

Disposiciones de Tecnologías de Información

Secretaría Técnica del Sistema Banca para el Desarrollo - SBD

Aprobado por la Dirección Ejecutiva de la Secretaría Técnica del SBD en oficio CR/SBD-0176-2021 del 17 de setiembre del 2021



Descriptores de documento

Condiciones			
1. Finalidad			
Este documento tiene el propósito de normar el correcto uso de los activos tecnológicos de la Secretaría Técnica del SBD y FONADE y facilitar el mejor aprovechamiento de todos los recursos tecnológicos, que son propiedad o se encuentran a disposición de estos.			
2. Acceso y uso			
El documento está previsto para uso de:			
<input checked="" type="checkbox"/> Miembros del Consejo Rector			
<input checked="" type="checkbox"/> Personal de la Secretaría Técnica			
<input type="checkbox"/> Otro: _____			
Se prohíbe su distribución a terceras partes sin consentimiento previo del Director Ejecutivo de la Secretaría Técnica del SBD.			
3. Mantenimiento			
Inconsistencias, errores o mejoras detectadas, se solicita sean comunicadas a la Dirección de Estrategia Digital, indicando en el asunto: Disposiciones de Tecnologías de Información.			
Gestión documental			
Tipo documental: Políticas Institucionales	Versión: 1	Usuario/Destinatario: Interno	Propietario: DED
Vigencia: A partir del 17 de setiembre del 2021	Fecha control: Junio 2022	Archivo: <input checked="" type="checkbox"/> Gestión <input checked="" type="checkbox"/> Permanente	Código PI-STSD-DED2-V01
Observación:	Este documento se complementa con: <ul style="list-style-type: none"> • NA 		
Fecha de aprobación:	17 de setiembre 2021		

TABLA DE CONTENIDO

1	GLOSARIO, ABREVIATURAS Y ACRÓNIMOS	3
2	DISPOSICIONES.....	3
2.1	DISPOSICIONES GENERALES.....	3
2.1.1	<i>Sobre el Rol de los Usuarios y Jefaturas.....</i>	3
2.1.2	<i>Divulgación y cumplimiento.....</i>	4
2.2	DISPOSICIONES ADMINISTRATIVAS.....	4
2.2.1	<i>Servicios ofrecidos por DED</i>	4
2.2.2	<i>Acceso físico al área de servidores y comunicaciones</i>	4
2.2.3	<i>Documentación y mantenimiento de manuales de DED</i>	4
2.2.4	<i>Adquisición de nuevas tecnologías</i>	5
2.2.5	<i>Inventario de equipo.....</i>	6
2.2.6	<i>Reparación de equipos.....</i>	6
2.3	DISPOSICIONES RELATIVAS A SISTEMAS DE INFORMACIÓN Y APLICACIONES	6
2.3.1	<i>Contratación de sistemas de información y aplicaciones.....</i>	6
2.4	DISPOSICIONES RELATIVAS A BASES DE DATOS.	8
2.4.1	<i>Creación de bases de datos</i>	8
2.4.2	<i>Instalación, migración o mantenimiento de bases de datos.....</i>	8
2.4.3	<i>Seguridad y respaldos de las bases de datos.....</i>	8
2.5	DISPOSICIONES RELATIVAS A REDES Y TELECOMUNICACIONES.....	9
2.5.1	<i>Uso de las redes de datos</i>	9
2.6	DISPOSICIONES RELATIVAS AL SERVICIO DE INTERNET, CORREO ELECTRÓNICO Y ANTIVIRUS	10
2.6.1	<i>Uso de Internet, correo electrónico y antivirus.....</i>	10
2.7	DISPOSICIONES RELATIVAS AL HARDWARE.	12
2.7.1	<i>Responsabilidad de uso y resguardo</i>	12
2.7.2	<i>Mantenimiento del hardware instalado.....</i>	13
2.7.3	<i>Disposiciones para el desecho de equipos electrónicos.....</i>	13
2.8	DISPOSICIONES RELATIVAS AL SOFTWARE.	13
2.8.1	<i>Disposiciones sobre el uso de licencias o servicios de software</i>	13
2.8.2	<i>Disposiciones para la instalación de Software</i>	14
2.9	DISPOSICIONES RELATIVAS A LA CIBERSEGURIDAD.	15
2.9.1	<i>Seguridad de acceso a sistemas operativos y de información</i>	15
2.9.2	<i>Seguridad de acceso a redes.....</i>	16
2.9.3	<i>Seguridad y ubicación de los centros de procesamiento de información y comunicaciones</i>	17
2.9.4	<i>Ambiente de los centros de procesamiento de información y comunicaciones.....</i>	17
2.9.5	<i>Responsabilidad de los colaboradores del uso de los equipos de TI.....</i>	17
2.10	DISPOSICIONES RELATIVAS AL DESARROLLO DE PROYECTOS TI.	18
2.10.1	<i>Principios para el Desarrollo de Proyectos de TI</i>	18
3	SANCIONES.....	19

