen bajo la modalidad de teletrabajo, es fundamental que se adhieran a las configuraciones y restricciones establecidas por la Secretaría de las TIC respecto a los equipos proporcionados por la entidad. Asimismo, deberán cumplir con las configuraciones de conectividad proporcionadas por la entidad.
I. Los funcionarios, contratistas y terceros involucrados con la entidad que necesiten salir del país por motivos personales, durante la vigencia de su contrato laboral con la entidad, deberán informar a la entidad sobre su traslado y la ubicación de la ciudad de destino. Esto permitirá a la entidad tener conocimiento de los accesos desde el extranjero y garantizar un control adecuado de la seguridad de la información, dado los riesgos y amenazas de ciberseguridad que pueden surgir desde otros países. Asimismo, se debe cumplir con los apartados previamente mencionados.

5.3.21. Política de control de acceso físico.

La Política de Control de Acceso Físico de la Gobernación del Valle del Cauca tiene como objetivo garantizar la seguridad y protección de nuestras instalaciones al limitar el acceso exclusivamente al personal y visitantes autorizados. Esta política establece procedimientos claros para el registro de dispositivos electrónicos, control de acceso fuera del horario laboral y durante fines de semana, así como, la gestión del ingreso de visitantes y la prohibición de animales en zonas seguras. La implementación efectiva de estas normas asegura un entorno seguro y controlado, previniendo riesgos y protegiendo nuestros recursos.

A. El acceso a las instalaciones de la Gobernación del Valle del Cauca debe estar estrictamente limitado al personal autorizado.
B. El personal de vigilancia de la Entidad debe registrar los dispositivos electrónicos, tales como portátiles, torres de computador y video beams, entre otros. Este registro debe incluir la marca, modelo y número de serie (o su equivalente) del equipo, y aplicarse a funcionarios, contratistas y terceros involucrados con la entidad. El registro se efectuará

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

tanto al ingreso como a la salida de las instalaciones de la Gobernación del Valle del Cauca.

C. El ingreso de funcionarios, contratistas y terceros involucrados con la entidad, a las instalaciones de la Gobernación del Valle del Cauca, durante los fines de semana debe contar con autorización previa.
D. Cualquier ingreso de funcionarios, contratistas y terceros involucrados con la entidad a las instalaciones de la Gobernación del Valle del Cauca de lunes a viernes después de las 5:30 p.m., debe ser concertado y autorizado previamente con la respectiva dependencia a donde se va ingresar.
E. Sin excepción, todos los visitantes deben llegar al sitio designado para el registro de visitantes (recepción de las instalaciones) y ser dirigido por el personal de vigilancia.
F. El registro de visitantes debe incluir el nombre y la identificación del visitante, la fecha y hora de entrada y salida, así como, el nombre de la dependencia al que se dirige.
G. Un visitante no tiene la autorización para validar la entrada de otro visitante.
H. En las zonas seguras, estará estrictamente prohibida la presencia de animales bajo cualquier circunstancia.
I. Los visitantes que necesiten acceder a áreas seguras controladas por lectores de tarjetas de acceso, como el centro de datos, deben solicitar acceso temporal previamente al funcionario o contratista responsable de autorizar su entrada.

5.3.22. Política de gestión de incidentes de seguridad de la información.

Un incidente de seguridad de la información se define como cualquier evento que cause daño o represente una amenaza significativa para la infraestructura de información y tecnología de la Gobernación del Valle del Cauca, abarcando sistemas de cómputo, sistemas de información y sistemas de telefonía. Ejemplos de tales incidentes incluyen la interrupción de servicios, la inhabilitación de sistemas de información, así como, cambios no autorizados en hardware, firmware, software o datos, conforme a lo establecido por la Ley 1273 de 2009 y otras normativas aplicables a la Entidad.

A. Todo funcionario, contratista o tercero debe notificar a la Secretaría de las TIC de la Gobernación del Valle del Cauca cualquier incidente relacionado con la seguridad de la información de la entidad, siguiendo las directrices de la Guía vigente de Gestión de Incidentes del MinTIC. La Secretaría de las TIC, además de realizar un monitoreo constante para la detección proactiva de incidentes, debe realizar una gestión interna que incluya el registro, clasificación y seguimiento de los mismos, según los lineamientos del MinTIC. La Secretaría de las TIC debe liderar la gestión, trámite y respuesta, colaborando con otras áreas y, si es necesario, escalando a entidades externas como el CSIRT Gobierno o COLCERT, según los lineamientos internos establecidos, para llevar a cabo acciones de investigación, análisis, contención, erradicación, recuperación y lecciones aprendidas.
B. La Secretaría de las TIC es responsable del aislamiento y la recuperación de accesos a sistemas de comunicaciones y cómputo afectados por incidentes. Dependiendo de la naturaleza del incidente, podrán convocarse niveles directivos de la Entidad, áreas de control interno, así como, equipos jurídicos o técnicos especializados.
C. Cuando sea viable, la Secretaría de las TIC implementará procedimientos destinados a prevenir incidentes, supervisar y filtrar anomalías que puedan comprometer la seguridad de la información y los recursos tecnológicos de la entidad.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

D. La Secretaría de las TIC continuará implementando procedimientos para responder e investigar diversos incidentes de seguridad de la información, garantizando además la adecuada custodia de las evidencias recolectadas durante dichas investigaciones.
E. Es responsabilidad de cada funcionario, contratista o tercero, informar de manera inmediata cualquier incidente de seguridad o situación sospechosa que pueda poner en riesgo la confidencialidad, integridad o disponibilidad de la información.
F. En situaciones donde los incidentes reportados puedan constituir un delito, se deberá informar a las autoridades competentes, como la Fiscalía General de la Nación o la Policía Nacional, quienes llevarán a cabo la investigación y, si es necesario, la prosecución legal correspondiente.
G. Es esencial llevar un registro minucioso de los incidentes de Seguridad de la Información, incluyendo las respuestas implementadas para cada uno de ellos. Este registro debe comprender una evaluación de los daños ocasionados y, en la medida de lo posible, una valoración detallada de los mismos.

5.3.23. Política de controles criptográficos.

La Política de Controles Criptográficos establece directrices para proteger la información digital clasificada como reservada mediante el uso de cifrado. Su propósito es garantizar la confidencialidad e integridad de los datos a lo largo de su transmisión, almacenamiento y recepción. Esta política define los estándares para la implementación de medidas criptográficas, el uso de certificados digitales, y el cumplimiento de normativas vigentes. Los controles criptográficos son esenciales para salvaguardar la información sensible de la Gobernación del Valle del Cauca y asegurar la confianza en las transacciones electrónicas.

