# POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## Justificación

Establecer las Políticas de Seguridad de la Información basadas en el Anexo A de la norma ISO/IEC 27001:2013 para la Gobernación de Bolívar.

## Alcance

Estas políticas aplican a todos los funcionarios y contratistas que para el cumplimiento de sus funciones y obligaciones contractuales recolecta, utilizan y almacenan información para la ejecución de los procesos enmarcados en el mapa de procesos de la entidad.

En consonancia con la Resolución 247 de 2020 *"Por medio de la cual se adopta la actualización del Manual para la Administración del Riesgo de la Gobernación de Bolívar y se dictan otras disposiciones"* ***Alcance****: El Manual para la Administración del Riesgo en la Gobernación de Bolívar, será de aplicación obligatoria para la identificación, análisis, valoración, tratamiento, monitoreo, control y comunicación de los riesgos de gestión, corrupción y seguridad digital, de todos los procesos que conforman la entidad.*

## Cumplimiento

Todos los servidores públicos deberán dar cumplimiento con las presentes políticas. El incumplimiento a las políticas de seguridad y privacidad de la información traerás consigo, las consecuencias legales que apliquen a la normativa de la entidad, incluyendo lo establecido en las normas que competen al gobierno nacional y territorial en cuanto a seguridad y privacidad de la información se refiere.

**Declaración de Aplicabilidad - Statement of Applicability (SoA)**

La Gobernación de Bolívar utilizará todos los controles del Anexo A de la norma ISO/IEC 27001:2013.

Conforme lo indica la Resolución 247 de 2020 **"Por medio de la cual se adopta la actualización del Manual para la Administración del Riesgo de la Gobernación de Bolívar y se dictan otras disposiciones"**

***3.1. Controles a los riesgos:***

*El control se efectuará a todos los riesgos que queden consignados en los Mapas de Riesgos de la Gobernación de Bolívar, una vez se hayan realizado todas las etapas de identificación, análisis y valoración de riesgos. Se prestará especial atención a aquellos de alto impacto y probabilidad de ocurrencia, con el fin de mantener actualizado el estado de dichos riesgos y prevenir situaciones que pongan en peligro el logro de la misión, objetivos, planes y proyectos de la Entidad.*

***3.4. Acciones a desarrollar:***

*Los líderes de proceso serán responsables de aplicar la metodología para el desarrollo de la identificación, análisis y valoración de los riesgos de gestión por cada uno de los procesos, sobre todo, para aquellos procesos más vulnerables. De igual forma cada líder de proceso propondrá y ejecutará las acciones necesarias para mitigar sus riesgos y el equipo auditor de la oficina de Control Interno hará seguimiento al cumplimiento de las acciones formuladas.*

## 5, POLITICAS DE SEGURIDAD

### 5.1 , Orientación de la dirección para la gestión de la seguridad de la información

### 5.1.1 , Políticas para la seguridad de la información

- La Gobernación de Bolívar estableció la Política de Seguridad y Privacidad de La Información.
- Según el **Decreto 169 de 2018 "*Por la cual se adopta el Modelo Integrado de Planeación y Gestión -MIPG- en la Gobernación de Bolívar y se crean los Comités necesarios para su adecuado funcionamiento*"**

  ***ARTÍCULO 9o.- FUNCIONES DEL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO:*** *El Comité Institucional de Gestión y Desempeño, cumplirá las siguientes funciones:*

  ***6. Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.***

- Las políticas de seguridad de la información serán aprobadas por el Comité Institucional de Gestión y Desempeño.
- Las políticas de seguridad de la información están basadas en el Anexo A de la norma ISO/IEC 27001:2013.
- La Dirección TIC tendrá la responsabilidad de divulgar las Políticas Las Políticas de Seguridad de la Información y tendrá un Responsable de su implementación.
- Las políticas de seguridad de la información serán divulgadas para conocimiento de todos los interesados utilizando los canales disponibles.
- La Gobernación de Bolívar velará por que las Políticas descritas en este documento sean desarrolladas, aprobadas, implementadas, socializadas e interiorizadas por todos los interesados.

**5.1.2 , Revisión de las políticas para la seguridad de la información**

- Para guardar la concordancia con la Política de Seguridad de la Información, estas políticas se revisarán anualmente, o antes si existiesen cambios relevantes en el contexto interno y externo que afecten el logro de los objetivos institucionales y de seguridad de la información gestionada por la entidad, con el objeto de mantener las políticas oportuna, eficaz y suficiente.

## 6 , ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

### 6.1 , Organización interna

#### 6.1.1 , Roles y responsabilidades para la seguridad de información

- Según el **Decreto 169 de 2018 "*Por la cual se adopta el Modelo Integrado de Planeación y Gestión -MIPG- en la Gobernación de Bolívar y se crean los Comités necesarios para su adecuado funcionamiento***"

  *"**ARTÍCULO 11°. - EQUIPOS DE TRABAJO TEMÁTICOS:** Para la ejecución de las Dimensiones de Gestión y Desempeño Institucional previstas en el Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG y las políticas enlistadas en el Decreto 1499 de 2017, se conformarán los siguientes equipos temáticos, los cuales serán los responsables de presentar propuestas y estrategias de operación para la implementación y sostenibilidad de las políticas y los componentes y requisitos del modelo."*

| DIMENSIONES DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL / EQUIPOS DE TRABAJO TEMÁTICOS | POLÍTICAS | RESPONSABLES | COMPONENTES Y REQUISITOS |
|---|---|---|---|
| **GESTIÓN PARA EL RESULTADO CON VALORES** | Política de Gobierno Digital | Dirección de las Tecnologías de la Información y de las Comunicaciones | • Adopción y formulación de la estrategia de tecnologías de la información.<br>• **Implementación de mecanismos para alcanzar niveles óptimos de calidad, seguridad y confiabilidad de la información.**<br>• Promoción del uso y apropiación de las tecnologías de la información.<br>• Diagnóstico de capacidades institucionales.<br>• **Gestión de la Seguridad Informática.** |
| | Política de Seguridad Digital | Dirección de las Tecnologías de la Información y de las Comunicaciones | • **Gestión de la Seguridad de la Información.**<br>• Rendición de cuentas al coordinador nacional de seguridad nacional sobre la implementación de la política.<br>• Articulación de esfuerzos, recursos, metodologías y estrategias en la entidad. |

- Que el **Decreto 489 de 2018 "Por la cual se modifica parcialmente el Decreto 169 de 2018"**, "*Por medio del cual adopta Integrado de Planeación y Gestión -MIPG- en la Gobernación de Bolívar y se crean los comités necesarios para su adecuado funcionamiento" y se dictan otras disposiciones.*

***Artículo 2****".- MODIFIQUESE el artículo 5 de las funciones del Comité Institucional de Gestión y Desempeño, el cual en lo sucesivo quedará así:*

*"ARTÍCULO 5".- FUNCIONES DEL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO: El Comité institucional de Gestión y Desempeño, cumplirá las siguientes funciones:*

*Parágrafo 1: Serán en adelante funciones del comité Institucional de Gestión y Desempeño las Siguientes:*

- *En materia de Antitrámites y de Gobierno Digital:*

*II. En materia de Gobierno Digital:*

1. *Ser la instancia responsable del liderazgo, planeación e impulso de la Estrategia de Gobierno Digital en la entidad y canal de comunicación con la institución responsable de coordinar la Estrategia de Gobierno Digital, con la Comisión Interinstitucional de Políticas y de Gestión de la Información para la Administración Pública (COINFO) y de los demás grupos de trabajo relacionados con la transformación y modernización de la administración pública, apoyados en el aprovechamiento de la tecnología.*
2. *Definir los mecanismos para dar cumplimiento a la normatividad relacionada con el Gobierno Digital.*
3. *Liderar, bajo los lineamientos de la Estrategia de Gobierno Digital, la elaboración del diagnóstico y la elaboración y seguimiento al plan de acción de Gobierno Digital de la entidad.*

4. *Coordinar y articular la Estrategia de Gobierno Digital en el Departamento de Bolívar.*
5. *Incorporar el aprovechamiento de las TIC en las acciones de racionalización de trámites, atención efectiva al ciudadano y acompañar a los demás grupos conformados al interior de la entidad, tales como calidad y control interno.*
6. *identificar las barreras normativas para la provisión de trámites y servicios en línea y propender por levantar dichos obstáculos, de manera que puedan ser prestados por medios electrónicos.*
7. ***Definir los lineamientos para la implementación efectiva de políticas y estándares asociados, como la política de actualización del sitio Web (donde deberán estar involucradas las diversas áreas, direcciones y/o programas de la entidad), política de uso aceptable de los servicios de Red y de internet, política de servicio por medios electrónicos, política de privacidad y condiciones de uso y política de seguridad del sitio Web, entre otros.***
8. *Definir e implementar el esquema de vinculación de la entidad a la Intranet Gubernamental y cada uno de sus componentes.*
9. *Definir y generar incentivos y/o estímulos para el uso de los servicios de Gobierno Digital por parte de los ciudadanos, las empresas y la entidad misma.*
10. *Adelantar investigaciones, de tipo cualitativo y cuantitativo, que permitan identificar necesidades, expectativas, uso, calidad e impacto de los servicios y trámites de Gobierno Digital de la entidad.*
11. *Garantizar la participación de funcionarios de la entidad en procesos de generación de capacidades (sensibilización, capacitación y formación) que se desarrollen bajo el liderazgo de la institución responsable de coordinarla implementación de la Estratégica de Gobierno Digital.*

*PARAGRAFO 1.2.: Para efectos del desarrollo y cumplimiento de tales funciones, el Comité Institucional de Gestión y Desempeño se apoyará en los Equipos de Trabajo Temáticos correspondiente a las Políticas de Racionalización de Trámites, Política de Gobierno Digital y Seguridad Digital, establecidos en el Artículo 7 del presente decreto.*