1 Glosario, abreviaturas y acrónimos

- ❖ Cloud Computing: El Cloud Computing o la computación en la nube es la disponibilidad bajo demanda de recursos del sistema informático, especialmente el almacenamiento de datos, procesamiento y soluciones o aplicaciones que se contratan como servicio, sin una gestión activa directa por parte del usuario y accesible a través de Internet.
- ❖ DED: Dirección de Estrategia Digital. Instancia dispuesta dentro de la estructura jerárquica de la Secretaría Técnica del SBD responsable de todo lo relacionado a las tecnologías de información y comunicaciones (TIC).
- ❖ FONADE: Fondo Nacional para el Desarrollo, creado por el artículo 15 de la Ley 9654, Reforma Ley Sistema de Banca para el Desarrollo, Ley Orgánica del Instituto Nacional de Aprendizaje (INA), Ley de Fortalecimiento de las Pequeñas y Medianas Empresas, Ley del Impuesto sobre la Renta, como un patrimonio autónomo, administrado por la Secretaría Técnica del Consejo Rector del Sistema de Banca para el Desarrollo; el cual se rige por lo establecido en la Ley del SBD y su Reglamento, así como por los lineamientos y directrices del Consejo Rector.
- ❖ PETI: Plan Estratégico de Tecnologías de Información.
- ❖ POI: Plan Operativo Institucional.
- ❖ SBD: Sistema de Banca para el Desarrollo.
- ❖ TIC: Tecnologías de información y comunicaciones.

2 Disposiciones

2.1 Disposiciones Generales

2.1.1 Sobre el Rol de los Usuarios y Jefaturas

1. Todo usuario que reciba y tenga bajo su custodia bienes de la Secretaría Técnica del SBD y FONADE, será responsable por el uso adecuado y el cuidado del equipo de cómputo asignado. Cualquier daño, pérdida, abuso o empleo ilegal que le sea imputable por falta al deber de cuidado, negligencia o dolo será responsabilidad del usuario principal y de las jefaturas o encargados cuando se compruebe negligencia de su parte en su deber de control de los recursos tecnológicos asignados en sus dependencias.
2. La jefatura o encargado de cada área será el responsable de velar por que estas disposiciones se cumplan y reportará a la mayor brevedad a DED cualquier anomalía que se presente al correo equipoded@sbdcr.com. Asimismo, la jefatura podrá también solicitar a DED una revisión técnica del sistema informático en aquellas dependencias donde existan indicios de una utilización inadecuada de éstos.

2.1.2 Divulgación y cumplimiento

1. Las disposiciones deben ser divulgadas adecuadamente a través de los directores, jefaturas y el sitio web institucional. Estas disposiciones son de materia obligada en los procesos de inducción a los nuevos funcionarios. Todos los usuarios de la Secretaría Técnica del SBD y FONADE, deberán conocer los documentos de disposiciones relativos a Tecnología de Información y regirse en su actuar por los principios consignados en ellos.

2.2 Disposiciones Administrativas

2.2.1 Servicios ofrecidos por DED

1. DED creará y mantendrá actualizado un registro de los servicios que ofrece a todas las áreas de la Secretaría Técnica del SBD y FONADE y los informará a través de la intranet.
2. Los servicios ofrecidos por DED, atención de incidentes y consultas de TI se solicitarán formalmente y siguiendo los procedimientos que se emitan para dicho fin mediante las opciones de contacto que se definan.

2.2.2 Acceso físico al área de servidores y comunicaciones

1. En general las áreas de servidores y comunicaciones de Tecnologías de Información son de acceso restringido, dadas las características de los equipos que se encuentra en dichas instalaciones. Dichos accesos deberán ser controlados por medio de algún tipo de sensor biométrico cuyo acceso está restringido y controlado por DED.
2. Los funcionarios de las diferentes dependencias podrán ingresar a lo interno de las dichas áreas siempre que haya un funcionario de DED que los acompañe personalmente.
3. Se debe contar con una hoja de firmas que registre los ingresos para los cuartos de servidores de personal ajeno a DED.

2.2.3 Documentación y mantenimiento de manuales de DED

1. DED deberá documentar formalmente todas las actividades que realice en el desarrollo de los servicios que brinda a la Institución.
2. DED mantendrá un archivo digital de gestión de documentos, debidamente ordenado y clasificado para el registro y custodia de la documentación administrativa,

correspondencia y de actividades técnicas que desarrolla. Mantendrá, como mínimo, dentro de sus archivos de gestión, las siguientes documentaciones:

- ❖ Oficios y correspondencia relacionados con DED.
 - ❖ Documentación del Plan Estratégico de Tecnologías de Información (PETI).
 - ❖ Documentación de Planes Operativos Institucionales (POI).
 - ❖ Documentación de inventario de equipos de cómputo, periféricos y de telecomunicaciones.
 - ❖ Documentación de inventario de software instalado en equipos.
 - ❖ Documentación del mantenimiento correctivo de equipos de cómputo, periféricos y telecomunicaciones.
 - ❖ Documentación de licencias de software adquiridas.
 - ❖ Documentación de proyectos formalmente desarrollados.
 - ❖ Documentación sobre solicitudes de servicio recibidas (Tickets).
3. DED mantendrá en su archivo de gestión un Compendio de Manuales que contendrá como mínimo:
- ❖ Política de TI y sus disposiciones
 - ❖ Manual de Puestos de DED.
 - ❖ Marco de Gestión de TI
 - ❖ Inventario de servicios DED
4. DED utilizará toda la documentación formal definida en la organización para el desarrollo de trámites administrativos, ejemplo compra de activos y/o contratación de bienes y servicios.