A. La Gobernación del Valle del Cauca, a través de la Secretaría de las TIC, se debe asegurar de que la información digital clasificada como reservada sea cifrada durante su transmisión, almacenamiento y recepción, garantizando así la preservación de su confidencialidad e integridad.
B. La Secretaría de las TIC debe establecer, implementar y difundir los estándares para la aplicación de controles criptográficos.
C. Los certificados de sitio seguro y los certificados de firma digital deben ser emitidos por una Autoridad Certificadora que garantice la autenticidad y validez de la asociación entre el responsable del certificado y el certificado mismo.
D. La duración de los certificados de sitio seguro y los certificados de firma digital emitidos por la entidad certificadora de la Secretaría de las TIC debe ser de al menos un año desde la fecha de su emisión. Cuando los certificados caduquen, deben ser actualizados dependiendo de su relevancia y utilidad.
E. La Secretaría de las TIC tendrá en cuenta y dará cumplimiento a la legislación y marcos normativos vigentes cuando se utilizan sistemas criptográficos sobre la información, en especial la Ley 594 de 2000 (Ley General de Archivo), la Ley 527 de 1999 (Acceso y Uso de Mensajes de datos) y el Decreto 1747 de 2000 (Secure Data Colombia), Ley 1273 (Ley de delitos Informáticos), Ley 1581 de 2012 (Protección de Datos personales), Ley 1712 de 2014 Transparencia de datos, Ley 1581 habeas data y demás reglamentación que cobije la protección de datos en Colombia.
F. Es fundamental establecer criterios de evaluación para la implementación de controles criptográficos destinados a la protección de información. Estos criterios permitirán

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

verificar la adecuación y efectividad de las medidas criptográficas empleadas, asegurando así la confidencialidad e integridad de los datos sensibles.

Es necesario aplicar cifrado a los datos cuando:

A. Los dispositivos de la Gobernación del Valle del Cauca que contienen información confidencial se usarán por fuera de la entidad.
B. Se envía un correo electrónico con información reservada.
C. Se tiene un sitio web público en el que todos los usuarios puedan acceder mediante la introducción de nombre de usuario y contraseña.
D. Se tiene un sitio web desde el que se realizan trámites financieros.
E. Los funcionarios, contratistas y terceros involucrados con la entidad se conectan con la red corporativa desde casa para acceder a los recursos de la entidad.
F. Se emiten certificados digitales para garantizar la confianza entre emisor y receptor (Cuando exista entidad certificadora en común).
G. Se emitan llaves de cifrado públicas y/o privadas para realizar transferencia de información reservada entre las partes.
H. Se emiten tokens con firmas digitales para propósitos específicos.

5.3.24. Política gestión de seguridad en las redes.

Esta política contempla un conjunto integral de lineamientos que buscan proteger la infraestructura de red y los datos por medio de diferentes medidas de seguridad. Esto incluye la protección de servicios prioritarios, la segmentación de la red, el uso de VPN para conexiones remotas seguras y la implementación de medidas de seguridad en sistemas de acceso público, garantizando así la continuidad de las operaciones y la confianza de los usuarios.

5.3.25. Medidas de seguridad en redes.

A. La Secretaría de las TIC debe establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos transmitidos a través de redes públicas o inalámbricas.
B. La Secretaría de las TIC debe establecer las responsabilidades y lineamientos necesarios para la gestión adecuada de los equipos de redes.
C. Los usuarios de la red interna de la Gobernación del Valle del Cauca no están autorizados para realizar o ejecutar acciones que son exclusivas de los administradores de red.
D. Los funcionarios, contratistas y terceros, no deben realizar ningún tipo de instalación de líneas telefónicas, canales de transmisión de datos, equipos tecnológicos para la interconexión de dispositivos en la red, ni cambiar su configuración sin haber obtenido la aprobación formal de la Secretaría de las TIC.

5.3.25.1. Protección de servicios de red.

A. La Secretaría de las TIC debe garantizar la confidencialidad de la información sobre el direccionamiento y enrutamiento de las redes de datos de la Gobernación del Valle del Cauca.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

B. La Secretaría de las TIC deberá implementar medidas de protección entre las redes internas y cualquier red externa de la Gobernación del Valle del Cauca para salvaguardar la integridad de la información institucional frente a posibles amenazas externas. Para este propósito, se recomienda el uso de dispositivos de seguridad perimetral, como firewalls y sistemas de detección de intrusos, asegurando así un ambiente seguro para la comunicación y el intercambio de datos.
C. Es crucial garantizar que los proveedores de servicios de redes implementen mecanismos de seguridad robustos. Esto implica asegurarse de que las redes sean protegidas adecuadamente contra posibles vulnerabilidades y amenazas cibernéticas.

5.3.25.2. Segmentación de redes.

A. La Secretaría de las TIC debe implementar una estrategia de segmentación de redes adaptada a los diferentes niveles de seguridad y tráfico requeridos por los sistemas que operan bajo su responsabilidad.
B. La Gobernación del Valle del Cauca debe organizar las redes y grupos de servicios de información en dominios lógicos de red separados, cada uno protegido por perímetros de seguridad claramente definidos.
C. Cada dominio que se cree debe recibir aprobación por parte de la Secretaría de las TIC y debe ser registrado en la topología de la red de datos de la entidad. Es crucial que este proceso garantice la integridad y seguridad de la infraestructura tecnológica, asegurando así que todos los dominios sean correctamente integrados y gestionados dentro del entorno de red.
D. Las redes inalámbricas deben estar segregadas de la red principal de usuarios para mitigar posibles riesgos en los activos de información. Es fundamental implementar controles rigurosos de acceso y garantizar autenticación segura en todos los puntos de conexión a estas redes, asegurando así la protección integral de los datos y sistemas involucrados.

5.3.25.3. Conexión remota mediante red privada virtual (VPN).

A. La Secretaría de las TIC debe asegurar que cualquier conexión remota a la red interna de la Gobernación del Valle del Cauca se realice utilizando exclusivamente una conexión VPN con cifrado SSL/TLS proporcionada por la entidad. Es fundamental garantizar la seguridad de las comunicaciones para proteger la integridad y confidencialidad de la información sensible gestionada por la administración pública.
B. La Secretaría de las TIC deberá implementar métodos efectivos de autenticación para los usuarios que accedan de manera remota.
C. Toda solicitud para la creación de una VPN con cifrado SSL/TLS debe ser tramitada por medio de los canales designados para tal fin (herramienta de mesa de ayuda, correo electrónico institucional o extensión de soporte vigente) y debe incluir la autorización correspondiente del jefe inmediato del funcionario, contratista o tercero involucrado. Este proceso asegura que las conexiones VPN dentro de la organización se establezcan de manera formal y con el respaldo adecuado de las autoridades competentes.
D. Al establecer conexiones VPN haciendo uso de equipos ajenos a la Entidad, las y los usuarios entienden y aceptan que sus equipos de cómputo son una extensión de la red de datos de la Gobernación del Valle del Cauca, y por esta razón deben cumplir con las mismas políticas que aplican para los equipos propiedad de la entidad.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

E. Es responsabilidad de los usuarios que emplean servicios de VPN con cifrado SSL/TLS garantizar que accesos no autorizados a las redes internas de datos de la Gobernación del Valle del Cauca sean prevenidos.
F. Las conexiones por VPN con cifrado SSL/TLS se eliminarán si no se utilizan durante un período de 30 días sin una justa causa proporcionada por correo electrónico a la Secretaría de las TIC solicitando su reserva. Una vez transcurrido este tiempo, si se requiere nuevamente la conexión por VPN, se deberá realizar todo el proceso de solicitud de creación mencionado en el literal C.

