Manual de Políticas y Procedimientos de las Tecnologías de Información del Instituto Crecer Juntos

AÑO 2024

GOBIERNO DE EL SALVADOR

Índice

Acuerdo de Dirección Ejecutiva ICJ-DE-033-2024

San Salvador, 30 de septiembre de 2024. El Instituto Crecer Juntos,

Considerando:

I. Que la Constitución de la República, en el artículo 34, reconoce a las niñas y niños el derecho a vivir en condiciones familiares y ambientales que le permitan su desarrollo integral, para lo cual tendrá la protección del Estado. La Ley establecerá y determinará los deberes del Estado y creará las instituciones para la protección de la maternidad y de la infancia.

II. Que la Ley Crecer Juntos para la Protección Integral de la Primera Infancia, Niñez y Adolescencia crea el Instituto Crecer Juntos como institución oficial con personalidad jurídica de derecho público, patrimonio propio y autonomía en lo técnico, financiero y administrativo; referente en materia de Primera Infancia; con énfasis en la atención de niñas y niños desde su gestación hasta cumplir los cuatro años, que forma parte del Sistema Nacional de Protección Integral a la Primera Infancia, Niñez y Adolescencia.

III. Que Los Lineamientos Específicos para la Elaboración del Proyecto de Normas Técnicas de Control Interno Específicas por las Entidades del Sector Público, reconoce, que la normativa interna es uno de los aspectos a considerar en el Sistema de Control Interno de cada entidad del sector público y uno de los documentos normativos que deberá establecerse es el Manual de Políticas y Procedimientos de las Tecnologías de Información, que definirá los controles aplicables al procesamiento electrónico de datos, con el propósito de salvaguardar el diseño, ciclo de operación y desarrollo de los sistemas; así como, la utilización de los sistemas operativos y equipos tecnológicos.

IV. Que es necesario emitir el Manual de Políticas y Procedimientos de las Tecnologías de Información del Instituto Crecer Juntos, a efecto de permitirle cumplir, de manera eficaz y eficiente, sus obligaciones legales en materia fiscal.

Por tanto:

En uso de sus facultades legales,

Acuerda,

Emitir el siguiente:

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS DE LAS TECNOLOGÍAS DE INFORMACIÓN DEL INSTITUTO CRECER JUNTOS

CAPÍTULO I
GENERALIDADES

1.1. Objetivo

Establecer los controles aplicables al procesamiento electrónico de datos, con el propósito de salvaguardar el diseño, ciclo de operación y desarrollo de los sistemas; así como, la utilización de los sistemas operativos y equipos tecnológicos del Instituto Crecer Juntos.

1.2. Alcance y campo de aplicación

1.2.1. Alcance:

Comprende las políticas y procedimientos para el procesamiento electrónico de datos, con el propósito de salvaguardar el diseño, ciclo de operación y desarrollo de los sistemas; así como, la utilización de los sistemas operativos y equipos tecnológicos del Instituto Crecer Juntos, en adelante, ICJ.

1.2.2. Campo de aplicación:

El presente instructivo es de obligatoria aplicación para todas las Unidades Organizativas del ICJ.

1.3. Base legal

1.3.1. Circular Externa No. 03/2018. Lineamientos Específicos para la Elaboración del Proyecto de Normas Técnicas de Control Interno Específicas por las Entidades del Sector Público.

1.4. Definiciones

- **Alta autoridad**: funcionario público que desempeña cargo de Gerente o Director/a Ejecutivo en el ICJ.
- **Automatización**: La automatización es un sistema donde se transfieren tareas realizadas habitualmente por operadores humanos a un conjunto de elementos tecnológicos, que sirven para estandarizar los procesos de trabajo; desarrollar componentes reutilizables y configurables; y automatizar actividades rutinarias con las tecnologías adecuadas.
- **Integridad de la información**: La información solo puede ser modificada por quien está autorizado y de manera controlada.
- **Jefatura de Unidad Organizativa**: Empleado público responsable jerárquicamente de una unidad organizativa determinada.
- **Seguridad de la información**: Es el conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten, resguardar y proteger la información, buscando mantener la confidencialidad, la disponibilidad e integridad de esta.
- **Sistemas de Legado**: Tecnología o aplicación, software antiguo o desactualizado que sigue en uso, no recibe mantenimiento ni soporte en una institución.
- **Unidad organizativa**: Instancias de la estructura organizacional, que según el organigrama vigente dependen directamente de una alta autoridad del Instituto Crecer Juntos.
- **Vulnerabilidad**: posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

CAPÍTULO II
DESARROLLO

2.1. Políticas

2.1.1. Políticas Generales

2.1.1.1. El presente documento normativo deberá actualizarse cada vez que sea necesario para poder implementar un proceso de mejora continua en la gestión de las tecnologías de información.