2.2.4 Adquisición de nuevas tecnologías

1. Todos los procesos institucionales de adquisición de recursos tecnológicos deben ser valorados y aprobados previamente por DED.
2. Para la adquisición o contratación de nuevos recursos de hardware, software y otros dispositivos tecnológicos, será política de DED recomendar aquellos que ofrezcan calidad comprobada y se considere son los adecuados para satisfacer las necesidades institucionales.
3. Para el trámite de adquisición o contratación de nuevos recursos informáticos, DED asesorará y apoyará al área interesada de la Secretaría Técnica del SBD y FONADE, en la definición de las características tecnológicas y evaluación de ofertas mediante recomendaciones técnicas.
4. Para la adquisición o contratación de nuevos recursos, DED verificará que no exista ningún software en la institución que pueda satisfacer las necesidades de la dirección solicitante y realizará un estudio de mercado y de proveedores en el cual comparará diversas soluciones informáticas.

5. DED velará porque los recursos informáticos adquiridos sean enviados, configurados o implementados de manera correcta. Es responsabilidad de la Dirección solicitante y usuaria de estos recursos, hacer el uso adecuado y obtener el mayor provecho de estos.

2.2.5 Inventario de equipo

1. DED mantendrá un inventario de equipo con las características de cada uno de ellos y de la persona que lo tiene asignado.
2. DED deberá revisar el inventario del equipo por lo menos una vez al año, realizando los cambios que sean necesarios y realizando un informe a la administración sobre los resultados y/o diferencias encontradas.

2.2.6 Reparación de equipos

1. Todos los usuarios deben acatar el procedimiento que DED implemente para controlar los servicios de reparación y la calidad de estos.
2. La obtención de fondos presupuestarios para la adquisición de repuestos y accesorios será gestionada a través de DED, quedando condicionado a la factibilidad técnica y presupuestaria.
3. DED tendrá un control de las garantías de los equipos adquiridos para hacer cumplir los compromisos contractuales. Para los equipos que ya no están en período de garantía se procederá a realizar el análisis de la conveniencia de reparación o sustitución quedando condicionado a la factibilidad técnica y presupuestaria.

2.3 Disposiciones relativas a sistemas de información y aplicaciones

2.3.1 Contratación de sistemas de información y aplicaciones

1. DED será el responsable de gestionar la contratación de los sistemas de información y aplicaciones que la organización requiera, de acuerdo con los recursos humanos y tecnológicos que tenga a su disposición para este fin, respetando en todo momento los procesos de contratación administrativa que rigen a la institución.
2. La contratación podrá ser para el desarrollo, la adquisición o pago por servicio del sistema de información y aplicaciones, según la conveniencia y necesidad requerida.
3. La contratación de sistemas de información y aplicaciones se hará bajo el concepto de tecnologías web, sin embargo, se podrán utilizar sistemas de información y aplicaciones “cliente” instaladas en los equipos en los casos que no sea posible obtenerlo en modalidad web.

4. La contratación de sistemas de información y aplicaciones se hará mediante proyectos debidamente formalizados, administrados y de acuerdo con la metodología y estándares de DED.
5. Las solicitudes de nuevos sistemas de información y aplicaciones deberán ser formalmente presentadas por las Direcciones de Área a DED, en forma escrita e indicando en estas los objetivos y requerimientos funcionales por cubrir, los cuales serán evaluados por DED para determinar factibilidad técnica y serán aprobados por la Dirección Ejecutiva.
6. Las pruebas de los nuevos sistemas de información y aplicaciones deberán hacerse en servidores y/o ambiente de pruebas y con la utilización de bases de datos de prueba antes de ser puestos en producción.
7. Para los proyectos de sistemas de información y aplicaciones deberán existir dos o más funcionarios que cumplan las funciones de contraparte técnica y contraparte funcional de la Institución, quienes deberán ser profesionales de DED y del área usuaria respectivamente.
8. DED coordinará con el proveedor y las Direcciones la capacitación en el sistema de información o aplicaciones contratado, y será obligación de los usuarios convocados asistir y asegurar el aprendizaje para el correcto uso del sistema y aprovecharlo al máximo.
9. Los sistemas de información y aplicaciones contratados deberán ser entregados por estas, de manera formal y debidamente documentados, incluyendo en dicha documentación el manual de los usuario correspondiente a la versión contratada. En caso de desarrollo deberán además entregar el manual técnico.
10. Los sistemas de información y aplicaciones serán de uso exclusivo de la Secretaría Técnica del SBD y FONADE, y no se permite el uso para funciones que no correspondan a las operaciones normales de la Secretaría Técnica del SBD y FONADE, excepto que exista algún convenio de cooperación entre instituciones o por autorización expresa del Director Ejecutivo.
11. Será considerado como mantenimiento de sistemas de información todas las acciones que impliquen modificaciones, correcciones, mejoras o adiciones a los sistemas de información que soliciten los usuarios de cualquier área de la Secretaría Técnica del SBD y FONADE. DED será la encargada se gestionar el mantenimiento según corresponda.