5.3.25.4. Sistemas de acceso público.

A. La información pública generada por las dependencias de la Entidad deberá ser protegida contra cualquier posible modificación que pueda comprometer la imagen institucional.
B. El portal institucional debe incluir tanto la política de privacidad y uso, como la política de seguridad de la información. Estas políticas son esenciales para garantizar la protección de los datos personales de los usuarios y definir las medidas de seguridad que se implementarán para salvaguardar la información del portal.
C. Toda la información publicada en el portal institucional o en cualquier otro medio deberá contar con la revisión y aprobación de la Secretaría de las TIC para asegurar su calidad y coherencia.

5.3.26. Política de activos de información, clasificación y etiquetado de la información.

Los activos de información de la Gobernación del Valle del Cauca deben ser identificados, clasificados de acuerdo con los requisitos legales vigentes y valorados según los criterios de confidencialidad, integridad y disponibilidad, para determinar su criticidad y proporcionarles el tratamiento adecuado, teniendo en cuenta lo siguiente:

A. La persona responsable de la información debe clasificarla adecuadamente y, a su vez, informar a la dependencia de la entidad encargada del proceso de clasificación. Esto garantiza que se adopten las medidas necesarias para preservar la confidencialidad, integridad y disponibilidad de la información.
B. Todos los aplicativos o sistemas de información deben tener un responsable designado, encargado de definir los niveles de privacidad de la información y de determinar los usuarios y los permisos que cada uno debe tener.
C. La persona responsable de la información debe actualizar su clasificación conforme a los cambios que se produzcan en la entidad.
D. El responsable de la información tiene la autonomía para reclasificar cuando lo considere necesario, lo que implica cambiar su rótulo o etiqueta y notificar a todos los usuarios afectados.
E. Todos los funcionarios, contratistas y terceros involucrados con la entidad tienen la responsabilidad de familiarizarse y cumplir con todos los aspectos de la política de seguridad de la información. Si surgen dudas respecto al manejo adecuado de la información, estas deben ser consultadas con el responsable de la información.
F. La información debe ser etiquetada de forma clara y precisa, indicando su nivel de clasificación de seguridad. Es esencial que todos los funcionarios, contratistas y terceros involucrados con la entidad conozcan y respeten estas clasificaciones. Para garantizar

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

una correcta implementación, se deben seguir rigurosamente los lineamientos vigentes establecidos en la entidad y utilizar únicamente los instrumentos de etiquetado revisados y aprobados por calidad.

G. Se deben utilizar los mecanismos apropiados de control de acceso a la información dependiendo de su nivel de clasificación.
H. Los funcionarios, contratistas y terceros involucrados con la entidad no pueden utilizar la información reservada o clasificada cuando dejan de trabajar o prestar sus servicios en la Entidad.
I. Cuando la información clasificada como reservada ya no sea necesaria, se debe solicitar formalmente su destrucción o desclasificación al área o persona responsable de la gestión de la información clasificada dentro de la entidad, siguiendo los procedimientos establecidos y asegurando el cumplimiento de las normativas y políticas internas aplicables.
J. Al enviar equipos para mantenimiento o al asignarlos a una persona diferente, si contienen información reservada o clasificada, dicha información debe transferirse al nuevo equipo donde se seguirá utilizando y borrarse del equipo original. De esta forma, se garantiza que la información no podrá ser recuperada o utilizada de forma indebida en el equipo original.
K. La información reservada o clasificada alojada en medios magnéticos (como discos externos, USB, entre otros), debe ser eliminada antes de su reutilización, transferencia o disposición final, utilizando métodos de borrado seguro aprobados por la entidad. En caso de necesitar desechar el medio o equipo, se debe seguir el lineamiento establecido por la entidad, que puede incluir la destrucción física certificada o la devolución al proveedor autorizado.
L. Los dispositivos móviles con acceso a información confidencial no deben almacenar esta información en sus discos duros internos para evitar el riesgo de acceso no autorizado en caso de pérdida de los equipos. En su lugar, deben usar un almacenamiento seguro en la nube designado por la entidad.
M. Todas las entidades vinculadas contractual o comercialmente con la Gobernación del Valle del Cauca tienen prohibido divulgar información reservada o clasificada a terceros sin la autorización previa y expresa del titular o responsable de la información y la firma de un acuerdo de confidencialidad por parte del receptor, garantizando su adecuada protección.
N. Con el objetivo de llevar a cabo el inventario, clasificación y etiquetado de los activos de información de la Gobernación del Cauca, los responsables deben emplear un instrumento que permita desarrollar esta actividad con una metodología clara, eficiente y alineada con la normativa vigente que cubra a las entidades del orden territorial.
O. El inventario de los activos de información de la entidad, debe actualizarse al menos una vez por año o cada vez que se incorpore un nuevo activo de información.
P. Al intercambiar bases de datos que contengan información sensible o reservada, es fundamental aplicar técnicas de protección de privacidad como la seudonimización o anonimización de datos, conforme a la legislación vigente. La seudonimización reemplaza identificadores directos por indirectos, permitiendo el análisis de datos con menor riesgo de reidentificación, mientras que la anonimización modifica irreversiblemente los datos para imposibilitar la identificación de individuos. La elección

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

entre ambas dependerá del propósito del intercambio y el nivel de riesgo, y siempre deben implementarse medidas de seguridad adicionales.

5.3.26.1. Uso Adecuado de los Activos de Información para la Gobernación del Valle del Cauca.

El uso de los activos de información proporcionados por la Gobernación del Valle del Cauca conlleva la aceptación expresa, por parte de los usuarios, de las políticas, normas y estándares diseñados para garantizar la seguridad de la información y el correcto aprovechamiento de estos recursos. Al acceder a estos activos, cada usuario asume la responsabilidad de cumplir con las disposiciones establecidas y se compromete a proteger la integridad, confidencialidad y disponibilidad de la información institucional. Este compromiso también incluye adoptar buenas prácticas y medidas preventivas que contribuyan a la salvaguardia de los datos, en alineación con los lineamientos establecidos por la entidad.