*ARTÍCULO 3°.- MODIFIQUESE el artículo 7 de los Equipos de Trabajo Temáticos que conforman el Comité Institucional de Gestión y Desempeño, el cual en lo sucesivo quedará así:*

| DIMENSIONES DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL / EQUIPOS DE TRABAJO TEMÁTICOS | POLÍTICAS | RESPONSABLES | COMPONENTES Y REQUISITOS |
|---|---|---|---|
| **GESTIÓN PARA EL RESULTADO CON VALORES** | Política de Gobierno Digital | Dirección de las Tecnologías de la Información y de las Comunicaciones | • Adopción y formulación de la estrategia de tecnologías de la información.<br>• **Implementación de mecanismos para alcanzar niveles óptimos de calidad, seguridad y confiabilidad de la información.**<br>• Promoción del uso y apropiación de las tecnologías de la información.<br>• Diagnóstico de capacidades institucionales.<br>• **Gestión de la Seguridad Informática.** |
| | Política de Seguridad Digital | Dirección de las Tecnologías de la Información y de las Comunicaciones | • **Gestión de la Seguridad de la Información.**<br>• Rendición de cuentas al coordinador nacional de seguridad nacional sobre la implementación de la política.<br>• Articulación de esfuerzos, recursos, metodologías y estrategias en la entidad. |

- Que la Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y la Comunicación "**Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital**"

**ARTÍCULO 1. Objeto.** La presente resolución tiene por objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.

- Conpes 3072 Agenda de Conectividad del 2000
- Conpes 3701 Lineamientos de Política para Ciberseguridad y Ciberdefensa del 2011
- Conpes 3854 Política Nacional de Seguridad Digital del 2016
- Conpes 3975 Política Nacional para la Transformación Digital e Inteligencia Artificial del 2019
- Conpes 3995 Política Nacional de Confianza y Seguridad Nacional del 2020
- Que el **Decreto 531 de 2018** ***"Por la cual se adopta el Manual de Políticas y Procedimientos de Protección de Datos de la Gobernación de Bolivar y se dictan otras disposiciones"***

***ARTICULO 1. ADOPCION:*** *Adóptase el Manual de Políticas y Procedimientos de Protección de Datos Personales de la Gobernación de Bolívar contenida en documento anexo, que hace parte integral del presente acto administrativo, contentiva de los lineamientos que garantizan la aplicación del marco normativo sobre la protección de datos personales establecida en la Ley 1581 de 2012 y sus decretos reglamentarios; el cual impone a todas las personas el deber de conocer, actualizar y rectificar la información que se haya recogido sobre ellas en las bases de datos que maneja la Gobernación, garantizando que la información suministrada por éstas, cuente con los principios que la rigen, como son la confidencialidad, integridad y disponibilidad.*

***ARTICULO 2. SUJETOS OBLIGADOS:*** *Todas las personas naturales y jurídicas que tengan algún vínculo con la Gobernación de Bolívar y que en el ejercicio de sus actividades y/o funciones deban recolectar datos personales para ser ingresados a las bases de datos, están obligadas a cumplir con los lineamientos dados en el documento de Política de Tratamiento de Datos Personales.*

***ARTÍCULO 3. SEGURIDAD DE LA INFORMACIÓN:*** *Con el propósito de cumplir con el principio de seguridad de la información que conforma los registros individuales constitutivos de los bancos de datos, se atenderán los lineamientos de esta Política, cuyo responsable es la Dirección de Tecnologías de la Información y las Comunicaciones -TIC- de la entidad.*

***ARTÍCULO 4. CONTROL:*** *La Dirección de Tecnologías de la Información y las Comunicaciones - TIC- será la encargada de velar por el cumplimiento de las políticas de protección de datos personales adoptadas a través del presente decreto, y realizará conjuntamente con la Secretaría de Planeación, las actuaciones necesarias para implementar la Política Pública de Protección de Datos Personales de la Gobernación de Bolívar.*

- Que la **Resolución No. 247 de 2020** ***"Por medio de la cual se adopta la actualización del Manual para la Administración del Riesgo de la Gobernación de Bolívar y se dictan otras disposiciones"***

  ***ARTÍCULO PRIMERO. ACTUALIZACIÓN****. Adoptar las actualizaciones al Manual para la Administración del Riesgo de la Gobernación de Bolívar, acogido mediante la Resolución 388 del 05 de junio de 2017, contemplado en documento anexo que hace parte integral del presente acto administrativo, contentivo de la Política de*

*Administración del Riesgos y de los lineamientos que permitirán fortalecer la implementación y desarrollo de las prácticas de la Administración del Riesgo en la Gobernación de Bolívar, a través del adecuado tratamiento de los riesgos de gestión, de corrupción y de seguridad digital, controlando las situaciones que puedan impactar en el cumplimiento de su misión y sus objetivos institucionales.*

***3.4. Acciones a desarrollar:*** *Los líderes de proceso serán responsables de aplicar la metodología para el desarrollo de la identificación, análisis y valoración de los riesgos de gestión por cada uno de los procesos, sobre todo, para aquellos procesos más vulnerables. De igual forma cada líder de proceso propondrá y ejecutará las acciones necesarias para mitigar sus riesgos y el equipo auditor de la oficina de Control Interno hará seguimiento al cumplimiento de las acciones formuladas.*

***3.5. Líneas de defensa y la definición de controles:*** *Las líneas de defensa establecidas por el modelo integrado de planeación y gestión en la séptima dimensión, tienen gran responsabilidad en la gestión de riesgos de la gobernación de Bolívar como se muestra a continuación:*

***Primera Línea de defensa****: Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.*

**6.1.2 , Separación de deberes**

- Los procesos críticos tendrán separadas las responsabilidades en las actividades de Solicitar encabezada por la dependencia, análisis y autorización encabezada por los profesionales de la Dirección TIC y la ejecución por parte de los administradores de infraestructura, las cuales no deberán ser realizadas por la misma persona.

- Las actividades de administración de la plataforma deberán estar separada en sus deberes Autorización, Administración y Monitoreo.

**6.1.3 , Contacto con las autoridades**

- La Gobernación de Bolívar establecerá contacto con autoridades civiles, militares, académicas, científicas y de entes de control que permitan mejorar la efectividad de la gestión de la seguridad de la información.

**6.1.4 , Contacto con grupos de interés especial**

- La Dirección TIC's de la Gobernación de Bolívar establecerá contacto con asociaciones técnicas con las cuales puede intercambiar experiencia, cooperar y desarrollar relaciones de mutuo beneficio tecnológico y de seguridad.

**6.1.5 , Seguridad de la información en la gestión de proyectos**

- La Dirección TIC proyectará los lineamientos de seguridad de la información para la gestión e implementación de proyectos.
- Las dependencias deberán solicitar acompañamiento de la Dirección TIC en los proyectos que impacten acceso a la información.
- En los proyectos adelantados por las diferentes dependencias se deben adoptar los requerimientos del oficial de seguridad con respecto al manejo de los datos personales y los equipos temáticos de Política de Gobierno Digital y Política de Seguridad Digital.
- En los proyectos adelantados por las diferentes dependencias y que impacten el componente tecnológico o sistemas de información se deben adoptar los requerimientos de la Dirección TIC con respecto a la Seguridad Informática.
- Todos los proyectos de nuevas implementaciones de Infraestructura Tecnológica y desarrollo de sistemas de información deberán contemplar el soporte nativo al protocolo IPv6.

### 6.2 , Dispositivos móviles y teletrabajo

#### 6.2.1 , Política para dispositivos móviles

- La Dirección TIC establecerá las políticas de seguridad para dispositivos móviles que accedan a la infraestructura o sistemas de información.
- Las redes utilizadas para que los dispositivos móviles accedan a la infraestructura de la Gobernación de Bolívar deben estar separados de la red corporativa.
- Se utilizarán credenciales para el acceso a los recursos de red cuando se utilicen dispositivos móviles.
- El servidor que use dispositivos móviles entregado por la Gobernación de Bolívar para sus realizar sus funciones deberá acatar las políticas consignadas en este documento.
- Los dispositivos móviles hurtados o extraviados deberán ser reportados a la Dirección Administrativa Logística y seguir el procedimiento correspondiente.
- La información producida en el uso de dispositivos móviles deberá reposar en la infraestructura tecnológica de la Gobernación de Bolívar, por lo tanto, la Dirección TIC no será responsable de su recuperación en caso de pérdida.
- El uso de dispositivos móviles de la Gobernación de Bolívar será para realizar actividades laborales.

#### 6.2.2 , Teletrabajo

- La Dirección TIC establecerá las políticas de seguridad para acceso a la infraestructura o sistemas de información usada en modalidad de “Trabajo en casa”.
- La información producida en modalidad de “Trabajo en casa” deberá reposar en la infraestructura tecnológica de la Gobernación de Bolívar.

- El acceso a los recursos y la información alojada en infraestructura tecnológica de la Gobernación de Bolívar para personal que se encuentre laborando bajo la modalidad de “Trabajo en casa” debe ser autorizado por el responsable de la información, quien deberá notificarlo por oficio a la Dirección TIC para habilitarlo.
- Los recursos informáticos asignados para la modalidad de “Trabajo en casa” son para uso exclusivo de actividades laborales.

## 7 , SEGURIDAD DE LOS RECURSOS HUMANOS

### 7.1 , Antes de asumir el empleo

#### 7.1.1 , Selección

- El proceso de selección de personal se lleva a cabo a través de la Dirección de Función Pública y se realiza de conformidad con la Ley 909 de 2004.

#### 7.1.2 , Términos y condiciones del empleo

- Los Términos y Condiciones del empleo del personal se define por parte de la Dirección de Función Pública y se realiza de conformidad con la Ley 909 de 2004.
- Los servidores y contratistas deberán firmar un acuerdo de confidencialidad cuando sus actividades impliquen acceso a Información Confidencial o a Datos Personales.

### 7.2 , Durante la ejecución del empleo

#### 7.2.1 , Responsabilidades de la dirección

- Los permisos de acceso a la información y a la infraestructura tecnológica de la Gobernación de Bolívar estarán vinculados a su contrato, manual de funciones y funciones asignadas por su líder funcional quien solicitará acceso especifico a los servicios necesarios usando el canal indicado.