2.4 Disposiciones relativas a bases de datos.

2.4.1 Creación de bases de datos

1. DED será la encargada de aprobar el diseño físico y lógico las bases de datos, que utilizarán los sistemas de información que se desarrollen internamente y solicitará toda la documentación técnica de dichas bases de datos que permita su fácil comprensión.
2. DED podrá hacer uso de herramientas para el modelaje de datos, creación y generación de base de datos, para lo cual debe adquirirse la respectiva licencia y la capacitación para su manejo.

2.4.2 Instalación, migración o mantenimiento de bases de datos

1. Toda instalación, migración o mantenimiento de base de datos deberá ser realizada por personal técnico capacitado interno o externo, el cual deberá ser supervisado por un profesional de DED.
2. Antes de cualquier proceso de instalación, migración o mantenimiento de bases de datos se deberán realizar los respaldos respectivos, para poder recuperar toda la información hasta el último momento en caso de un error o fallo en el proceso.
3. En los casos de instalación o migración se deberá realizarse previo a ejecutarlo en ambiente de producción, una prueba en un servidor de pruebas, para garantizar que el proceso de instalación o migración funcionará correctamente.
4. En las actividades de instalación, migración o mantenimiento de información a bases de datos, se deberá seguir el procedimiento definido por DED en cada caso particular para evitar atrasos y complicaciones, así como dejar documentado en una bitácora todo lo realizado para futuras migraciones.

2.4.3 Seguridad y respaldos de las bases de datos

1. Todo acceso a las bases de datos de la Secretaría Técnica del SBD y FONADE deberán contar con los mecanismos adecuados y controlados mediante un usuario y contraseña personal, que garanticen su seguridad y la confidencialidad de la información almacenada.
2. La información deberá ser conservada durante el período que se defina por parte del área de Cumplimiento, Control Interno y Seguridad de la Información.

3. Deberán de mantenerse y aplicarse sistemas de respaldos para todas las bases de datos de la Secretaría Técnica del SBD y FONADE, con el fin de garantizar su conservación y restauración en caso necesario.
4. Deberán existir planes de recuperación de la información de las bases de datos, para garantizar la continuidad del servicio que se presta por medio de los sistemas de información.
5. Toda transacción que se ejecute en las bases de datos dejará las pistas adecuadas de auditoría que defina el área de Cumplimiento, Control Interno y Seguridad de la Información.

2.5 Disposiciones relativas a redes y telecomunicaciones.

2.5.1 Uso de las redes de datos

1. DED será la dependencia responsable de la administración de la red interna de datos.
2. DED garantizará de manera razonada el acceso controlado en la red interna de datos a los funcionarios de la Secretaría Técnica del SBD y FONADE que así lo requieran.
3. Los usuarios accederán a la red de datos por medio de un usuario y contraseña que será único y exclusivo para cada usuario, el cual será responsable por su uso.
4. Todas las operaciones que se efectúen por medio de las redes internas serán responsabilidad única de la persona al que se le asignó el usuario relacionado con las mismas.
5. DED monitoreará periódicamente los accesos a la red interna mediante herramientas de seguridad y administración.
6. No es permitido a ningún funcionario, excepto al personal del DED o a terceros autorizados por DED, instalar, configurar, administrar o manipular los componentes de la red como pueden ser y sin limitarse a: switches, routers, access points, firewalls, cableado, entre otros.
7. No se permitirá la instalación de puntos de acceso de redes inalámbricas con conexión a la red de la Secretaría Técnica del SBD y FONADE sin la debida información y autorización de DED. En caso de detección de un punto de acceso no autorizado se procederá a su inmediata desconexión de la red Institucional.
8. DED solamente prestará apoyo a los equipos conectados a la red institucional; a estos efectos, se consideran conectados a la red de la Secretaría Técnica del SBD y FONADE los equipos que accedan a la misma de forma remota a través de los medios proporcionados por DED.
9. Ningún usuario está autorizado a utilizar analizadores del tráfico que circula por la red de la Secretaría Técnica del SBD y FONADE. Igualmente está prohibido utilizar herramientas de rastreo de puertos o que permitan detectar vulnerabilidades. El uso

de estas herramientas sólo está permitido a funcionarios de DED y bajo situaciones especiales (incidentes de seguridad, denuncias de usuarios, evaluaciones, pruebas, entre otros) que lo justifiquen.

10. DED pondrá en funcionamiento herramientas de control que permitan detectar, analizar y bloquear accesos no permitidos, aquellos que no guarden relación con aspectos de trabajo o que pongan en riesgo la seguridad de los recursos informáticos y atenten contra su desempeño.