Los siguientes se consideran actos no autorizados para el uso de los activos informáticos de la Gobernación del Valle del Cauca y están expresamente prohibidos, así:

A. Cualquier intento o violación de los controles de seguridad establecidos para proteger los activos de información de la Gobernación del Valle del Cauca se considera una amenaza a su integridad.
B. Evitar cualquier acción que pueda poner en riesgo la seguridad de los activos de información de la Gobernación del Valle del Cauca.
C. El acceso y la utilización no autorizada de los recursos informáticos de la Gobernación del Valle del Cauca.
D. El acceso no autorizado o inapropiado a la infraestructura tecnológica de la Gobernación del Valle del Cauca.
E. Intentar acceder sin autorización a sistemas, redes o cuentas, eludiendo las medidas de seguridad o autenticación establecidas.
F. El uso indebido de las contraseñas, firmas digitales o dispositivos de autenticación.
G. El acceso a servicios informáticos con cuentas o métodos de autenticación de otros usuarios está prohibido, incluso con el consentimiento explícito del titular de la cuenta.
H. Almacenamiento, instalación, configuración o uso de software no autorizado o datos sin permisos en los activos de información de la Gobernación del Valle del Cauca.
I. Está prohibido el uso, distribución o ejecución de software malicioso que pueda causar daño, hostigamiento, alteración de información, interrupción de servicios informáticos o comprometer la seguridad de los sistemas de información.
J. El hurto, robo, sustracción o uso no autorizado de datos, información, materiales, equipos y otros activos de información de la Gobernación del Valle del Cauca.
K. Está prohibido sacar activos de información de las instalaciones de la Gobernación del Valle del Cauca o sus áreas administradas sin contar con la autorización previa correspondiente.
L. El ingreso, modificación o alteración sin autorización de elementos, datos o información de los activos informáticos de la Gobernación del Valle del Cauca.
M. El uso de medios electrónicos, medios de almacenamiento, software, hardware, datos o información en medios digitales provenientes de fuentes no certificadas o

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

de terceros sin la previa revisión o autorización de la Secretaría de las TIC y/o el Oficial de Seguridad de la Información.

N. El uso del servicio de internet debe realizarse exclusivamente para fines legales y autorizados. Se prohíbe la transmisión, distribución o almacenamiento de material que infrinja derechos de autor, marcas, secretos comerciales u otros derechos de propiedad intelectual, así como, contenido obsceno, pornográfico, difamatorio o que pueda ocasionar consecuencias legales.

O. El uso del correo electrónico prohíbe: Spam, acoso (troll), bombardeo de mensajes (mailbombing), envío de comunicaciones no oficiales y suscripciones no autorizadas a listas de correo.

P. Los correos electrónicos deben ajustarse a las leyes vigentes, respetar la moralidad y las buenas costumbres, y adherirse a las normas y derechos aplicables en internet y respecto a terceros.

Q. Está prohibido almacenar o reproducir aplicaciones, programas y archivos de audio que no sean necesarios para las funciones y actividades de la dependencia o el usuario.

R. No se permite instalar, modificar ni eliminar programas utilitarios en los equipos de cómputo de la Gobernación del Valle del Cauca. La autorización o restricción de estos programas dependerá de la Secretaría de las TIC y el Operador Tecnológico.

S. Las cuentas de red en la Gobernación del Valle del Cauca deben utilizarse de manera responsable. El abuso de estos recursos compartidos que degrade su rendimiento está estrictamente prohibido.

T. Está prohibido usar la red de datos para actividades no institucionales, como obtener, mantener o difundir material publicitario o comercial, así como, para enviar cadenas de correos.

U. Divulgar información clasificada de la entidad por correo físico, electrónico o copia impresa sin la autorización adecuada y sin cumplir los protocolos establecidos.

V. Está prohibido almacenar información clasificada en cualquier medio de almacenamiento ajeno a la Gobernación del Valle del Cauca.

W. Conectar dispositivos personales, como laptops, a la red de la entidad sin contar con la autorización correspondiente.

X. Acceder sin permiso a la red de datos de la entidad a través de cualquier servicio de acceso remoto, sin la aprobación previa de la Secretaría de las TIC,

Y. Usar servicios de internet distintos a los ofrecidos por la Secretaría de las TIC en los equipos de la Entidad.

Z. Extraer de las instalaciones de la Gobernación del Valle del Cauca los equipos y documentos clasificados, tanto físicos como digitales, de forma no autorizada.

AA. Distribuir, mostrar o revelar información confidencial de la Gobernación del Valle del Cauca a individuos u organizaciones sin la debida autorización.

BB. Realizar actividades ilegales o intentar acceder sin autorización a plataformas tecnológicas de la entidad o de terceros.

CC. Está prohibido utilizar plataformas tecnológicas para difamar, dañar la reputación o afectar la imagen de la Gobernación del Valle del Cauca o de sus funcionarios.

DD. Proporcionar acceso a los activos de información a personas no autorizadas, ya sean funcionarios o terceros.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

EE. Realizar actos destinados a evadir o alterar los controles definidos en esta política de Seguridad de la Información.

A continuación, se describen algunas acciones que afectan la Seguridad y privacidad de la Información, y que ponen en riesgo su disponibilidad, confidencialidad e integridad:

A. Mantener los computadores en funcionamiento durante las horas no laborables.
B. No se debe permitir el acceso no autorizado de personas externas a las áreas restringidas o de procesamiento de información confidencial.
C. No clasificar y/o etiquetar la información.
D. No guardar bajo llave documentos impresos que contengan información clasificada al terminar la jornada laboral
E. No retirar de forma inmediata todos los documentos con información sensible que envíen a las impresoras y dispositivos de copiado.
F. Reutilizar papel con datos confidenciales, asegurarse de borrar toda la información de tableros y pizarras después de las reuniones, y verificar que no queden documentos o notas en las mesas.
G. El uso de los recursos tecnológicos de la Gobernación del Valle del Cauca para fines personales, como la promoción o el mantenimiento de actividades privadas, está prohibido.
H. Está prohibido compartir o prestar la cuenta de usuario y contraseña institucional con otras personas, ya sean funcionarios o contratistas, así como, permitir que otros utilicen estas credenciales.
I. Dejar al alcance de personas no autorizadas los dispositivos portátiles, móviles y de almacenamiento removibles, entregados para actividades propias del cumplimiento de sus funciones.
J. Consumir alimentos y bebidas, cerca de la plataforma tecnológica.
K. Conectar a la corriente regulada dispositivos diferentes a equipos de cómputo.
L. Realizar cualquier otra acción que contravenga disposiciones constitucionales, legales o institucionales.

La implementación de cualquier práctica que afecte la Seguridad de la Información conlleva la aplicación de medidas administrativas, disciplinarias y/o legales según los procedimientos vigentes. Las violaciones o sospechas de violaciones a los controles de seguridad o políticas de la información deben ser reportadas de inmediato a Secretaría TIC y/o al Oficial de Seguridad de la Información para su correspondiente gestión.

5.3.26.2. Clasificación de la información.

La información gestionada por la Gobernación del Valle del Cauca debe ser protegida para garantizar que no sea accesible ni revelada a personas, entidades o procesos no autorizados. Para ello, se implementarán medidas de seguridad adecuadas que salvaguarden la confidencialidad, integridad y disponibilidad de la información, considerando las características específicas de cada tipo de activo y los riesgos asociados.

Esta política de protección de la información se alinea con la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional (Ley 1712 de 2014), así como con la

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

Ley 1581 de 2012 (Ley de Protección de Datos Personales). En cumplimiento de estas normativas, la información puede ser considerada cómo pública, pública clasificada o pública reservada.

Es importante tener en cuenta que la clasificación de la información como pública clasificada o reservada debe estar debidamente justificada y cumplir con los requisitos establecidos en la ley. Además, los sujetos obligados deben mantener un índice actualizado de la información clasificada, incluyendo su motivación y el acto que la califica como tal.

La Gobernación del Valle del Cauca se compromete a garantizar el acceso a la información pública, facilitando su consulta y divulgación, al tiempo que protege la información reservada y confidencial mediante medidas de seguridad adecuadas y el cumplimiento estricto de la normativa vigente.