#### 7.2.2 , Toma de conciencia, educación y formación en la seguridad y privacidad de la información.

- La Dirección TIC impartirá en común acuerdo con la Dirección de Función Pública capacitaciones y entrenamientos en Seguridad y Privacidad de la Información.
- Todo empleado de la Gobernación de Bolívar de nuevo ingreso deberá recibir inducción las Políticas institucionales de seguridad y privacidad de la información.

- Los funcionarios deberán asistir a las capacitaciones de Seguridad Informática que para el efecto sean impartidas o coordinadas por la Dirección TIC.
- Anualmente se impartirán inducciones y reinducciones sobre Seguridad Informática y Tratamiento de Datos personales.

**7.2.3 , Proceso disciplinario**

- Cuando la Dirección TIC identifique el incumplimiento al presente Manual remitirá el correspondiente reporte a la Dirección de control Interno de la Gobernación de Bolívar, para los efectos de su competencia y atribuciones.

**7.3 , Terminación o cambio de empleo**

**7.3.1 , Terminación o cambio de responsabilidades de empleo**

- Los permisos de acceso a la infraestructura se deben establecer máximo a la fecha de terminación de la vinculación laboral.
- El responsable de la información, líder funcional o supervisor de contrato debe reportar todo ingreso, cambio de responsabilidad o terminación de contrato a la Dirección TIC para la actualización de permisos.
- El responsable de la información, líder funcional o supervisor debe solicitar la información necesaria de los funcionarios antes de terminar el contrato, evitando así incidentes de indisponibilidad de la información en poder del funcionario desvinculado.
- Las cuentas de usuario deberán permanecer inactivas en situaciones de vacancia temporal y vacaciones.
- Todos los permisos asociados al funcionario se eliminarán al finalizar la relación laboral.

## 8 , GESTIÓN DE ACTIVOS

### 8.1 , Responsabilidad sobre los activos

#### 8.1.1 , Inventario de activos

- La Dirección TIC programará y realizará el inventario de activos de información que tenga a cargo.
- El inventario de activos deberá contener información relevante para la identificación, ubicación, uso y propietario del activo.
- La actualización del inventario se debe realizar al menos una vez al año.
- En el inventario se tendrá especial atención al inventario de software y a la asignación de las licencias.
- El responsable de los activos deberá identificarlos y clasificarlos adecuadamente, especialmente los activos de información que contengan Datos Personales.

#### 8.1.2 , Propiedad de los activos

- En el inventario de activos cada activo de información deberá tener un usuario responsable que defina las actividades que se pueden realizar con el.
- El responsable del activo deberá solicitar la actualización de los permisos de los funcionarios cuando haya lugar.
- El responsable del activo deberá revisar los permisos asignados a los funcionarios al menos una vez al año.

#### 8.1.3 , Uso aceptable de los activos

- Todo funcionario de bienes y servicios informáticos se comprometen a conducirse bajo los principios de seguridad de la información y de uso adecuado de los recursos

informáticos de La Gobernación de Bolívar, así como el estricto apego a la Política institucional de seguridad y privacidad de la información.

- Los funcionarios son responsables de la información entregada o producida en la realización de sus actividades laborales.
- El acceso a internet suministrado a los usuarios de la Gobernación de Bolívar es exclusivamente para las actividades relacionadas con las necesidades del servicio.
- El servicio de acceso a internet debe ser utilizado con responsabilidad entendiendo que todos los servicios son limitados en su prestación.
- Los usuarios con servicio de navegación en internet al utilizar el servicio aceptan que:
    - Serán sujetos de monitoreo de las actividades que realizan en internet.
    - Saben que existe la prohibición al acceso de páginas no autorizadas.
    - Saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
    - Saben que existe la prohibición de descarga de software.
- Es responsabilidad de los usuarios almacenar su información únicamente en el directorio de trabajo que se le asigne, la información institucional deberá permanecer en los repositorios institucionales ya sean locales o en la nube.
- Se prohíbe el consumo de alimentos cerca a los equipos de computo.
- Se prohíbe colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del gabinete.
- El personal de la Dirección TIC estará encargado de llevar a cabo los servicios y reparaciones al equipo informático.
- Los funcionarios de la Gobernación de Bolívar que hagan uso de equipos de cómputo deben conocer y aplicar las medidas pertinentes para la prevención de código malicioso como pueden ser virus, malware o spyware. Las capacitaciones serán programadas en conjunto por la dirección pública y la Dirección TIC.

- Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas institucionales de seguridad y privacidad de la información adoptadas en el presente documento.
- El responsable de la información velará porque la información repose en los repositorios oficiales.
- El responsable de los activos velará por el buen uso de los mismos por parte de los funcionarios que los tienen a cargo.
- El correo electrónico será tratado como documentación formal.
- Los equipos de propiedad de la Gobernación de Bolívar deben estar integrados al Directorio Activo, ningún equipo externo deberá tener acceso al mismo.

**8.1.4 , Devolución de activos**

- Cuando los usuarios necesiten ausentarse por cualquier situación administrativa (Licencia, Permiso, Comisión, Suspensión, Vacaciones) deberán entregar los activos e información a cargo al líder funcional o al supervisor del contrato.
- Será responsabilidad del líder funcional o del supervisor del contrato el recibo de los activos a cargo del funcionario.
- Los activos de información pertenecen a la dependencia específica por lo que al ser cambiar de actividades los funcionarios deberán devolverlos al Responsable de los activos.

**8.2 , Clasificación de la Información**

**8.2.1 , Clasificación de la información**

- La Dirección de Atención al Ciudadano y Gestión Documental establecerá la Política de Gestión Documental.

- La Dirección de Atención al Ciudadano y Gestión Documental establecerá las directrices para las clasificaciones de los documentos basada en la legislación aplicable.
- Las dependencias serán responsables de clasificar la información según los lineamientos indicados por la Dirección de Atención al Ciudadano y Gestión Documental.
- Para las bases de datos o archivos donde reposen datos personales es necesario identificar y clasificar los tipos de información según lineamientos de la Superintendencia de Industria y Comercio.

**8.2.2 , Etiquetado de la información**

- La Dirección de Atención al Ciudadano y Gestión Documental establecerá las directrices para la creación de las Tablas de Valoración Documental y las Tablas de Retención Documental.
- Las dependencias serán responsables del etiquetado de la información según los lineamientos indicados por la Dirección de Atención al Ciudadano y Gestión Documental.
- Para las bases de datos o archivos donde reposen datos personales es responsabilidad de la dependencia Responsable de información etiquetar los tipos de información según lineamientos de la Superintendencia de Industria y Comercio.

**8.2.3 , Manejo de activos**

- La Dirección TIC debe definir Procedimientos e Instructivos para el manejo de cada tipo de activo.

- La Dirección de Atención al Ciudadano y Gestión Documental establecerá las directrices para la creación de Plan de Conservación Documental y Plan de Preservación Digital a largo plazo.
- Los funcionarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura de la Gobernación de Bolívar, de igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna de la Gobernación de Bolívar o hacia redes externas como la nube e internet.
- El acceso a todos los servicios y activos de información de Bolívar debe ser controlado, por lo anterior, la Dirección TIC verificará todos los accesos a los servicios y asignación de activos en la medida que sea pertinente.

**8.3 , Manejo de medios**

**8.3.1 , Gestión de medios removibles**

- El usuario tiene la obligación de proteger los CD-ROM, DVDs, memorias USB, tarjetas de memoria, discos externos, computadoras y dispositivos portátiles que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.
- La información persistente debe ser alojada en los repositorios oficiales de la Gobernación de Bolívar, los medios removibles no deben utilizarse para almacenarla.

**8.3.2 , Disposición de los medios**

- La disposición final de los medios removibles deberá realizarse de acuerdo a lo dispuesto en la Ley 1672 de 2013 “POR LA CUAL SE ESTABLECEN LOS LINEAMIENTOS PARA LA ADOPCIÓN DE UNA POLITICA PÚBLICA DE GESTIÓN INTEGRAL DE RESIDUOS

DE APARATOS ELÉCTRICOS Y ELECTRÓNICOS (RAEE), Y SE DICTAN OTRAS DISPOSICIONES"

- La Gobernación de Bolívar establecerá el Plan de Disposición de Residuos Tecnológicos en el cual deberá contemplar la disposición de los medios removibles.
- El responsable del activo deberá respaldar la información antes de la disposición final de los medios o los equipos.

**8.3.3 , Transferencia de medios físicos**

- En las comunicaciones hacia y desde la Gobernación de Bolívar se deberá privilegiar la utilización de transmisiones cifradas, en detrimento del uso de medios grabados.
- En las transferencias de información que se utilicen medios removibles se debe privilegiar el grabado utilizando mecanismos de cifrado.

## 9 , CONTROL DE ACCESO

### 9.1 , Requisitos de negocio para el control de acceso

#### 9.1.1 , Política de control de acceso

- El acceso físico a las instalaciones será controlado por la Dirección Administrativa Logística en la asignación, autorización y cancelación de los carnets.
- La dirección de TIC controlará el acceso físico o lógico a las instalaciones que conforman infraestructura tecnológica de la Gobernación de Bolívar y establecerá los mecanismos necesarios para realizarlo.
- El control de acceso lógico a la infraestructura o información de la Gobernación de Bolívar deberá ser realizado utilizando credenciales asignadas al usuario específico.
- Cada usuario deberá tener credenciales para el sistema específico al que necesite acceder.
- Las credenciales de acceso a los servicios y la infraestructura tecnológica de la Gobernación de Bolívar son personales e intransferibles.
- Las actividades realizadas usando las credenciales se entenderán realizadas por el titular de las mismas.
- La Dirección TIC establecerá los permisos mínimos necesarios para el desempeño de las funciones.
- Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la Dirección TIC, antes de poder usar la infraestructura tecnológica de la Gobernación de Bolívar.
- Cada usuario deberá tener credenciales para ser utilizadas como mecanismo de autenticación en los accesos a la red, aplicaciones y/o sistemas de información de la Gobernación de Bolívar.