2.6 Disposiciones relativas al servicio de Internet, correo electrónico y antivirus

2.6.1 Uso de Internet, correo electrónico y antivirus

1. Los servicios de Internet, correo electrónico y antivirus serán administrados por DED.
2. Se gestionará una normativa interna de la Secretaría Técnica del SBD y FONADE para la Regulación de la Navegación en Internet.
3. Para la comunicación oficial de la Secretaría Técnica del SBD y FONADE debe utilizarse la cuenta de correo institucional.
4. El acceso a los servicios de Internet, correo electrónico y antivirus serán suministrados a todos los funcionarios de la Secretaría Técnica del SBD y FONADE en las condiciones que su puesto lo amerite.
5. El correo electrónico institucional es una herramienta de trabajo para la comunicación e intercambio oficial de información y no una herramienta de difusión indiscriminada de información o para fines no laborales.
6. Solo podrán tener cuentas de correo electrónico institucionales los miembros del Consejo Rector y los funcionarios de la Secretaría Técnica del SBD y FONADE.
7. Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar todos los lineamientos referentes al uso apropiado del lenguaje.
8. Para el envío de mensajes se aplicarán las siguientes reglas:
 - ❖ Se utilizará siempre el campo de Asunto, a fin de resumir el tema del mensaje.
 - ❖ No se enviarán mensajes a personas desconocidas, a menos que se trate de un asunto oficial que las involucre.
 - ❖ No se enviarán mensajes a listas globales, a menos que el propietario sea la persona autorizada por el superior para enviar mensajes que involucren a toda la Institución.
9. Está prohibida la utilización abusiva del correo electrónico y de las listas de distribución incluyendo la realización de prácticas tales como:

- ❖ En caso de que fuera necesario un envío masivo se recomienda usar las listas de distribución y usar el campo de "copia oculta" (Bcc ó Cco) para poner la lista de destinatarios, en caso de duda bien ponerse en contacto con DED.
 - ❖ Actividades comerciales privadas, propagación de cartas encadenadas o cualquier otra actividad no relacionada con sus funciones.
 - ❖ El insulto, la amenaza o la difamación a cualquier persona.
 - ❖ Suscribirse a periódicos, revistas, semanarios, buscadores de parejas, chats ni a ningún otro tipo de actividades o boletines electrónicos que no sean los estrictamente relacionados con el área profesional de trabajo del funcionario.
 - ❖ Descargar archivos de música, programas, videos, pornografía y cualquier otro tipo de información que no guarde estricta relación con el área profesional del funcionario. DED procurará tomar las previsiones del caso para que se bloquee por medio de software especializado, el acceso no autorizado a los servicios antes mencionados.
10. El uso de los servicios de Internet y correo electrónico deberán ser exclusivamente para desarrollar, apoyar y mejorar la calidad de las funciones asignadas a cada puesto de trabajo.
 11. Se prohíbe a los colaboradores formar parte de cadenas de mensajes o SPAM, ya que esto contribuye a la saturación de las redes de telecomunicación y facilita la divulgación de su cuenta de correo y la posible proliferación de virus en la red.
 12. Cada funcionario será responsable y cuidadoso de no abrir correos sospechosos provenientes de cuentas desconocidas. En caso de duda deberá reportarlo a algún funcionario de DED para la revisión respectiva.
 13. El funcionario que tenga acceso a servicios de correo electrónico debe evitar divulgar su cuenta a personas o entes desconocidos o con fines distintos a los laborales.
 14. Ningún equipo que esté designado como servidor debe tener asociada una cuenta de correo electrónica.
 15. El área de Capital Humano o el Director por de Área deberán notificar a DED cuando se deba crear, cerrar o inhabilitar una cuenta de correo electrónico o lista de distribución de correo.
 16. El usuario debe atender a los avisos de actualización automática del programa de detección de virus e informar a DED, cuando la actualización no se realice satisfactoriamente.
 17. Ningún usuario deberá desactivar el servicio de antivirus y en caso que aparezca desactivado por cualquier motivo deberán reportarlo de inmediato a DED.
 18. Los valores de seguridad, de aceptación de cookies y los certificados de los navegadores o browser no deberán ser cambiados, excepto por indicaciones de DED.

2.7 Disposiciones relativas al hardware.

2.7.1 Responsabilidad de uso y resguardo

1. El hardware que se encuentra en el área de servidores y los rack de comunicaciones es responsabilidad directa del personal de DED, que tendrá que velar por su correcto uso y cuidado.
2. Los otros equipos de cómputo quedan bajo la responsabilidad del usuario al que se asignen. Estos tendrán la obligación de cuidarlos, mantenerlos limpios, en buen estado y velar por su buen funcionamiento. En el caso de existir algún problema con el equipo deberán de reportarlo inmediatamente a DED para que se proceda a su revisión.
3. Los equipos portátiles (laptops, tabletas, celulares, proyectores y MIFIs), serán asignadas a los usuarios con el objetivo de cumplir sus funciones y no deberán utilizarse para uso personal.
4. Es responsabilidad del usuario custodiar los equipos portátiles asignados, por lo que deberá tomar las medidas de seguridad correspondiente dentro y fuera de la institución para evitar el robo del equipo o información. En caso de robo, deberá reportarlo inmediatamente a DED, además de realizar la respectiva denuncia a la autoridad policial respectiva.
5. Queda entendido que los recursos informáticos asignados a cada usuario lo serán en calidad de herramienta de trabajo; como tal se encuentran permanentemente bajo dominio y control de la Secretaría Técnica del SBD y FONADE, sin perjuicio del derecho a la privacidad de la información almacenada y demás derechos fundamentales establecidos por la Constitución Política.
6. Es responsabilidad de DED hacer cumplir las garantías respectivas de cada uno de los equipos; por tal razón se deberán respetar los sellos de garantía que vienen adheridos a los equipos, y velar porque el usuario final no los despegue. Es responsabilidad de DED valorar la necesidad de sustituir algún equipo cuando el mismo no garantice la funcionalidad y operatividad adecuada, esto con base en la disponibilidad presupuestaria.
7. DED llevará y mantendrá el inventario de los equipos informáticos, así como de las licencias de uso del software adquirido. Se deberá informar al Director de Área y a DED, sobre cualquier cambio del estado o ubicación del activo.
8. Los equipos de cómputo, a excepción de las computadoras portátiles (laptops), no podrán ser trasladados a otras oficinas que no sean de la Secretaría Técnica del SBD y FONADE, salvo para alguna situación específica siempre que se cuente con la debida autorización de la Dirección respectiva, lo cual se hará igualmente con conocimiento de DED y del Área de Bienes y Servicios Generales.