2.1.1.2. El DTDI, elaborará y ejecutará el presupuesto asignado para la gestión de las tecnologías de información y comunicación institucional y los proyectos tecnológicos viables a desarrollar, conforme a su nivel de madurez tecnológico de acuerdo con su tamaño, alcance y ámbito de gestión, los objetivos estratégicos y operativos de la institución y acorde con el plan de compras institucional.

2.1.1.3. El DTDI debe garantizar el equipamiento de todas las unidades organizativas, técnicas y administrativas, de acuerdo con la disposición y el presupuesto asignado para la compra de bienes y servicios.

2.1.1.4. El Departamento de Tecnología y Desarrollo Informático, en adelante, DTDI, será la Unidad Organizativa responsable de gestionar el ciclo de los sistemas operativos y equipos tecnológicos del ICJ.

2.1.1.5. El DTDI, gestionará el ciclo de los sistemas operativos y equipos tecnológicos, estableciendo bases y acciones tendientes a:

- Fomentar el desarrollo de una estructura informática institucional, innovadora, compatible, segura y eficiente.
- Promover la optimización de los recursos humanos y materiales por medio del uso de sistemas informáticos adecuados.
- Optimizar los recursos financieros destinados a las tecnologías de la información.
- Fomentar la automatización eficiente de los procesos administrativos y operativos, institucionales.

2.1.2. Políticas específicas para el uso de licencias de software

2.1.2.1. Es responsabilidad de la DTDI, levantar por cada equipo tecnológico instalado, el acta de hardware y software correspondiente, indicando en ella las disposiciones establecidas para un uso ético y adecuado, las cuales deberán ser respetadas por todo el personal del ICJ.

2.1.2.2. El DTDI deberá mantener bajo su custodia las licencias originales que se adquieran en la modalidad de compra de software en versión completa (dentro de la caja).

2.1.2.3. El DTDI deberá administrar el acceso al sitio web de los fabricantes de software, para las adquisiciones de software en la modalidad de "compras por volumen".

2.1.2.4. Ningún empleado público del ICJ podrá hacer copias del software instalado, sin el expreso consentimiento del propietario del software, permitiendo solamente copia del software, para fines de respaldo o de seguridad, si la licencia así lo permite.

2.1.2.5. Se prohíbe el uso de software obtenido de cualquier otra fuente que pueda amenazar la seguridad y aspectos legales del ICJ.

2.1.2.6. Será responsabilidad del DTDI, velar por el cumplimiento y respeto de las disposiciones establecidas en el "Acta de software o hardware" instalado, de cada uno de los

empleados que tenga bajo su responsabilidad el uso de una computadora, realizando para ello inspecciones periódicas anunciadas o sorpresivas.

2.1.2.7. Cuando la DTDI compruebe ilegalidad en el uso de softwares, borrará copias instaladas en el equipo informático, sin previa autorización de los empleados públicos.

2.1.2.8. Toda licencia de software que no esté en uso podrá ser reasignada por la DTDI, en alineación a las necesidades institucionales.

2.1.2.9. El ICJ podrá optar por el uso de software libre, pero siempre se deberá justificar las necesidades de su utilización, siendo la DTDI, la responsable de efectuar el análisis técnico correspondiente, para asegurar que no sea fuente de código malicioso que pudiese afectar el recurso informático institucional.

2.1.3. Políticas específicas para el control de Equipo Informático

2.1.3.1. El proceso de recepción de todo equipo informático nuevo se realizará en coordinación con la Sección de Activo Fijo del Departamento de Administración, Bienes y Servicios, de acuerdo con los procedimientos establecidos y apoyándose en las especificaciones técnicas aprobadas por el DTDI.

2.1.3.2. Cada equipo informático deberá poseer un acta de mantenimiento preventivo actualizado, en el que se detallarán las actividades de mantenimiento realizadas. Dicha actualización será responsabilidad del DTDI.

2.1.3.3. Se deberá programar y ejecutar anualmente el mantenimiento preventivo a cada equipo informático dos veces por año, siendo responsabilidad del DTDI incluir en el plan de compras anual, el presupuesto para la adquisición de los materiales que se utilizarán en dicho servicio o la contratación de una empresa especializada en dichos tipos de equipos.

2.1.3.4. Toda anomalía relacionada al funcionamiento del equipo informático institucional deberá ser reportada oportunamente por la persona responsable del mismo a el DTDI.

2.1.3.5. Ningún empleado público de equipo informático está autorizado a remover la cubierta, quitar o dañar la etiqueta de garantía, esta responsabilidad será exclusivamente del DTDI.

2.1.3.6. El DTDI, será responsable de llevar un control de la ubicación de todo recurso informático, por lo que las jefaturas de Unidades Organizativas o Altas Autoridades deberán informar al DTDI cualquier movimiento o traslado de los recursos informáticos.

2.1.3.7. El DTDI, será responsable de la administración del contrato de telefonía y se encargará de asignar un dispositivo móvil a cada empleado, también tendrá a disposición tablets y dispositivos similares, los cuales asignará de acuerdo sean necesarios.