- Todos los usuarios de servicios de información son responsables por su identificador de usuario y contraseña que recibe para el uso y acceso de los recursos.
- Cada usuario que accede a la infraestructura tecnológica de la Gobernación de Bolívar debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de usuario por varios funcionarios.
- Los usuarios no deben proporcionar información a personal externo sobre los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la Gobernación de Bolívar.

**9.1.2 , Acceso a las redes y servicios en red**

- El acceso lógico o físico a la información e infraestructura de la Gobernación de Bolívar será autorizada por el responsable de la información o infraestructura según aplique, en la solicitud se deben indicar los permisos específicos.
- La dirección TIC solo establecerá permisos a las cuentas que hayan sido solicitados por el responsable de la información o de la infraestructura.
- Está prohibido que los usuarios utilicen la infraestructura tecnológica de la Gobernación de Bolívar para acceder a información u otros sistemas de información institucionales o externos para los cuales no está autorizado.
- Los permisos de acceso remoto desde internet deben ser solicitados por el responsable de la información o la infraestructura y aprobados por la Dirección TIC.
- Los accesos a la información e infraestructura serán realizados usando cuentas nombradas, no se utilizarán cuentas genéricas o usuarios anónimos.

**9.2 , Gestión de acceso de usuarios**

**9.2.1 , Registro y cancelación del registro de usuarios**

- La Dirección TIC es responsable de Crear, Actualizar, Desactivar y Eliminar cuentas de acceso a los recursos informáticos.
- La identificación y autorización a recursos informáticos debe ser solicitada formalmente por el responsable de la información a la Dirección TIC, conforme a los procedimientos definidos para la creación de usuarios de los sistemas de información.

**9.2.2 , Suministro de acceso de usuarios**

- El suministro de acceso a los usuarios será realizado formalmente por la Dirección TIC.
- Las credenciales deberán ser entregadas por los encargados de la Dirección TIC y los desarrolladores según sea el caso, previa solicitud del responsable de la información.
- Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica de la Gobernación de Bolívar, deberán ser solicitado formalmente a la Dirección TIC por parte del responsable de la información.
- El acceso al dominio de la Gobernación de Bolívar solo será permitido para los equipos corporativos de propiedad de la

**9.2.3 , Gestión de derechos de acceso privilegiado**

- La gestión de derechos de acceso privilegiado será realizada por la Dirección TIC.
- Los derechos de acceso privilegiado a la infraestructura solo serán autorizados formalmente por el Director TIC, avalados por el Profesional de Seguridad y ejecutados por los administradores de la infraestructura.
- El acceso privilegiado solo se permite a los Administradores de infraestructura.
- Los derechos de acceso privilegiado podrán ser monitoreados por la dirección TIC.

**9.2.4 , Gestión de información de autenticación secreta de usuarios**

- La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas debe ser realizada de forma individual y confidencial.
- La contraseña podrá ser cambiada por requerimiento del propietario de la cuenta.

**9.2.5 , Revisión de los derechos de acceso de los usuarios**

- Los registros de auditoría de los diferentes sistemas de información e infraestructura deberán estar activados.
- La Dirección TIC revisará la asignación, modificación, revisión o revocación de derechos y/o privilegios conforme los registros de auditoría y los formatos de solicitudes usados para la gestión.
- Anualmente se validará la utilización de las cuentas, circunstancialmente se realizarán depuraciones cuando sea necesario reasignar cuentas no utilizadas durante un periodo superior a 2 meses.
- El responsable de la información revisará la asignación, modificación, revisión o revocación de derechos y/o privilegios.

**9.2.6 , Retiro o ajuste de los derechos de acceso**

- El responsable de la información y sistemas de información a los cuales un funcionario en situación administrativa tiene permisos de acceso, deberá reportarlo a la Dirección TIC para ajustar los permisos.
- Al finalizar el contrato, el responsable de la información o el supervisor del respectivo contrato deberá solicitar el retiro de los permisos asignados a los usuarios.
- Las cuentas de usuario serán inhabilitadas inmediatamente alcancen el periodo de vigencia.

### 9.3 , Responsabilidades de los usuarios

#### 9.3.1 , Uso de la información de autenticación secreta

- La obtención o cambio de una contraseña debe hacerse de forma segura; el usuario deberá acreditarse ante la Dirección TIC como empleado de la Gobernación de Bolívar.
- Las contraseñas de las cuentas son datos confidenciales, por lo tanto, solo debe ser conocida por el titular de la misma y no debe ser compartida ni utilizada por otra persona.
- Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo a la Dirección TIC.

### 9.4 , Control de acceso a sistemas y aplicaciones

#### 9.4.1 , Restricción del acceso a la información

- La dirección TIC es responsable del control del acceso a la información, sistemas y aplicaciones.
- La Dirección TIC deberá establecer controles de acceso a la infraestructura, para lo cual realizará un análisis de riesgos.
- El responsable de la información deberá autorizar y solicitar implementación de controles de acceso a la información, para lo cual realizará un análisis de riesgos.

#### 9.4.2 , Procedimiento de ingreso seguro

- Todo acceso a sistema de información e información corporativa deberá ser autorizado por el responsable de la información quien deberá solicitarlo por escrito.
- La dirección TIC a través de los administradores de infraestructura permitirá el acceso a la información y los sistemas de información previa autorización del responsable de la información.

**9.4.3 , Sistema de gestión de contraseñas**

- Todo acceso a la información será permitido credenciales de acceso registrados en repositorios centralizados como el directorio activo, no se autorizará acceso a sistemas de información usando accesos anónimos.
- La dirección TIC indicará los parámetros de necesario para creación de contraseñas mediante un instructivo técnico.
- Las contraseñas de acceso a los diferentes sistemas de información e infraestructura deberán ser cambiadas cada 3 meses.
- Los desarrolladores de aplicaciones deberán implementar los controles establecidos para las cuentas de acceso.
- Las credenciales de acceso a los sistemas de información serán almacenadas de manera cifrada.
- Se debe evitar el cambio manual de las credenciales, siempre es necesario que el usuario digite directamente la contraseña que quiere utilizar.

**9.4.4 , Uso de programas utilitarios privilegiados**

- La dirección TIC o quien esta delegue será la única autorizada para realizar instalación de software.
- Los funcionarios no deberán tener acceso directo a la información, siempre debe mediar una interfaz de aplicación.
- El software especializado en administración de infraestructura de red, compiladores, soluciones de hacking ético, herramientas de desarrollo solo será utilizado por administradores de plataforma.

**9.4.5 , Control de acceso al código fuente de los programas**

- El código fuente de todo software desarrollado en la Gobernación de Bolívar debe reposar en custodia de la dependencia o custodiado por la Dirección TIC.
- El código fuente de los aplicativos desarrollados solo debe ser conocido por los desarrolladores y el custodio designado por el responsable de la información.
- El código fuente de las aplicaciones solo será modificado por los desarrolladores autorizados.
- El código fuente en custodia de la Dirección TIC deberá ser guardado y respaldado en repositorios oficiales.
- El código fuente de las aplicaciones será marcado como documento confidencial.

## 10 , CRIPTOGRAFÍA

### 10.1 , Controles criptográficos

#### 10.1.1 , Política sobre el uso de controles criptográficos

- La Dirección TIC autorizará la utilización de controles criptográficos utilizados en la Gobernación de Bolívar.
- Los administradores de plataformas deberán usar comunicación cifrada en sus labores de administración.
- Todo recurso publicado en internet deberá estar protegido por certificados digitales.
- Las bases de datos donde reposen las credenciales deben estar cifradas.
- La transferencia de información desde y hacia la Gobernación de Bolívar debe ser cifrada, se privilegiará su uso frente a la transferencia en texto plano.

#### 10.1.2 , Gestión de llaves

- Las llaves o certificados digitales de los diferentes servicios deben reposar en custodia de la Dirección TIC o de quien esta haya delegado la función.

## 11 , SEGURIDAD FÍSICA Y DEL ENTORNO

### 11.1 , Áreas Seguras

#### 11.1.1 , Perímetro de seguridad física

- La Dirección TIC definirá los controles a la Seguridad Física y del Entorno para los activos a cargo.
- Las oficinas de la oficina de Dirección TIC, los Centros de Cómputo, los cuartos de cableado, entre otras áreas que alberguen elementos de procesamiento y comunicación de la Gobernación de Bolívar son áreas restringidas, por lo tanto, sólo el personal autorizado por la dirección TIC puede acceder a ellos.
- El acceso a los centros de cómputo y los cuartos de cableado por parte de personal autorizado y visitantes será registrado y conservado su registro.

#### 11.1.2 , Controles físicos de entrada

- La Dirección TIC controlará el acceso a los centros de cómputo y los cuartos de cableado.
- Solo se permitirá el acceso a los centros de cómputo y los cuartos de cableado de la Gobernación de Bolívar a personas autorizadas usando los mecanismos asignados por la Dirección TIC y la Dirección Administrativa Logística, para la salvaguarda de equipos de cómputo y comunicaciones en general.

#### 11.1.3 , Seguridad de oficinas, recintos e instalaciones

- La Dirección Administrativa Logística establecerá e implementará los controles de acceso a oficinas, recintos e instalaciones.
- Los usuarios deberán seguir el principio de Escritorio Limpio, la cual consiste en mantener el escritorio libre de contraseñas escritas, documentos impresos o cualquier otro soporte que pueda entregar información confidencial a personas no autorizadas.
-

- Se prohíbe el consumo de alimentos en los Centros de Cómputo, los cuartos de cableado, entre otras áreas que alberguen elementos de procesamiento y comunicación de la Gobernación de Bolívar.

**11.1.4 , Protección contra las amenazas externas y ambientales**

- La Dirección Administrativa Logística establecerá los controles de protección ante desastres naturales, terrorismo, vandalismo, accidente u otros a las oficinas, recintos e instalaciones de la Gobernación de Bolívar.
- La Dirección Administrativa Logística controlará el acceso físico de servidores, contratistas y personal externo a las oficinas, recintos e instalaciones de la Gobernación de Bolívar.