5.3.26.3. Etiquetado de la información.

Para garantizar un etiquetado coherente y efectivo de la información, se definirán criterios claros y precisos que deberán ser considerados en todo momento. Estos criterios serán establecidos en colaboración con las dependencias responsables de la gestión de la información, asegurando así una clasificación adecuada y una protección óptima de los activos de información.

- Se etiquetará el nivel de clasificación en relación con Confidencialidad, Integridad y Disponibilidad.
- Si un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado en todos sus niveles (Confidencialidad, Integridad y Disponibilidad) como NO CLASIFICADA.
- Para los activos clasificados en confidencialidad se etiquetarán como INFORMACIÓN PÚBLICA, INFORMACIÓN PÚBLICA CLASIFICADA e INFORMACIÓN PÚBLICA RESERVADA.
- Para los activos clasificados en integridad como ALTA se utilizará la etiqueta A, MEDIA, M y BAJA B.
- Para los activos clasificados en disponibilidad como ALTA se utilizará la etiqueta 1, MEDIA 2 y BAJA 3.

5.3.27. Política de adquisición, desarrollo y mantenimiento de sistemas.

Esta política tiene como objetivo proteger la confidencialidad, integridad y disponibilidad de la información, asegurando que los sistemas sean seguros y fiables a lo largo de su ciclo de vida. Mediante una gestión rigurosa y la aplicación de buenas prácticas en cada etapa, se busca mitigar riesgos y asegurar que los recursos tecnológicos contribuyan efectivamente a la seguridad y operatividad de la organización.

5.3.27.1. Adquisición de sistemas.

A. Evaluar todos los sistemas informáticos y software adquiridos previamente por la Secretaría de las TIC para asegurar que cumplen con los estándares de seguridad establecidos. Además, para poder poner en producción un Sistema de Información (S.I.), este debe cumplir con los formatos exigidos, la entrega de guiones de prueba, y contar

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

con el recibido a entera satisfacción por parte de la dependencia que lidera la contratación o el proceso que impacta dicho sistema.

B. Se deben preferir proveedores que sigan prácticas de seguridad reconocidas y que ofrezcan actualizaciones y soporte continuo.
C. Antes de la adquisición, se realizará una evaluación de riesgos para determinar cualquier impacto potencial en la seguridad de la información.

5.3.27.2. Desarrollo de sistemas.

A. Los sistemas y aplicaciones desarrollados internamente deben seguir un proceso formal de gestión de seguridad desde el inicio del ciclo de vida del desarrollo.
B. Se aplicarán pruebas de seguridad y revisiones periódicas durante el desarrollo para identificar y mitigar posibles vulnerabilidades.
C. Todo el código desarrollado deberá cumplir con estándares de seguridad reconocidos y buenas prácticas de codificación segura.

5.3.27.3. Mantenimiento de sistemas.

A. Se establecerán procedimientos para el mantenimiento regular de sistemas y aplicaciones, incluyendo la aplicación oportuna de parches de seguridad y actualizaciones.
B. La Secretaría de las TIC coordinará y supervisará las actividades de mantenimiento para asegurar que se realicen de manera adecuada y sin interrupciones significativas en el servicio.
C. Se implementarán medidas de respaldo regular y pruebas de restauración para asegurar la disponibilidad y la integridad de los datos en caso de incidentes.

5.3.28. Política de seguridad de talento humano.

La Política de Seguridad de talento humano tiene como objetivo garantizar que todos los funcionarios, contratistas y terceros involucrados con la entidad mantengan los más altos estándares de integridad y confidencialidad en el manejo de información sensible. Esta política acoge las directrices de la entidad para la selección y formación del personal, así como, para la gestión de accesos y el manejo seguro de los recursos tecnológicos.

A. Todos los funcionarios, contratistas y terceros involucrados con la entidad, deben someterse a un proceso de verificación de antecedentes para asegurar el manejo adecuado de la información sensible.
B. Se llevarán a cabo programas regulares de formación en seguridad de la información para todos funcionarios, contratistas y terceros, enfatizando la importancia de proteger los activos de información y los procedimientos para hacerlo.
C. Se establecerá y comunicará los lineamientos de uso aceptable de los recursos de tecnología de la información, especificando las prácticas permitidas y prohibidas para garantizar el uso adecuado y seguro de los sistemas informáticos y de red.
D. Se implementará un mecanismo seguro para la gestión de identidades y accesos, que incluya la asignación de derechos de acceso basados en el principio de mínimo privilegio, así como, procedimientos para la revisión y revocación de accesos cuando sea necesario.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

E. Se establecerá un mecanismo para la gestión de la salida de funcionarios, contratistas y terceros involucrados con la entidad, asegurando la revocación inmediata de accesos y la devolución de todos los activos de información y dispositivos tecnológicos propiedad de la organización.
F. Todos los funcionarios, contratistas y terceros involucrados con la entidad, serán responsables de adherirse a las políticas de seguridad de la información de la entidad y cumplir con las normativas legales y regulatorias pertinentes relacionadas con la protección de datos y la seguridad de la información.

5.3.29. Política de manejo integral con gestión documental.

Con el sentido y 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.

- Dado que la Gobernación del Valle del Cauca cuenta con Internet y servicios de correo electrónico institucional, la Secretaría de las TIC reglamentará su utilización de acuerdo a las políticas y asignará responsabilidades de acuerdo con la cantidad de cuentas habilitadas. En todo caso, las unidades de correspondencia tendrán el control de estos, 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.

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:

- La política de manejo de documentos electrónicos está integrada con el sistema de gestión Integral.
- La política de manejo de documentos electrónicos es transversal a todas las dependencias de la Gobernación.
- Cada documento electrónico generado tiene asociado un responsable.
- Cada documento electrónico generado por la Gobernación hará parte de su sistema de gestión documental.
- 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 vigente en la entidad.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

- Cada documento electrónico debe tener garantizada su trazabilidad a través de todo su ciclo de vida.
- Para garantizar la preservación a largo plazo de los documentos electrónicos, es fundamental asignarles una valoración que permita clasificarlos. Esta clasificación servirá de base para establecer los procedimientos adecuados para su disposición final.
- La Secretaría de las Tecnologías de la Información y las Comunicaciones debe establecer y comunicar a las dependencias de la Gobernación del Valle del Cauca, de manera clara y precisa, los lineamientos para la administración de documentos electrónicos, incluyendo su creación, uso, mantenimiento, retención, acceso y preservación.

5.3.30. Privacidad y protección de información de datos personales.

La Gobernación del Valle del Cauca, responsable del tratamiento de los datos personales definidos en la Ley 1581 de 2012, se compromete a respetar la privacidad de todos los terceros que proporcionen sus datos personales a través de los distintos puntos de recolección y captura de información.