2.7.2 Mantenimiento del hardware instalado

1. Los usuarios tienen el deber de informar sobre fallas en el rendimiento de cada equipo, para que sea valorado y de ser necesario proceder con su corrección.
2. En el caso de fallas técnicas del equipo de cómputo, DED realizará un diagnóstico preliminar, con el objeto de procurar la solución, o en su defecto, girar las instrucciones del procedimiento a seguir para su reparación.
3. Las ampliaciones, modificaciones o adquisición (compra o renta) de equipo de cómputo, así como la actualización e instalación de software, se harán únicamente por funcionarios de DED.
4. La entrega, puesta en funcionamiento y cambio de equipo tecnológico se efectuará en coordinación con DED, utilizando para ello los procedimientos establecidos.
5. Los equipos de cómputo no podrán ser desmantelados, cambiados, abiertos ni reparados por los usuarios. Asimismo, sus componentes (entiéndase “mouse”, disco duro, teclado, memoria, fuente de poder, tarjeta madre, entre otros) no podrán ser removidos por personal no autorizado por DED.

2.7.3 Disposiciones para el desecho de equipos electrónicos

1. Los equipos electrónicos para desechar serán revisados por funcionarios de DED, generando un acta de desecho la cual será entregada al Área de Bienes y Servicios Generales como evidencia de su daño u obsolescencia para que proceda con el respetivo desecho.
2. La Secretaría Técnica del SBD procurará la entrega de sus desechos tecnológicos a empresas recicladoras que cumplan con las normativas vigentes de protección al medio ambiente.
3. Todos los equipos que se vayan a desechar o a donar, se les debe aplicar mecanismos de borrado seguro, con el fin de eliminar toda información de la Institución, contenida en los mismos.

2.8 Disposiciones relativas al software.

2.8.1 Disposiciones sobre el uso de licencias o servicios de software

1. Los programas que se utilizarán en los equipos de la Secretaría Técnica del SBD y FONADE tendrán su respectiva licencia o derecho de uso, de lo contrario es ilegal y debe eliminarse de inmediato.

2. Solo se podrán utilizar software que cuente con licencias adquiridas de forma centralizada por la Secretaría Técnica del SBD y FONADE (para software de uso común), por pago por servicio o bien por el uso de software libre.
3. DED llevará un registro actualizado de los equipos y las licencias vigentes.
4. Se prohíbe la instalación de software propiedad de la Secretaría Técnica del SBD y FONADE en equipos que no pertenezcan a la institución. En los casos de convenios de cooperación debe existir una cláusula que así lo permita. Para el caso de MS Office 365 que permite la instalación de los programas hasta en 5 equipos distintos, es el único software que queda exento de esta restricción, esto por cuanto al eliminarse la cuenta personal de cada usuario en caso de salida de la Secretaría Técnica del SBD o FONADE, las licencias instaladas quedan automáticamente desactivadas.
5. DED dará de baja todos los sistemas que estén al margen de la Ley de Derechos de Autor, lo cual se hará en un plazo razonable y será comunicado a la Dirección respectiva.
6. DED gestionará mediante los presupuestos ordinarios o extraordinarios, la compra de licencias de software con la finalidad de que siempre la Secretaría Técnica del SBD y FONADE se mantengan al día con el uso de licencias.
7. DED removerá cualquier programa de las máquinas cuando no exista licencia o derecho de uso, sin responsabilidad para ésta de los problemas que ocasione directa o indirectamente. Llevará un registro de los programas instalados ilegalmente, para que, ante la reincidencia de mantener programas instalados en forma ilegal, se proceda a reportar el asunto al área de Capital Humano y ante la Dirección correspondiente. Para la desinstalación de los programas instalados ilegalmente, DED cuidará de no violentar el derecho a la privacidad de las personas, solicitando previamente la autorización al usuario para proceder con la remoción del programa ilegal debido a la posible pérdida de datos relacionados con dichos programas.
8. Los medios de instalación originales o acceso a los portales de descarga serán custodiados por DED.

2.8.2 Disposiciones para la instalación de Software

1. DED es la responsable de la instalación de los programas de software en cada una de las computadoras de la Secretaría Técnica del SBD y FONADE.
2. Queda prohibido que los usuarios realicen instalaciones o desinstalaciones de software en sus computadoras. De requerir un software específico debe solicitarse a DED para que se valore la necesidad laboral de su instalación.
3. En caso de que los usuarios requieran instalar, ejecutar, o copiar de Internet programas (software) diferentes al instalado en sus equipos, deberán coordinar previamente con DED. Lo anterior, con el fin de evitar riesgos legales o de funcionamiento de los equipos.

4. Queda prohibida la instalación del software adquirido por DED en equipos que no sean de su propiedad.
5. Conforme se adquieran nuevas versiones del Software, DED realizará la respectiva instalación en los equipos de la institución.