**11.1.5 , Trabajo en áreas seguras**

- La Dirección TIC debe autorizar el acceso del personal externo o interno que deba realizar trabajo, implementación, actualización, soporte o cualquier otra actividad de la misma naturaleza dentro de los centros de cómputo y los cuartos de cableado de la Gobernación de Bolívar.
- Todo trabajo, implementación, actualización, soporte o cualquier otra actividad de la misma naturaleza que se deba realizar a la infraestructura tecnológica de la Gobernación de Bolívar deberá ser autorizado mediante un Comité de Control de Cambios por la Dirección TIC.
- Para realizar cualquier trabajo en las los centros de cómputo y los cuartos de cableado de la Gobernación de Bolívar debe ser realizado siguiendo un cronograma de actividades.

**11.1.6 , Áreas de despacho y carga**

- El Director TIC autorizará el recibo o la entrega de los equipos.

- Las operaciones de recibo, entrega y alistamiento de equipos se realizarán en la oficina técnica de la Dirección TIC.

**11.2 , Equipos**

11.2.1 , Ubicación y protección de los equipos

- La Dirección TIC establecerá el lugar de ubicación de los Servidores y Equipos de Red y sus responsables.
- Los líderes funcionales de las dependencias establecerán el sitio de ubicación de los equipos para realización de las actividades misionales y sus responsables.
- Los Servidores y Equipos de red serán ubicados en los Centros de Cómputo y los cuartos de cableado.
- Cuando se requiera realizar cambios múltiples de equipos de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con anticipación a la Dirección TIC y la Dirección Administrativa Logística a través de un plan detallado de movimientos debidamente autorizados por el titular del área que corresponda.
- Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos, debiendo solicitar apoyo a la Dirección TIC en caso de necesitar realizar estas actividades.
- El área de soporte técnico de la Dirección TIC, será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por la Dirección de Logística.
- El equipo de cómputo asignado deberá ser para uso exclusivo de las funciones asignadas en la Gobernación de Bolívar.

- El usuario deberá dar aviso de inmediato a la Dirección Administrativa Logística de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

**11.2.2 , Servicios de suministro**

- La Gobernación de Bolívar asignará los recursos para la protección de la infraestructura tecnológica contra fallas de servicios públicos.
- La Dirección TIC establecerá los controles para lo protección de la infraestructura tecnológica contra fallas de servicios públicos.
- Los Servidores y Equipos de red deberán conectarse a Sistemas de Alimentación Ininterrumpida.
- Siempre que sea posible se debe adquirir infraestructura en Alta Disponibilidad.
- En la adquisición se deben priorizar las compras de equipos que ofrezcan redundancia en fuentes de alimentación, discos, conectores, memorias.

**11.2.3 , Seguridad del cableado**

- La Dirección TIC autorizará y controlará las actividades relacionadas con el cableado estructurado.
- Toda instalación, actualización y gestión sobre el cableado eléctrico será realizada por la Dirección Administrativa Logística.
- Los suministros para las actividades relacionadas con el cableado estructurado y de potencia serán suministrados por la Dirección Administrativa Logística.
- La Dirección TIC establecerá los controles necesarios para mitigar riesgos en las transferencias de información contra intercepción, interferencia o daño.

**11.2.4 , Mantenimiento de los equipos**

- La Dirección TIC programará y ejecutará un plan anual de mantenimiento de equipos, este plan deberá incluir mantenimiento preventivo y correctivo de hardware y software.
-

- La Dirección TIC o quien esta delegué realizará el mantenimiento de equipos, por lo tanto, queda prohibido que el usuario intervenga, abra o desarme los equipos de cómputo lo que conlleva pérdida de garantías que proporciona el proveedor de dicho equipo.
- Cualquier mantenimiento o intervención de los equipo e infraestructura deberá ser registrado en el aplicativo configurado para este fin.

**11.2.5 , Retiro de activos**

- La Dirección Administrativa Logística establecerá e implementará las políticas para el ingreso y retiro de equipos de cómputo de las instalaciones de la Gobernación de Bolívar.
- El retiro de equipos de las instalaciones de la Gobernación de Bolívar será autorizado por la Dirección Administrativa Logística.
- La Dirección Administrativa Logística establecerá e implementará los controles para el traslado de equipos de computo dentro de las instalaciones de la Gobernación de Bolívar.

**11.2.6 , Seguridad de equipos y activos fuera de las instalaciones**

- El usuario que tenga bajo su responsabilidad algún equipo de cómputo o dispositivo móvil será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.
- La responsabilidad ante la entrega de PC’s o portátiles tiene el carácter de personal y será intransferible. Por tal motivo, queda prohibido su préstamo.
- Los equipos portátiles y dispositivos móviles deben tener los mismos controles de seguridad definidos para los equipos dentro de las instalaciones de la Gobernación de Bolívar.

**11.2.7 , Disposición segura o reutilización de equipos**

- La Dirección Administrativa Logística establecerá e implementará las políticas para la reutilización y disposición final de equipos de cómputo.
- La Dirección TIC establecerá las políticas de disposición segura de repuestos y equipos según el Plan de tratamiento de residuos tecnológicos.
- La Dirección Administrativa Logística realizará el proceso de trámite de las garantías de los equipos y la baja de los que en este proceso sean reemplazados.
- La Dirección TIC establecerá el procedimiento para la eliminación total de información alojada en los equipos dados de baja o reutilizados.

**11.2.8 , Equipos de usuario desatendidos**

- Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (previamente instalados y autorizados por la Dirección, como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo.
- Los usuarios deberán bloquear la sesión cuando su equipo se encuentre desatendido.

**11.2.9 , Política de escritorio limpio y pantalla limpia**

- La Dirección TIC establecerá un papel tapiz y protector de pantalla de los equipos del dominio.
- Los funcionarios y contratistas deberán mantener libres de información disponible a cualquier persona que no esté autorizada para acceder a los equipos a su cargo.
- El escritorio deberá permanecer libre de documentos que permitan obtener información confidencial del usuario ya sea corporativa o personal.
- Al realizar configuraciones a los servidores o equipos el administrador deberá eliminar el registro de las actividades o bloquear su sesión.

## 12 , SEGURIDAD DE LAS OPERACIONES

### 12.1 , Procedimientos operacionales y responsabilidades

#### 12.1.1 , Procedimientos de operación documentados

- La Dirección TIC documentará y socializará las políticas, procedimientos, instructivos, formatos necesarios para asegurar las operaciones sobre la infraestructura tecnológica de la Gobernación de Bolívar.
- Los usuarios de la infraestructura tecnológica de la Gobernación de Bolívar deberán atender y aplicar las políticas, procedimientos, instructivos, formatos para el correcto desarrollo de las operaciones.

#### 12.1.2 , Gestión de cambios

- La Dirección TIC y las dependencias impactadas deberán autorizar cualquier modificación a la infraestructura tecnológica o de los sistemas de información por medio de un comité de cambio.
- Los cambios realizados a la infraestructura tecnológica o de los sistemas de información deberán ser registrados y los documentos asociados deberán ser actualizados.
- Solo será realizados los cambios autorizados en la infraestructura tecnológica o de los sistemas de información en un comité de cambios.
- Los responsables de las modificaciones a la infraestructura tecnológica o de los sistemas de información deberán respetar lo acordado en el comité de cambios.

#### 12.1.3 , Gestión de capacidad

- La Dirección TIC junto con las Dependencias correspondientes realizarán estudios y proyecciones de las capacidades de la infraestructura tecnológica instalada para la

realización de sus actividades misionales o de apoyo, con base en esos estudios se realizarán las inversiones correspondientes para asegurar la disponibilidad de los servicios.

**12.1.4 , Separación de los ambientes de desarrollo, pruebas y operación**

- Los ambientes de desarrollo, pruebas y operación deberán separarse evitando así riesgos de integridad de la información entre estos, disponibilidad de los sistemas y confidencialidad de la información.

**12.2 , Protección contra código malicioso**

**12.2.1 , Controles contra el código malicioso.**

- La Dirección TIC implementará y gestionará controles antimalware para proteger la infraestructura tecnológica de la Gobernación de Bolívar.
- Para prevenir infecciones por virus informáticos, los usuarios de la Gobernación de Bolívar deben evitar hacer uso de cualquier clase de software que no haya sido proporcionado y validado por la Dirección TIC.
- Los usuarios de la Gobernación de Bolívar deben verificar que la información y los medios de almacenamiento, considerando al menos memorias USB, discos flexibles, CD´s, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por la Dirección TIC.
- El usuario debe verificar mediante el software de antivirus autorizado por la Dirección TIC, que estén libres de virus todos los archivos de computadora, bases de datos, documentos u hojas de cálculo, etc. que sean proporcionados por personal externo o interno.
- Ningún usuario de la Gobernación de Bolívar debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para autorreplicarse, dañar o en otros casos impedir el funcionamiento de

cualquier memoria de computadora, archivos de sistema o software, así como no debe probarlos en cualquiera de los ambientes o plataformas de la Gobernación de Bolívar.

- Los usuarios internos o servidores de la Gobernación de Bolívar, o personal externo No podrán descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, la instalación de cualquier software corresponde a la Dirección TIC.
- Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá seguir el procedimiento de reporte de incidente de seguridad.
- Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil será responsable de solicitar de manera periódica a la Dirección las actualizaciones del software de antivirus.
- Los usuarios no deberán alterar o eliminar las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por la Dirección TIC.