5.3.31. Uso de Internet para la Gobernación del Valle del Cauca.

El internet, como herramienta laboral, debe ser usado de manera adecuada, sujeto a control, verificación y monitoreo, en todas las actividades diarias relacionadas con el trabajo, conforme a las políticas establecidas, considerando para todos los casos, las siguientes políticas:

A. La navegación por Internet, en las diferentes dependencias de la entidad, debe ajustarse a las restricciones establecidas para los grupos de usuarios administrados por la Secretaria TIC. Los funcionarios, contratistas y terceros involucrados con la entidad con acceso a navegación avanzada serán designados por la alta dirección y los jefes de área; sin embargo, ciertos usos no están permitidos en ningún caso:

- Acceso a sitios con contenido sexual explícito, discriminatorio, actividades delictivas en línea o cualquier uso no autorizado está prohibido.
- Difusión, recepción o compra de material explícito, discriminatorio, delictivo o cualquier contenido que exceda las normas establecidas.
- Divulgación de información confidencial sin aplicar controles de seguridad previos ni contar con la autorización de los titulares correspondientes.
- Uso de servicios en línea que posibiliten conexiones o intercambios no autorizados por la Secretaría de las TIC.
- Promover o mantener asuntos o negocios personales.
- La descarga, instalación y uso de software no vinculado a las funciones laborales que pueda afectar el rendimiento de la estación de trabajo o la red.
- Uso de herramientas de mensajería instantánea no autorizadas por la Secretaría de las TIC.
- Utilizar correos electrónicos personales o externos para intercambiar información institucional.

B. La Secretaría de las TIC debe monitorear el uso apropiado de los canales de internet y la navegación a sitios web visitados por los funcionarios, contratistas y terceros involucrados con la entidad. También inspeccionará el registro de las actividades

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

realizadas durante la navegación, generando criterios suficientes para determinar la continuidad del servicio o su bloqueo por acciones no permitidas.

C. El uso de Internet está permitido de forma ética y responsable, sin afectar la productividad ni comprometer la seguridad de la información.

5.3.32. Uso del Correo Electrónico para la Gobernación del Valle del Cauca.

La asignación de cuentas de correo electrónico de la Gobernación del Valle del Cauca se realiza para que los funcionarios, contratistas y terceros puedan cumplir con sus funciones laborales, previa autorización. Su uso debe ajustarse a las siguientes normas:

A. El correo electrónico debe ser utilizado únicamente para llevar a cabo las funciones asignadas dentro de la Gobernación del Valle del Cauca.

B. Los correos electrónicos y sus contenidos son propiedad de la Entidad. Los usuarios deben guardar únicamente los mensajes vinculados a sus funciones labores.

C. La Secretaria de las TIC fijará los límites para el tamaño de los buzones y los mensajes de correo electrónico.

D. Toda información confidencial generada por la Gobernación del Valle del Cauca debe ser compartida en formatos no editables (como PDF) y con medidas de seguridad (como contraseñas) para garantizar su protección. Esta información sólo puede ser enviada en su formato original si el receptor requiere realizar modificaciones, siendo el usuario quien asume la responsabilidad de su envío.

E. No se considera aceptado el uso del correo electrónico de la Entidad para los siguientes fines:

- Está prohibido enviar o reenviar correos o mensajes que contengan contenido racista, sexista, pornográfico, publicidad no autorizada, o que violen la dignidad humana, pongan en riesgo sistemas internos o ajenos, transgredan normas morales y éticas, o promuevan actividades ilegales.
- Enviar mensajes no autorizados con contenido religioso o político.
- El envío de archivos con extensiones potencialmente peligrosas, como .mp3, .wav, .exe, .com, .dll, .bat, .msi u otras similares, debe ser previamente aprobado por la Secretaría de las TIC.
- Para realizar envíos masivos de mensajes corporativos, es necesario solicitar a la Secretaría de las TIC su aprobación.

F. En caso de que el mensaje sea recibido por alguna persona o empresa no autorizada, solicitar borrarlo de forma inmediata.

G. Suspender las cuentas de correo electrónico de contratistas que nunca han iniciado sesión al mes de haber sido asignadas, y eliminar dichas cuentas a los dos meses de inactividad.

H. Suspender las cuentas de correo electrónico de funcionarios nombrados que nunca han iniciado sesión a los seis meses de haber sido asignadas, y eliminar dichas cuentas a los dos meses de suspensión.

I. Suspender las cuentas genéricas que no han sido utilizadas en los últimos cinco meses, previa validación con el administrador, y eliminar dichas cuentas dos meses después. Se debe contactar al usuario antes de la eliminación.

J. Suspender las cuentas de correo electrónico de funcionarios nombrados que no hayan iniciado sesión en los últimos seis meses, y eliminar dichas cuentas a los dos meses de inactividad, contactando previamente al usuario.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

K. Suspender las cuentas de correo electrónico de contratistas al finalizar su contrato, y eliminar dichas cuentas a los tres meses de suspensión.
L. Revisar mensualmente las cuentas de contratistas vencidas, y suspender las que no hayan iniciado sesión, eliminándolas tres meses después de su suspensión.

5.3.33. Política de Uso de Redes Inalámbricas para la Gobernación del Valle del Cauca.

Las redes inalámbricas en la Gobernación del Valle del Cauca facilitan la conectividad para ciudadanos, personal y contratistas. Esta política establece normas para su uso seguro y efectivo, definiendo claramente las responsabilidades de la Secretaría de TIC en la gestión de perfiles de usuario, horarios de acceso y condiciones de servicio. Se asegura que todas las redes inalámbricas cumplan con altos estándares de seguridad, similar a las redes cableadas, y prohíbe el uso de configuraciones y contraseñas predeterminadas para proteger la integridad de la red.

A. La Secretaría de las TIC será responsable de establecer los perfiles de usuario, horarios, accesos y demás condiciones para el servicio de Wi-Fi destinado a los ciudadanos.
B. La Secretaría de las TIC gestionará la asignación de servicios de redes inalámbricas corporativas, estableciendo perfiles, horarios y condiciones de acceso para el personal y contratistas en la Gobernación del Valle del Cauca.
C. Las redes inalámbricas corporativas deben cumplir con los mismos estándares de seguridad que las redes cableadas, incluyendo identificación, autenticación, control de contenido en internet y cifrado de datos.
D. En ningún caso se podrá dejar configuraciones y contraseñas por defecto en los equipos inalámbricos.

5.3.34. Política de Uso de Computación en la Nube para la Gobernación del Valle del Cauca.

La Política de Uso de Computación en la Nube de la Gobernación del Valle del Cauca establece directrices para garantizar que toda la información institucional se maneje de manera segura y conforme a las normativas vigentes. Esta política prohíbe el almacenamiento de datos en plataformas de nube no autorizadas y exige que la Secretaría de las TIC asegure la protección de la información a través de cláusulas contractuales estrictas. Estas cláusulas deben incluir métodos de transferencia segura, autenticación y cifrado robustos, y procesos para la devolución y eliminación segura de datos. Además, se requiere que los proveedores de servicios en la nube mantengan altos estándares de ciberseguridad.