2.9 Disposiciones relativas a la ciberseguridad.

2.9.1 Seguridad de acceso a sistemas operativos y de información

1. DED es la responsable de establecer y gestionar adecuadamente un usuario y contraseña para la seguridad de acceso a los sistemas operativos, sistemas de información, bases de datos y redes que operen en los equipos de la Secretaría Técnica del SBD y FONADE.
2. En la activación de usuarios de sistemas operativos, se crearán identificadores de usuario utilizando el estándar de *nombre.apellido* y de ser necesario la primera letra del segundo apellido.
3. Siempre que los sistemas operativos utilizados lo permitan, deberá controlarse el número de intentos de ingreso fallidos. Luego de 5 intentos, deberá bloquearse la cuenta del usuario y no permitir su ingreso al sistema. La cuenta debe estar bloqueada por 30 minutos y personal DED podría desbloquearla antes por solicitud del usuario involucrado.
4. En el caso que el sistema operativo lo permita, se deberán implementar las bitácoras de seguimiento a los accesos, donde se registren los ingresos al sistema y los intentos fallidos.
5. Para evitar situaciones de peligro para la Secretaría Técnica del SBD y FONADE, se desactivarán o bloquearán las cuentas de usuario a aquellas personas que estén en vacaciones, con permisos o incapacidades mayores a quince días, para lo cual Capital Humano debe informar a DED con al menos 3 días hábiles de antelación. En caso que deba mantenerse activa la cuenta deberá contarse con la autorización del Director del Área.
6. En caso de despido de un funcionario, el permiso de acceso deberá desactivarse o bloquearse previamente a la notificación de la persona sobre la situación.
7. El área de Capital Humano deberá notificar a DED cuando se deba crear, bloquear o inhabilitar los accesos a un funcionario sea por motivo de ingreso, salida, suspensión, incapacidad, vacaciones, etc.
8. Los directores de la Secretaría Técnica del SBD serán los responsables de autorizar o solicitar modificación de los accesos que tendrán los funcionarios de sus áreas en los sistemas y redes de la Secretaría Técnica del SBD y FONADE.

9. Ningún funcionario de DED podrá cambiar ninguna clave de acceso, si no es por solicitud expresa de su dueño. En caso de ser necesario y a solicitud de la jefatura o del director se bloquearán los accesos de un usuario específico.
10. Se requiere salvaguardar la confidencialidad de la clave de acceso (contraseña) y abstenerse de facilitarla a terceros por cualquier motivo. Cada usuario será responsable de las acciones que se reporten ejecutadas con su clave de acceso. En los casos de sustitución, se asignará al sustituto, un nombre de usuario y una clave de acceso transitoria y nunca la correspondiente a la persona sustituida.
11. Cada usuario generará sus propias claves de acceso, cada cierto período de tiempo en la medida que las posibilidades técnicas así lo permitan. Las claves de acceso como mínimo deberá contener letras mayúsculas, minúsculas y números. El período lo establecerá DED, dependiendo de la sensibilidad de la información.
12. El usuario no debe dejar las claves de acceso escritas en medios o lugares donde puedan ser obtenidas por terceros (Ej.: monitor, carpetas, escritorio)
13. Cuando el usuario olvide u extravíe su clave de acceso, deberá acudir a DED e identificarse como propietario de la cuenta para que se le proporcione una nueva, o la utilización de cualquier otro medio de verificación que DED defina para la restauración de contraseñas.
14. Cuando un usuario se ausente de su puesto de trabajo deberá dejar bloqueado el equipo para no dejar información expuesta en pantalla o la posibilidad que alguien más pueda operar o ejecutar alguna acción desde esa computadora. Al concluir las labores del día o la tarea en el sistema que esté utilizando deberá dejar cerradas todas las sesiones que tenga abiertas.
15. Está prohibido el almacenamiento, la transmisión, transferencia y, difusión de datos de carácter personal en los equipos de la Secretaría Técnica del SBD y FONADE, sin contar con autorización válidamente emitida por quien esté legitimado para ello.
16. Todos los archivos de trabajo y documentos digitales se deben de almacenar en el OneDrive de cada colaborador, donde dichos documentos están debidamente respaldos y accesibles desde la nube de MS Office 365.

2.9.2 Seguridad de acceso a redes

1. DED asignará las claves de acceso a los usuarios, además procederá conforme con la activación y desactivación de usuarios de las redes de la Secretaría Técnica del SBD y FONADE.
2. Para la utilización de las redes de datos, los nombres de usuario para las mismas se crearán siguiendo el esquema de *nombre.apellido* y de ser necesario la primera letra del segundo apellido.

2.9.3 Seguridad y ubicación de los centros de procesamiento de información y comunicaciones

1. Los centros de procesamiento de información y comunicaciones deberán estar ubicados dentro del edificio de la Secretaría Técnica del SBD y FONADE, a menos que se disponga por parte de DED a instalarlos en sitios externos (ejemplo data center, cómputo en la nube) especializados y con la seguridad necesaria.
2. Los centros de Datos deben estar completamente cerrados y con puertas de acceso controladas con sensores o llaves bajo la custodia de DED, las cuales deberán permanecer siempre cerradas.
3. Todo el cableado eléctrico que sea utilizado en los equipos de los centros de procesamiento de información y comunicaciones deberá ser totalmente independiente al cableado normal del edificio.
4. Para efectos de cableado eléctrico y de datos se utilizarán las normas de cableado que se fundamenten en las mejores prácticas utilizadas en el mercado.