**12.3 , Copias de seguridad**

**12.3.1 , Copias de seguridad de la información**

- La Dirección TIC será responsable de realizar copias de seguridad de las configuraciones, archivos y demás elementos necesarios para la operación de los sistemas de información e infraestructura tecnológica de la Gobernación de Bolívar.
- El respaldo de la información de las dependencias que repose en equipos o en servidores de archivo deberá ser solicitado por el Responsable de la Información.
- Los usuarios deberán solicitar respaldo de la información cuando considere que la información es relevante para su actividad laboral.
- Los usuarios deberán solicitar respaldo de la información que considere relevante cuando el equipo sea enviado a reparación, previendo así la pérdida involuntaria de

información, derivada de proceso de reparación; solicitando la asesoría del personal de la Dirección TIC.

**12.4 , Registro y seguimiento**

**12.4.1 , Registro de eventos**

- Las actividades que realicen los usuarios de la Gobernación de Bolívar, en la infraestructura de Tecnología de la Información podrán ser registradas y susceptibles de auditoría.
- Las implementaciones necesarias en razón de obtener registro de actividades deben ser solicitadas y financiadas por la dependencia correspondiente.
- La dirección TIC realizará asesoría técnica para la adquisición de las soluciones de registro de actividades.
- Las solicitudes de recuperación de registros de eventos deben ser realizadas por el líder funcional de la dependencia indicando fecha, hora, sistema o cualquier dato que permita refinar la consulta, además, debe indicar la razón de dicha solicitud para efectos de auditoría.

**12.4.2 , Protección de la información de registro**

- La dirección TIC propenderá por la conservación de los registros de eventos de los elementos que tiene a cargo, asegurando la disponibilidad de los mismos, la confidencialidad y la integridad de los mismos.

**12.4.3 , Registros del administrador y del operador**

- Las actividades que realicen los administradores de infraestructura de la Gobernación de Bolívar, en la infraestructura de Tecnología de la Información podrán ser registradas y susceptibles de auditoría.

**12.4.4 , Sincronización de relojes**

- El reloj de los diferentes dispositivos será sincronizado con el Servidor de Tiempo de Red configurado para los mismos en el Directorio Activo.

**12.5 , Control de software operacional**

**12.5.1 , Instalación de software en sistemas operativos**

- La Dirección TIC será responsable de la instalación de los sistemas operativos y las aplicaciones de los equipos y la infraestructura tecnológica de la Gobernación de Bolívar.
- Todo software que se instale en los equipos de la Gobernación de Bolívar deberá estar licenciado a nombre de la misma.
- En las instalaciones que impliquen posibilidad de indisponibilidad de la plataforma tecnológica, se deberá realizar el respectivo comité de cambios.

**12.6 , Gestión de la vulnerabilidad técnica**

**12.6.1 , Gestión de las vulnerabilidades técnicas**

- La Dirección TIC realizará semestralmente análisis de vulnerabilidades de la infraestructura a su cargo y realizará las correspondientes remediaciones a las que haya lugar.
- Las vulnerabilidades críticas deberán ser remediadas en su totalidad.
- En los nuevos desarrollos deberán realizar análisis de vulnerabilidades y se deberán realizar las remediaciones correspondientes por parte del implementador o contratista.
- Será considerado como un ataque a la seguridad informática, cualquier actividad no autorizada por la Dirección TIC, en la cual los usuarios realicen la exploración de los

recursos informáticos en la red de la Gobernación de Bolívar, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y mostrar una posible vulnerabilidad.

**12.6.2 , Restricciones sobre la instalación de software**

- La Dirección TIC será responsable de la instalación de las aplicaciones en los equipos y la infraestructura tecnológica de la Gobernación de Bolívar.
- Los usuarios finales no deberán instalar software en sus computadoras, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de la Gobernación de Bolívar, que no esté autorizado por la Dirección TIC.
- Si un usuario necesita utilizar un software no licenciado a nombre de la Gobernación de Bolívar deberá solicitar la compra de dicho software.

**12.7 , Consideraciones sobre auditorias de sistemas de información**

**12.7.1 , Controles de auditorías de sistemas de información**

- La Dirección Tic será responsable de la planeación y ejecución de auditorías a los sistemas de información e infraestructura tecnológica de la Gobernación de Bolívar.
- Toda auditoría de sistemas que suponga un riesgo para la disponibilidad de los activos de información deberá ser autorizado por la Dirección TIC mediante un acta de control de cambios.

## 13 , SEGURIDAD EN LAS TELECOMUNICACIONES

### 13.1 , Gestión de la seguridad en las redes

#### 13.1.1 , Controles de red

- La Dirección TIC será responsable de la planeación e implementación de los controles de seguridad para los sistemas de información e infraestructura tecnológica de la Gobernación de Bolívar.
- Los controles de seguridad estarán basados en los correspondientes análisis de riesgos de los activos de información de las diferentes dependencias.

#### 13.1.2 , Seguridad de los servicios de red.

- Todo software de gestión de red utilizado en la Gobernación de Bolívar deberá ser licenciado.
- En todos los contratos de servicios de seguridad se deben establecer los correspondientes Acuerdos de Niveles de Servicio.
- Los usuarios de Despachos y Secretarias de la Gobernación de Bolívar no deben establecer otras redes, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la Gobernación de Bolívar sin la autorización de la Dirección TIC.
- El acceso a los servicios de red deberá realizarse posteriormente a el establecimiento de todos los controles de seguridad implementados por la Gobernación de Bolívar para su infraestructura tecnológica y de sistemas de información.
- Todo software de control remoto deberá ser autorizado por la Dirección TIC.
- La Dirección TIC establecerá reserva de las direcciones IP para los servicios que lo necesiten.

**13.1.3 , Segregación de redes**

- La Dirección TIC establecerá los requerimientos para controlar el acceso entre las redes de datos.
- Se establecerán diferentes redes para diferentes propósitos, dependiendo del medio y de los elementos a conectar.
- Las redes de datos estarán separadas dependiendo de las necesidades y de acuerdo a los servicios necesarios.
- No se permite el acceso a las redes de producción a equipos o dispositivos que no pertenezcan a la Gobernación de Bolívar, estos elementos estarán separados en redes específicas.

**13.2 , Transferencia de información**

**13.2.1 , Políticas y procedimientos de intercambio de información**

- La Dirección TIC establecerá las políticas y procedimientos sobre intercambio de información.
- Para mitigar los riesgos asociados al intercambio de información las dependencias deberán utilizar los canales establecidos por la Dirección TIC para tal fin.
- El responsable de la información de cada dependencia establecerá que información podrá ser compartida dentro y fuera de la Gobernación de Bolívar.

**13.2.2 , Acuerdos sobre transferencia de información**

- La información corporativa no podrá ser alojada en servicios de almacenamiento con los que no exista contrato de servicio, ni en cuentas personales.
- Para las transferencias y transmisiones de datos personales se deberá seguir la legislación correspondiente.

- Cuando sea necesario transferir Información Publica Clasificada o Información Publica Reservada con personas naturales o jurídicas externas deberá firmarse un Acuerdo de Confidencialidad.

**13.2.3 , Mensajería electrónica**

- La Dirección TIC establecerá los requerimientos de los controles de seguridad para la mensajería electrónica.
- Cuando sea necesario el envío por mensajería electrónica de Información Publica Clasificada o Información Publica Reservada la comunicación y/o la información deberá ser protegida utilizando canales y soluciones de cifrado.
- Las cuentas de correo son personales e intransferibles, los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, si es necesario leer el correo de alguien más (mientras esta persona se encuentra fuera o ausente), el usuario ausente debe redireccionar el correo a otra cuenta de correo interno.
- Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información que es propiedad de la Gobernación de Bolívar. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
- Los usuarios podrán enviar información reservada y/o confidencial exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones, a través del correo institucional que le proporcionó la dependencia a través de la Dirección TIC.
- La asignación de una cuenta de dominio, correo electrónico, SIGOB o cualquier credencial a los aplicativos institucionales, será solicitada por escrito por el líder funcional del usuario que requiere el acceso al servicio a la Dirección TIC, señalando los motivos por los que se desea el servicio.
- Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

**13.2.4 , Acuerdos de confidencialidad o de no divulgación**

- Los responsables de la información identificarán la Información en las actividades para las cuales sea necesario firmar un acuerdo de confidencialidad.
- Todos los servidores y contratistas de la Gobernación de Bolívar deberán firmar un Acuerdo de Confidencialidad con el compromiso de no divulgar la información confidencial interna y externa que conozca de la Gobernación de Bolívar, así como la relacionada con las funciones que desempeña. La firma del acuerdo implica que la información conocida por todo servidor, contratista y/o tercero, bajo ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente sin autorización previa.
- Todo servidor o contratista que deba acceder a bases de datos con Datos Personales deberá firmar Acuerdo de Confidencialidad con la dependencia correspondiente para el acceso al recurso solicitado.

## 14 , ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

### 14.1 , Requisitos de seguridad de los sistemas de información

#### 14.1.1 , Análisis y especificación de requisitos de seguridad de la información

- La Dirección TIC establecerá las especificaciones de seguridad para los sistemas de información e infraestructura tecnológica de la Gobernación de Bolívar.
- Las personas encargadas de los diferentes proyectos de desarrollo e implementación de sistemas de información deberán colaborar en el análisis de riesgos que supone su implementación dentro de la infraestructura tecnológica de la Gobernación de Bolívar.

#### 14.1.2 , Seguridad de servicios de las aplicaciones en redes públicas

- La Dirección TIC establecerá los requerimientos de los controles de seguridad para los servicios de aplicaciones en redes públicas de la Gobernación de Bolívar.
- Todo sistema de información publicado en internet deberá ser protegido por el correspondiente certificado digital.
- Todo sistema de información publicado en internet deberá establecer uso de credenciales de usuario.
- Todas las transacciones realizadas en sistemas de información publicados en internet deberán guardar registro de actividades de usuario (Trazabilidad).
- Toda transacción realizada en sistemas de información publicados en internet deberá tener criterio de Información Publica Clasificada e Información Publica Reservada según corresponda, el responsable de la información indicará cual caso corresponde.

#### 14.1.3 , Protección de transacciones de los servicios de las aplicaciones

- La Dirección TIC establecerá los requerimientos de los controles de seguridad para la

protección de transacciones de la Gobernación de Bolívar.