A. Todos los funcionarios, contratistas y terceros involucrados con la entidad no tienen permitido almacenar información de la Gobernación del Valle del Cauca en servicios de alojamiento de archivos multiplataforma en la nube que no hayan sido autorizados por la Secretaría de las TIC.
B. Al contratar servicios en la nube, la Secretaría de las TIC debe garantizar cláusulas contractuales para proteger la información. Esto incluye asegurar métodos seguros para la transferencia de datos, autenticación y cifrado robustos, procesos para la devolución y eliminación segura de datos, y acuerdos sobre la confidencialidad, integridad y disponibilidad de la información. Además, debe verificar que el proveedor de servicios en la nube gestione adecuadamente la ciberseguridad en su plataforma.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

5.3.35. Política Protección contra Software Malicioso para la Gobernación del Valle del Cauca.

La Política de Protección contra Software Malicioso de la Gobernación del Valle del Cauca tiene como objetivo salvaguardar la integridad y seguridad de los sistemas informáticos y la información institucional frente a amenazas de software malicioso. Esta política establece directrices para la implementación de herramientas de seguridad, el manejo adecuado de dispositivos de almacenamiento, la educación de los usuarios sobre riesgos y la vigilancia continua de los sistemas, para asegurar que todos los mecanismos de protección estén activamente en funcionamiento, actualizados y supervisados para prevenir, detectar y mitigar posibles ataques y fallos relacionados con código malicioso.

A. Todos los sistemas informáticos, incluyendo la infraestructura de procesamiento y comunicaciones, deben estar resguardados con herramientas y software de seguridad que eviten la entrada de código malicioso, así como, con mecanismos para detectar, prevenir y recuperarse de posibles fallos originados por dicho código.
B. Los mecanismos de seguridad deben estar activos y no pueden ser deshabilitados o eliminados sin la autorización de la Secretaría de las TIC. Además, deben recibir actualizaciones de manera continua.
C. No está permitido crear, ejecutar, distribuir, replicar o intentar introducir código que tenga la intención de auto replicarse, causar daño o afectar el funcionamiento de equipos o redes institucionales.
D. Todos los dispositivos de almacenamiento que se conecten a los sistemas de la entidad deben ser sometidos a un escaneo para identificar cualquier código malicioso u otro elemento que pueda comprometer la seguridad de la información.
E. La entidad debe asegurar que sus usuarios estén al tanto de los riesgos de infecciones por código malicioso derivados de correos electrónicos, sitios web, intercambio de archivos u otras actividades diarias que podrían ser explotadas por amenazas.
F. Los sistemas, equipos e información institucionales deben ser revisados periódicamente para verificar que no haya presencia de código malicioso.
G. Los siguientes usos se consideran usos no autorizados del servicio de antivirus y constituyen un incidente de seguridad de la información:

- Modificar, desactivar o eliminar la configuración de los programas antivirus o de detección de malware en los sistemas en los que estén instalados.
- Instalar o emplear programas de antivirus no autorizados por la Entidad.
- No se deben intercambiar ni transmitir archivos que el software antivirus o de detección de malware haya identificado como infectados o potencialmente peligrosos.
- Evitar la apertura o descarga de archivos identificados como infectados o potencialmente dañinos por el software antivirus o de detección de malware.

5.3.36. Política de Administración de Backups, Recuperación y Restauración de la Información para la Gobernación del Valle del Cauca.

La Política de Administración de Backups, Recuperación y Restauración de la Información de la Gobernación del Valle del Cauca establece directrices esenciales para proteger y gestionar la información crítica. Esta política asegura que todos los datos respaldados sean guardados de manera segura, recuperados eficazmente en caso de pérdida y restaurados conforme a los requisitos legales y organizacionales. Su propósito es garantizar la

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

integridad, disponibilidad y seguridad de la información, alineándose con las normativas vigentes y mejorando la resiliencia operativa de la entidad.

A. La información sobre procesos, procedimientos y actividades de la entidad se respalda siguiendo los requisitos legales, la clasificación adecuada, los períodos de retención establecidos y los requerimientos de la Gobernación del Valle del Cauca.
B. Las copias de respaldo deben conservarse durante el tiempo establecido en las tablas de retención, garantizando la protección de su acceso según su nivel de clasificación y cumpliendo con la disposición final indicada en las tablas de retención documental de la Entidad.
C. Toda información que respalde procesos, procedimientos o actividades de la Gobernación del Valle del Cauca debe contar con una documentación formal que defina y apruebe las necesidades de respaldo, especificando la información a respaldar, la frecuencia de los respaldos, la clasificación de la información y el tiempo de conservación de las copias.
D. Cada sistema de información que apoya las operaciones de la Gobernación del Valle del Cauca debe contar con documentación formal que describa las estrategias, procedimientos, estándares y actividades esenciales para la adecuada ejecución de los respaldos de la información del sistema.
E. Cualquier respaldo de información en dispositivos o equipos que no estén integrados en la infraestructura tecnológica de la Gobernación del Valle del Cauca debe solicitarse formalmente a la mesa de servicios. Los responsables del respaldo trabajarán con el solicitante para definir la estrategia más adecuada, teniendo en cuenta los requisitos de negocio, la clasificación de la información, las necesidades de recuperación y los recursos tecnológicos disponibles.
F. Todos los sistemas de información que apoyan los procesos y actividades de la Gobernación del Valle del Cauca deben disponer de tecnologías adecuadas para asegurar la creación de copias de respaldo, considerando las necesidades de uso, niveles de acceso permitidos, y los plazos de retención que establezca el responsable de la información.
G. Los períodos de retención para la información respaldada deben establecerse considerando las normativas legales, las metas de los procesos, los riesgos identificados, y las sugerencias de los usuarios y responsables de la información.
H. Los procedimientos para realizar copias de respaldo deben definir los métodos para asegurar la trazabilidad de cada etapa del proceso, incluyendo la ejecución, resultados obtenidos, responsables, medios empleados, la información respaldada y las acciones realizadas durante la copia y su eventual restauración.
I. Las copias de respaldo se guardan en ubicaciones seguras, protegidas por controles físicos y tecnológicos, asegurando su conservación durante el tiempo requerido, acceso restringido sólo a personas autorizadas, y disponibilidad inmediata cuando sea necesario.
J. Cuando se necesite realizar respaldos fuera de la estrategia establecida, los responsables de los procesos deberán gestionar su ejecución a través de los procedimientos de solicitud de servicio definidos por la Gobernación del Valle del Cauca.
K. Las copias de respaldo deben someterse a pruebas de restauración mensuales para garantizar su efectividad. Los resultados de estas pruebas se utilizarán para ajustar los procedimientos de respaldo, identificar mejoras, y gestionar riesgos. Los responsables

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

de la información deben participar en estas pruebas para certificar que las estrategias de respaldo y restauración cumplen con los requerimientos de sus procesos.

L. Cuando los requisitos legales o de retención, así como, las condiciones de los medios de respaldo, lo exijan, se debe proceder con la destrucción o disposición final de los medios asegurando que la información contenida sea completamente inaccesible. La destrucción de los medios deberá ajustarse a los procedimientos aprobados por el modelo integrado de gestión para asegurar la protección del medio ambiente.
M. Los servicios en la nube tipo SaaS y PaaS deben contar con copias de seguridad que cumplan con las normativas legales vigentes. Los contratos deben permitir la auditoría de estos respaldos y el proceso de restauración para asegurar su conformidad con las disposiciones normativas.
N. Antes de realizar actividades de mantenimiento preventivo programado es necesario realizar backup completo de la información, esta tarea será realizada por el personal de la Secretaría de las TIC o el operador tecnológico.