2.9.4 Ambiente de los centros de procesamiento de información y comunicaciones

1. El área asignada para los centros de procesamiento de información y comunicaciones debe estar dotada con las condiciones ambientales de humedad y temperatura necesarias para garantizar un entorno físico conveniente para su funcionamiento y contar con sensores automáticos para su control.
2. Los centros de procesamiento de información y comunicaciones deberán estar climatizado permanentemente a una temperatura que se encuentre entre los 18º y 22º para garantizar el mejor rendimiento de los componentes electrónicos y alargar la vida útil de los mismos.
3. Se requiere que exista control mediante cámaras de videovigilancia para el registro de personas y actividades dentro de estos centros de procesamiento.

2.9.5 Responsabilidad de los colaboradores del uso de los equipos de TI

1. Los colaboradores de la Secretaría Técnica del SBD y FONADE usarán el equipo de cómputo en labores exclusivamente de trabajo y serán responsables por el uso adecuado de las herramientas tecnológicas.
2. Los colaboradores de la Secretaría Técnica del SBD y FONADE deberán abstenerse de utilizar los recursos informáticos de la institución para realizar actividades personales o con fines lucrativos. Los recursos asignados deberán ser utilizados únicamente para cumplir los objetivos organizacionales.

3. Los colaboradores de la Secretaría Técnica del SBD y FONADE no deberán consumir ni preparar alimentos en la mesa destinada para el computador, para evitar derrame de estos sobre los equipos, que pueden ocasionar trastornos en su operación.
4. El costo por la reparación o sustitución de los equipos de cómputo a raíz de los desperfectos causados por situaciones de descuido en su uso, lo asumirá el colaborador responsable, sin perjuicio de las sanciones disciplinarias que correspondan, para lo cual se seguirá el respectivo procedimiento administrativo.
5. Ningún colaborador está autorizado para almacenar material pornográfico u ofensivo en ningún medio de almacenamiento de las computadoras, dispositivos periféricos u dispositivo de almacenamiento en la nube, mucho menos propagarlo a otras personas.
6. Por razones de seguridad se prohíbe el uso de mensajería instantánea, chat o similares fuera del canal oficial de la Secretaría Técnica del SBD y FONADE que es Webex Teams o Microsoft Teams, a menos que se justifique el uso para lo cual debe solicitarse por medio de la jefatura, manifestándose los cuidados y supervisión que ejercerá sobre su uso.
7. Está prohibido conectarse a Internet utilizando equipos diferentes a los que oficialmente se encuentren en servicio.
8. Las computadoras y dispositivos móviles son propiedad de la institución y son asignadas a los colaboradores para que desarrollen sus funciones en la institución, por tanto, para efectos del SDB toda la información contenida en las mismas es de acceso permitido. En caso de requerirse por cualquier motivo acceder al equipo de un funcionario, este no podrá alegar que la institución está violando su privacidad, por cuanto toda la información almacenada en los equipos es propiedad de la Secretaría Técnica del SBD y FONADE excepto la claramente identificada como de carácter personal.

2.10 Disposiciones Relativas al Desarrollo de Proyectos TI.

2.10.1 Principios para el Desarrollo de Proyectos de TI

1. Toda solicitud de modificación a sistemas existentes, así como nuevos desarrollos o adquisición de nuevos sistemas debe presentarse a través de la una solicitud de cambios o de nuevos requerimientos de sistemas autorizada por el Director de Área.
2. DED debe analizar la solicitud, su justificación, objetivos y evaluar la factibilidad para llevar la modificación de un sistema actual o la ejecución de un nuevo proyecto.
3. DED debe homologar y fomentar la utilización de las herramientas de apoyo disponibles en la Institución, que mejor se adapten a la metodología aplicada y que cumpla con los requisitos mínimos exigibles por los controles institucionales:

1. Identificación del objetivo del proyecto, necesidad o problema
 2. Documento de requerimientos y plan de ejecución
 3. Indicadores de seguimiento y control de avance
 4. Documento de aceptación del proyecto y su respectivo cierre
4. Los nuevos proyectos deben adherirse a un procedimiento institucional formal de iniciación del proyecto definido por la Secretaría Técnica del SBD cuando el impacto de estos lo amerite, ya sea por su importancia en la organización, como lo es un sistema de misión crítica o bien porque el tiempo de desarrollo e implementación estimado es igual o superior a los 4 meses.
 5. Para todos los proyectos que dependan de la contratación de servicios o adquisición de bienes tecnológicos, la definición de los recursos económicos, humanos y materiales dependerá de la disponibilidad presupuestaria y se deberán cumplir los procedimientos y normatividad establecidos por la Institución.
 6. DED será responsable de coordinar la conformación del equipo de proyecto, para lo cual cada Dirección de Área involucrada en el proyecto deberá asignar el personal requerido.

3 Sanciones

Sanciones aplicables ante faltas a estas disposiciones seguirán los lineamientos administrativos definidos por la institución, con respeto a las leyes de la República vigentes y los tratados internacionales que apliquen.