- El responsable de la información de la dependencia entregará los recursos financieros para establecer controles que mitiguen riesgos a la integridad y confidencialidad de las transacciones, a su vez, mitiguen riesgos a la disponibilidad del servicio.

**14.2 , Seguridad en los procesos de desarrollo y soporte**

**14.2.1 , Política de desarrollo seguro**

- La Dirección TIC establecerá las especificaciones de seguridad para el desarrollo y mantenimiento de los sistemas de información de la Gobernación de Bolívar.
- Los desarrolladores deberán seguir los lineamientos de desarrollo seguro establecidos por la Dirección TIC.
- Todo proyecto que impacte la infraestructura tecnológica de la gobernación de bolívar debe ser acompañado por la Dirección TIC, la dependencia encargada debe solicitar el acompañamiento.

**14.2.2 , Procedimientos de control de cambios en sistemas**

- Todo cambio que pueda impactar la disponibilidad, integridad o confidencialidad de la infraestructura de la Gobernación de Bolívar deberá ser autorizado por la Dirección TIC mediante un acta de control de cambios.
- Todo cambio programado que pueda impactar la disponibilidad de la infraestructura de la Gobernación de Bolívar deberá ser informado y se procurará ser realizado en horario no laboral.

**14.2.3 , Revisión técnica de las aplicaciones después de cambios en la plataforma de operación**

- La Dirección TIC establecerá las especificaciones de seguridad para la revisión técnica de los sistemas de información de la Gobernación de Bolívar.

- El responsable de la información especificará a los implementadores la obligatoriedad de la realización de pruebas y mitigación de vulnerabilidades, así como, el restablecimiento de la operación cuando aplique.

**14.2.4 , Restricciones en los cambios a los paquetes de software**

- La Dirección TIC establecerá los requerimientos en los cambios de paquetes de software.
- Los códigos fuente del software deberán permanecer en custodia del responsable de la información o de la Dirección TIC si así lo requiere el responsable.
- Los códigos fuente del software deberán permanecer inalterados hasta que medie contrato y solicitud formal del responsable de la información.
- Los cambios en el software deben ser solicitados formalmente por el responsable de la información a la persona natural o jurídica desarrolladora.
- Los cambios en el software deben ser aprobados en un comité de control de cambios.
- Todo cambio en sistemas de información o infraestructura tecnológica deberá ser documentado y versionado.

**14.2.5 , Principios de construcción de sistemas seguros**

- La Dirección TIC establecerá las especificaciones de seguridad para la construcción de sistemas de información de la Gobernación de Bolívar.
- Los proyectos de desarrollo y mantenimiento de sistemas de información e infraestructura tecnológica deberán seguir las especificaciones de seguridad en lo referente a creación de contraseñas, requerimientos de desarrollo e implementación de sistemas desarrolladas por la Dirección TIC.
- Todo proyecto de desarrollo de software deberá contemplar la entrega de Manual de Usuario, Manual de Sistema, Diagramas, Manual de Configuración, con su correspondiente versionamiento.

**14.2.6 , Ambiente de desarrollo seguro**

- La Dirección TIC establecerá las especificaciones de seguridad para los ambientes de desarrollo de la Gobernación de Bolívar.
- Los ambientes de desarrollo deberán estar separados de los ambientes de pruebas y producción, así como del acceso de usuarios finales.

**14.2.7 , Desarrollo contratado externamente**

- La Dirección TIC establecerá las especificaciones de seguridad para el desarrollo de sistemas de información contratados a terceros de la Gobernación de Bolívar.
- Los sistemas de información contratados a terceros deberán cumplir los mismos requisitos de seguridad y entrega que los sistemas de información desarrollados por los equipos internos.

**14.2.8 , Pruebas de seguridad de sistemas**

- La Dirección TIC establecerá las especificaciones de seguridad para el desarrollo de pruebas de seguridad a sistemas de información de la Gobernación de Bolívar.
- Los desarrolladores realizarán las pruebas a la seguridad de los sistemas y mitigarán las vulnerabilidades encontradas en las pruebas de seguridad de los sistemas de información.

**14.2.9 , Pruebas de aceptación de sistemas**

- El responsable de la información establecerá los criterios de aceptación y pruebas necesarias para la entrega de los nuevos sistemas de información, así como de las actualizaciones de los sistemas en producción.

**14.3 , Datos de prueba**

**14.3.1 , Protección de datos de prueba**

- Los sistemas de información en los ambientes de desarrollo y pruebas deberán probarse con datos diferentes a los de producción.

## 15 , RELACIÓN CON PROVEEDORES

### 15.1 , Seguridad de la información en las relaciones con los proveedores

#### 15.1.1 , Política de seguridad de la información para las relaciones con proveedores

- El Responsable de la Información establecerá los permisos de acceso de los proveedores a la activos e información bajo su custodia.
- La Dirección TIC configurará los permisos correspondientes a los activos e información a los Proveedores y Contratistas indicados por el responsable de la información.
- Los proveedores y contratistas que deban tener acceso a Información Pública Clasificada o Información Pública Reservada de la Gobernación de Bolívar deberán firmar un Acuerdo de Confidencialidad.
- Los proveedores y contratistas deberán acoger las políticas de seguridad de la Gobernación de Bolívar.
- El Responsable de la Información indicará los permisos de acceso a la Información necesarios para los proveedores.
- El supervisor o interventor del contrato deberá solicitar de manera explícita los permisos de acceso a los sistemas de información, información o infraestructura tecnológica de la Gobernación de Bolívar para los proveedores y contratistas, así como remoción de los permisos al finalizar los respectivos contratos.

#### 15.1.2 , Tratamiento de la seguridad dentro de los acuerdos con proveedores

- El Responsable de la Información deberá realizar el correspondiente análisis de riesgo a los activos de información y establecer controles para los proveedores que deban tener acceso, procesar, almacenar, comunicar o suministrar componentes.

- La Dirección TIC implementará los controles solicitados con los recursos asignados por el Responsable de la información para las implementaciones entregadas por los proveedores.

**15.1.3 , Cadena de suministro de tecnología de información y comunicación**

- La Dirección Administrativa Logística establecerá las condiciones para el proceso de contratación para la adquisición de sistemas de información e infraestructura tecnológica según lo establecido en la legislación de contratación.

**15.2 , Gestión de la prestación de servicios con los proveedores**

**15.2.1 , Seguimiento y revisión de los servicios de los proveedores**

- La Gobernación de Bolívar realizará Supervisión e Interventoría de los contratos de suministro de Sistemas de Información e Infraestructura Tecnológica según legislación correspondiente.
- Los contratos de suministro de Sistemas de Información e Infraestructura Tecnológica deberán establecer Acuerdos de Niveles de Servicio.

**15.2.2 , Gestión de cambios en los servicios de proveedores**

- Todo cambio, mantenimiento, mejora de políticas y procedimiento de suministro de servicios en controles de seguridad de la información que pueda impactar la Disponibilidad, Integridad o Confidencialidad de la información deberá ser programado y autorizado mediante comité de cambios.
- Todo cambio programado por proveedores que pueda impactar la disponibilidad de la infraestructura de la Gobernación de Bolívar deberá ser informado y se procurará realización en horario no laboral.

## 16 , GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

### 16.1 , Gestión de incidentes y mejoras en la seguridad de la información

#### 16.1.1 , Responsabilidad y procedimientos

- La Gobernación de Bolívar establecerá las responsabilidades de la Gestión de Incidentes de Seguridad Informática mediante Comité Institucional de Gestión y Desempeño.
- El único responsable de gestionar incidentes de seguridad de la información en la Gobernación de Bolívar es el Equipo de respuesta a incidentes de la Gobernación de Bolívar.
- El Equipo de respuesta a incidentes de la Gobernación de Bolívar y sus responsabilidades estarán definidos en la Política de Gestión de Incidentes y en el Procedimiento de Gestión de Incidentes.
- Para los incidentes de Seguridad de la información asociados a Datos Personales se realizará el procedimiento correspondiente según lo indique el Programa Integral de Gestión de Datos personales y el Procedimiento de Gestión de Incidentes de Datos Personales.
- La política de gestión de incidentes está definida en el mismo documento, según lo recomienda el Anexo 16 de la Norma ISO 27001:2013

#### 16.1.2 , Reporte de eventos de seguridad de la información

- Los canales de reporte de eventos e incidentes de seguridad de la información, así como los actores estarán definidos en el Procedimiento de Gestión de Incidentes.
- Todo servidor o contratista que tenga conocimiento de la ocurrencia de un evento o incidente de seguridad informática en la plataforma tecnológica de la Gobernación de Bolívar, deberá reportarlo de inmediato por los medios dispuestos para ello.

- Cuando exista la sospecha o el conocimiento de que información Publica Clasificada o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático deberá notificarlo.
- Todo reporte de presunto evento o incidente se debe registrar por el Equipo de respuesta a incidentes de la Gobernación de Bolívar.

**16.1.3 , Reporte de debilidades de seguridad de la información**

- Todo servidor o contratista de la Gobernación de Bolívar que sospeche o detecte vulnerabilidades en la infraestructura, sistemas de información o procesos deberá reportarlo al Equipo de respuesta a incidentes de la Gobernación de Bolívar.

**16.1.4 , Evaluación de eventos de seguridad de la información y decisiones sobre ellos**

- Las actividades de Priorización de eventos e incidentes de seguridad informática por parte del Equipo de respuesta a incidentes de la Gobernación de Bolívar estarán definidas en el Procedimiento de Gestión de Incidentes de la Gobernación de Bolívar.
- El Equipo de respuesta a incidentes de la Gobernación de Bolívar deberá atender todos los incidentes de seguridad informática que se presenten, priorizando los incidentes de nivel alto y crítico, configurando las alertas ante precursores e indicadores.