5.3.37. Política de cumplimiento.

La Gobernación del Valle del Cauca debe cumplir rigurosamente con todas las leyes y regulaciones internas y externas relacionadas con la seguridad y privacidad de la información. Esto implica adherirse a normativas como la Ley de Delitos Informáticos (Ley 1273 de 2009), la Ley de Derechos de Autor (Ley 23 de 1982 y sus modificaciones), la Ley de Protección de Datos Personales (Ley 1581 de 2012) y su Decreto Reglamentario 1377 de 2013. Además, se deben observar los tiempos de retención de registros establecidos en la Ley General de Archivos (Ley 594 de 2000), garantizar el uso autorizado de los recursos de procesamiento, emplear algoritmos criptográficos robustos para proteger la información sensible, recopilar evidencias en caso de incidentes de seguridad y someterse a auditorías periódicas para evaluar el cumplimiento y la efectividad de las medidas implementadas. En cuanto al uso de controles criptográficos, la Gobernación se regirá por la legislación vigente, incluyendo las directrices y estándares técnicos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 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 involucrados con la entidad sin excepción. Todos los funcionarios, contratistas y terceros involucrados con la entidad son responsables de contribuir a la protección de la información de la entidad, en tanto que el Equipo de La Secretaría 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 y el Oficial de Seguridad de la Información, deben monitorear el cumplimiento de las políticas de seguridad definidas y gestionar las actualizaciones que sean necesarias.

Se deben definir claramente todas las responsabilidades en cuanto a seguridad de la información, en especial las relacionadas con el oficial de seguridad de la información.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

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 explícita y el conocimiento de las responsabilidades de la seguridad de la información. Este compromiso se verá reflejado a través de:

6.1.1. La Secretaría de las TIC de la GOBERNACIÓN DEL VALLE DEL CAUCA debe mantener dentro de sus colaboradores un funcionario o contratista con el Rol 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.

6.1.2. Se debe velar por el cumplimiento de las políticas de seguridad de la información, comprometerse para que los funcionarios, contratistas y terceros involucrados con la entidad, conozcan y apliquen las políticas de seguridad de la información.

6.1.3. Se deben asignar responsabilidades “a las áreas y personas” asociadas a temas de la seguridad de la información.

6.1.4. La alta dirección de la GOBERNACIÓN DEL VALLE DEL CAUCA debe apoyar, facilitar y mantener las relaciones con empresas, entidades u organismos que presten asesoría especializada en seguridad de la información.

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

- Oficial de Seguridad de la Información.
- funcionarios, contratistas y terceros.
- Responsable de la información.
- Administradores de sistemas.
- Enlaces TIC.

6.2. Oficial de seguridad de la información.

La Gobernación del Valle del Cauca debe contar con un Oficial de Seguridad de la Información, quien debe realizar las siguientes actividades:

6.2.1. Definir o actualizar la documentación asociada al SGSI.

6.2.2. Mantener actualizado el análisis y evaluación del riesgo sobre los activos de información de la Gobernación del Valle Del Cauca.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

6.2.3. 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.

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

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

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

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

6.2.8. Mantenerse actualizado en nuevas amenazas y vulnerabilidades existentes.

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

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

6.2.11. Apoyar la implementación de los lineamientos dispuestos por MinTIC en la entidad dando cumplimiento a las disposiciones reglamentarias vigentes.

El Oficial de Seguridad de la Información podrá convocar a 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.

El oficial de seguridad podrá obtener la asesoría de otros organismos o entidades, con el objeto de optimizar su gestión.

6.2.12. 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, secretarías y oficinas de la Gobernación del Valle del Cauca.

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

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

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 Secretaría 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 Secretaría de las TIC, único medio válido 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 contratistas, proveedores y grupos de interés, así como, en la gestión de proyectos, independientemente del tipo de proyecto.

6.4. Responsables de la información.

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

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

6.4.2. 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.

6.5. Administradores de los sistemas o plataformas de TI.

Los administradores de los diferentes sistemas o plataformas de TI, deben implementar de forma activa los lineamientos del SGSI adoptado por la entidad de la siguiente manera:

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

6.5.2. 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.

6.5.3. 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.

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

6.5.4. 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.

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

6.6. 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 la Información y las Comunicaciones
- Alta Consejería TIC
- CSIRT de la Policía Nacional
- ColCert
- Instituto Colombiano de Normas Técnicas ICONTEC
- Empresas especializadas del sector privado
- Academia
- Registraduría
- 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 participe en los temas que se tratan.

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 intervalos planificados (por lo menos una vez por año) o cuando se requiera, 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. Los resultados de las revisiones se deben documentar claramente y se deben llevar registros, de acuerdo a los lineamientos establecidos.
De la misma manera, las políticas de seguridad de la información y los demás documentos que de esta se deriven deben ser revisados y actualizados cuando se requiera, por parte del Oficial de seguridad de la Información y/o por el Comité de Seguridad de la Información

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.

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 vigente.

8. SOPORTE NORMATIVO Y DE REFERENCIA.

Ver normograma del proceso.

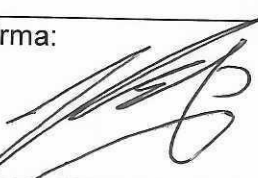
9. REGISTROS Y ANEXOS.

Todos los documentos relacionados con el SGSI.

10. CONTROL DE CAMBIOS.

CONTROL DE CAMBIOS		
Versión	**Descripción del cambio**	**Fecha**
1	Creación del documento acorde a los lineamientos y buenas prácticas de la norma ISO/IEC 27001:2013	12/12/2019
2	Actualización del documento donde se incluyen y complementan las políticas específicas de acuerdo con los establecido por el Ministerio de las TIC, a fin de garantizar el alineamiento con las normativas vigentes y fortalece la protección de datos, promoviendo una gestión integral y responsable de la información.	06/11/2024

11. CONTROL DE REVISIÓN Y APROBACIÓN.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Carlos Marino Santacruz, Waldor Drada Arango	**Nombre:** Héctor Fabio Bedoya Bedoya	Mesa de Trabajo con el Proceso M1-P3 Administración del MIPG. Acta No. 053 del 06 de noviembre del 2024. Comité Institucional de Gestión y Desempeño Acta No. 009 del 26 de noviembre del 2024.
Cargo: Profesional Universitario, Contratista	**Cargo**: Líder de Programa	
Firma: 	Firma: 	
Fecha: 06/11/2024	Fecha: 06/11/2024	Fecha: 06/11/2024

© ESTE DOCUMENTO ES PROPIEDAD DE LA GOBERNACIÓN DEL VALLE DEL CAUCA PROHIBIDA SU REPRODUCCIÓN POR CUALQUIER MEDIO, SIN AUTORIZACIÓN DEL GOBERNADOR(A) Y/O SU REPRESENTANTE.