**16.1.5 , Respuesta a incidentes de seguridad de la información**

- Las actividades de Respuesta a eventos e incidentes de seguridad informática por parte del Equipo de respuesta a incidentes de la Gobernación de Bolívar estará definido en el Procedimiento de Gestión de Incidentes de la Gobernación de Bolívar.
- Las comunicaciones oficiales a nombre del Equipo de respuesta a incidentes de la Gobernación de Bolívar de la entidad serán dadas o autorizadas por el Director TIC, actividad que estará definida en el Procedimiento de Gestión de Incidentes de la Gobernación de Bolívar.

**16.1.6 , Aprendizaje obtenido de los incidentes de seguridad de la información**

- Las actividades de aprendizaje y realimentación del proceso por parte del Equipo de respuesta a incidentes de la Gobernación de Bolívar estarán definidas en el Procedimiento de Gestión de Incidentes de la Gobernación de Bolívar.
- Los indicadores del proceso de Gestión de Incidentes por parte del Equipo de respuesta a incidentes de la Gobernación de Bolívar estarán definidas en el Procedimiento de Gestión de Incidentes de la Gobernación de Bolívar.

**16.1.7 , Recolección de evidencia**

- Las actividades de Identificación, Recolección, Adquisición y Preservación de Evidencias del proceso de Gestión de Incidentes por parte del Equipo de respuesta a incidentes de la Gobernación de Bolívar estarán definidas en el Procedimiento de Gestión de Incidentes de la Gobernación de Bolívar.

## 17 , ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

### 17.1 , Continuidad de seguridad de la información

#### 17.1.1 , Planificación de la continuidad de la seguridad de la información

- El Responsable de la Información de la dependencia deberá realizar análisis y establecer los requisitos de Planes, Procedimientos e Instructivos para el Manejo de Contingencias, Continuidad del Negocio y Recuperación de Desastres de la Información a su cargo y de la Infraestructura Tecnológica y Sistemas de Información que utilicen.
- La Dirección TIC realizará análisis y documentará Planes, Procedimientos e Instructivos para el Manejo de Contingencias, Continuidad del Negocio y Recuperación de Desastres de la Infraestructura Tecnológica y Sistemas de Información a su cargo.

#### 17.1.2 , Implementación de la continuidad de la seguridad de la información

- El Responsable de la Información de la dependencia Establecerá, Documentará, Implementará y Mantendrá planes, procedimientos e instructivos que permitan el Manejo de Contingencias, Continuidad del Negocio y Recuperación de Desastres de la Información a su cargo y de la Infraestructura Tecnológica y Sistemas de Información que utilicen, también, deberá asignar los recursos para la implementación de dichos planes.
- La Dirección TIC establecerá Planes, Procedimientos e Instructivos para el Manejo de Contingencias, Continuidad del Negocio y Recuperación de Desastres de la Infraestructura Tecnológica y Sistemas de Información a su cargo.

**17.1.3 , Verificación, revisión y evaluación de la continuidad de la seguridad de la información**

- El Responsable de la Información de la dependencia asignará recursos para realizar pruebas a intervalos regulares de los planes, procedimientos e instructivos que permitan el Manejo de Contingencias, Continuidad del Negocio y Recuperación de Desastres de la Información a su cargo y de la Infraestructura Tecnológica y Sistemas de Información que utilicen, estas evaluaciones estarán definidas en el mismo documento.
- La Dirección TIC realizará pruebas a intervalos regulares de los Planes, Procedimientos e Instructivos para el Manejo de Contingencias, Continuidad del Negocio y Recuperación de Desastres de la Infraestructura Tecnológica y Sistemas de Información a su cargo.

**17.2 , Redundancias**

**17.2.1 , Disponibilidad de instalaciones de procesamiento de información.**

- El Responsable de la adquisición de solución de Sistemas de Información o Infraestructura Tecnológica asignará los recursos para, siempre que sea posible dentro de los procesos de contratación se adquieran dispositivos redundantes, sistemas de alimentación ininterrumpida, sistemas redundantes de energía, líneas redundantes de internet, etc en aras de mitigar riesgos de Disponibilidad de la Información.

**18 , CUMPLIMIENTO**

**18.1 , Cumplimiento de requisitos legales y contractuales**

**18.1.1 , Identificación de la legislación aplicable y de los requisitos contractuales**

- La Dirección Administrativa Logística identificará y observará la normatividad dentro de los procesos de contratación para la adquisición de sistemas de información e infraestructura tecnológica según lo establecido en la legislación de contratación.
- El responsable de la adquisición del Sistema de Información, Infraestructura Tecnológica o información establecerá las reglas de utilización de la solución de tal manera que no se vulneren derechos ni se infrinja legislación vigente.
- De conformidad con el ***Decreto 1080 de 2015 ARTÍCULO 2.8.2.5.3. Responsabilidad de la gestión de documentos****. La gestión de documentos está asociada a la actividad administrativa del Estado, al cumplimiento de las funciones y al desarrollo de los procesos de todas las entidades del Estado; por lo tanto, es responsabilidad de los servidores y empleados públicos así como los contratistas que presten servicios a las entidades públicas; aplicar las normas que en esta materia establezca el Archivo General de la Nación Jorge Palacios Preciado, y las respectivas entidades públicas.*

**18.1.2 , Derechos de propiedad intelectual**

- La Gobernación de Bolívar adoptará medidas necesarias para la protección de derechos de autor y propiedad intelectual.
- Todo servidor o contratista de la Gobernación de Bolívar para la realización de actividades laborales utilizará únicamente software adquirido legalmente según el tipo de licenciamiento aplicable.
- Todo servidor, contratista o proveedor de la Gobernación de Bolívar que en el ejercicio de sus actividades laborales diseñe y desarrolle software, configure sistemas de

información o infraestructura tecnológica deberá ceder los derechos patrimoniales a la entidad.

- La cesión de derechos patrimoniales a nombre de la Gobernación de Bolívar deberá estipularse en las especificaciones esenciales de los contratos.
- Todo uso de propiedad intelectual o material protegido por derechos de autor deberá contar con permiso escrito del autor del mismo.
- La Dirección TIC será responsable de revisar el licenciamiento del software que deba instalar.
- En las especificaciones esenciales para los contratos de Sistema de Información e Infraestructura Tecnológica se deben estipular que el proveedor solo activará productos licenciados.
- En las especificaciones esenciales para los contratos de Sistema de Información e Infraestructura Tecnológica se debe estipular que el proveedor entregará todo el licenciamiento requerido para el funcionamiento de la solución.
- En las especificaciones esenciales para los contratos de Sistema de Información e Infraestructura Tecnológica se debe estipular que el proveedor entregará códigos fuentes.
- El software instalado en los equipos de cómputo de la Gobernación de Bolívar que no cuenten con su respectiva licencia debe ser desinstalado de inmediato.

**18.1.3 , Protección de registros**

- El responsable de la información asignará los recursos para la custodia de los registros de información que deban protegerse ante riesgos de Disponibilidad, Integridad y Confidencialidad según legislación vigente.
- La Dirección TIC establecerá los controles de seguridad para proteger los registros de acuerdo a los recursos asignados para tal fin.

**18.1.4 , Privacidad y protección de datos personales**

- Para todos los efectos la Gobernación de Bolívar será el Responsable del Tratamiento de Datos Personales que se hallen en sus bases de datos, el Responsable de la Información de la Dependencia tendrá la responsabilidad de aplicar la legislación correspondiente a datos personales a cada uno de sus activos.
- La Gobernación de Bolívar una Política de Protección de Datos Personales basado en la Ley 1581 de 2012 "*Por la cual se dictan disposiciones generales para la protección de datos personales*", sus decretos reglamentarios, la Guía de responsabilidad demostrada y documentos complementarios.
- La Gobernación de Bolívar implementó un Programa Integral de Gestión de Datos Personales basado en la Guía de responsabilidad demostrada y documentos complementarios.

**18.1.5 , Reglamentación de controles criptográficos**

- La Gobernación de Bolívar cumplirá todas las disposiciones de la Ley 527 de 1999 "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones" y de las leyes y decretos que la complementen o deroguen.

**18.2 , Revisiones de seguridad de la información**

**18.2.1 , Revisión independiente de la seguridad de la información**

- La Dirección TIC y el Comité Institucional de Gestión y Desempeño revisarán y actualizarán la política de seguridad de la información, las políticas de seguridad de la información, los procedimientos e instructivos y demás documentos asociados a la

- Seguridad de la Información y Datos Personales con una periodicidad anual o antes si existiesen cambios relevantes en el contexto interno y externo que afecten el logro de los objetivos institucionales y de seguridad de la información gestionada por la entidad, con el objeto de mantener las políticas oportuna, eficaz y suficiente.

**18.2.2 , Cumplimiento con las políticas y normas de seguridad**

- El Responsable de la Información de la Dependencia tendrá la responsabilidad de revisar regularmente la aplicación de estas políticas de seguridad de la información dentro de su proceso.

**18.2.3 , Revisión del cumplimiento técnico**

- El Responsable de la Información de la Dependencia tendrá la responsabilidad de asignar los recursos para la revisión periódica del cumplimiento técnico la aplicación de estas políticas de seguridad de la información dentro de su proceso.

- **Acceso a la Información Pública**: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)
- **Activo**: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
- **Activos de Información y recursos**: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 de 20116).
- **Amenazas**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
- **Bases de Datos Personales**: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)
- **Ciberseguridad**: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- **Ciberespacio**: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Datos Personales**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).
- **Datos Personales Públicos**: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)
- **Datos Personales Privados**: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)
- **Datos Personales Mixtos**: Para efectos de este documento es la información que contiene datos personales públicos junto con datos privados o sensibles.
- **Datos Personales Sensibles**: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

- **Derecho a la Intimidad**: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).
- **Gestión de incidentes de seguridad de la información**: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).
- **Información Pública Clasificada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Información Pública Reservada**: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)
- **Ley de Transparencia y Acceso a la Información Pública**: Se refiere a la Ley Estatutaria 1712 de 2014.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).
- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Responsable del Tratamiento de Datos**: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art. 3).
- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información**: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).
- **Seguridad digital**: Preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.
- **Titulares de la información**: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)
- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).
- **Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).