2.1.4. Políticas específicas para la Administración de Redes

2.1.4.1. El DTDI será responsable de administrar, mantener seguro y evitar el inadecuado uso de las redes institucionales.

2.1.4.2. El DTDI tendrá la responsabilidad de brindar el soporte técnico necesario para el buen funcionamiento de las páginas web oficiales. La responsabilidad de actualizar, asegurar y verificar el contenido de dichos sitios web, será de las Unidades Organizativas relacionadas misionalmente al contenido técnico y comunicacional.

2.1.5. Políticas específicas para Sistemas Informáticos.

2.1.5.1. Toda instalación, desarrollo o modificación de los sistemas informáticos institucionales, deberá ser solicitada a la DTDI, según corresponda.

2.1.5.2. Las Unidades Organizativas serán responsables de presentar al DTDI el perfil de proyecto de sistema informático a desarrollar en los formatos puestos a disposición por dicha Unidad Organizativa. El DTDI atenderá y priorizará en atención a las prioridades y recursos institucionales para su desarrollo.

2.1.5.3. El DTDI será responsable de atender y resolver los problemas que en cuanto a uso y funcionamiento de los sistemas institucionales puedan presentarse.

2.1.5.4. Todos los sistemas informáticos desarrollados y adquiridos, serán propiedad del Instituto Crecer Juntos, por lo que ningún empleado podrá comercializarlo.

2.1.5.5. Las unidades organizativas deberán desarrollar los manuales técnicos de uso de los sistemas informáticos desarrollados, los cuales deberán siempre remitirse al DTDI para la custodia correspondiente.

2.1.5.6. La calidad de los datos que se ingresarán en los sistemas informáticos institucionales será responsabilidad de cada empleado público responsable del registro en cada Unidad Organizativa.

2.1.6. Políticas específicas para sistemas especiales y nueva tecnología proporcionada por entidades externas.

2.1.6.1. Las Jefaturas de Unidades Organizativas deberán informar e integrar al DTDI en cualquier proceso de adquisición y de implementación de sistemas especiales que se basan en el uso de tecnologías informáticas.

2.1.6.2. La Unidad de Compras Públicas y las Jefaturas de Unidades Organizativas, deberán asegurarse de que, en los contratos de adquisición de sistemas especiales basados en él un plan de formación, copia de manuales, especificaciones técnicas, licencias originales del software y copias de las garantías de los equipos a nombre del ICJ.

2.1.6.3. Las Jefaturas de Unidades Organizativas, deberán asegurar que los proveedores de sistemas especiales que se basan en el uso de tecnologías informáticas incluyan en su plan de capacitación a un representante del DTDI.

2.1.7. Políticas específicas para manejo de datos e/o información

2.1.7.1. Todo empleado público que utilice sistemas informáticos institucionales será responsable del buen uso y confidencialidad de la información generada, quedando prohibida la utilización de dicha información para fines incompatibles a los intereses del ICJ.

2.1.7.2. Es responsabilidad de cada empleado público realizar respaldos periódicos de toda la información producida mediante el uso de software de oficina y/o especializado, en atención a los tiempos y lineamientos técnicos establecidos por el DTDI.

2.1.7.3. El DTDI es responsable de realizar los respaldos de datos que residen en los servidores de datos institucionales.

2.1.7.4. Toda documentación elaborada por el personal institucional en sistemas ofimáticos y otros tipos de software, será propiedad del ICJ, por lo que deberá ser resguardada adecuadamente por cada empleado público y entregada a su jefatura inmediata acorde a

los lineamientos establecidos por la sección de gestión documental y archivo, si este se retira de sus funciones en la institución.

2.1.7.5. El DTDI deberá efectuar un respaldo de toda la documentación desarrollada y de correos electrónicos que se encuentren en la computadora, ante el retiro de empleados públicos, con el fin de asegurar que dicha documentación no se pierda.

2.1.8. Políticas específicas para el cuido y uso de equipos

2.1.8.1. Se prohíbe ingerir todo tipo de alimentos y bebidas sobre el equipo informático institucional.

2.1.8.2. El buen uso y funcionamiento de los equipos informáticos es responsabilidad de cada empleado público que lo tiene asignado.

2.1.8.3. Todo traslado de equipo informático deberá ser informado por el responsable de este, al DTDI.

2.1.8.4. Todo equipo informático adquirido, deberá contar con una adecuada instalación eléctrica y los equipos o accesorios que se consideren necesarios para su adecuada protección.

2.1.8.5. Cualquier daño ocasionado al equipo informático, por negligencia comprobada del empleado público, se reportará al Jefe de la Unidad Organizativa correspondiente, para la deducción de responsabilidades y para que realice los trámites necesarios en la reparación del bien.

2.1.8.6. El mantenimiento preventivo y correctivo de equipos informáticos será coordinado por el DTDI.

2.1.9. Políticas específicas para Planes de Contingencia

2.1.9.1. El DTDI, deberá incorporar en el Plan de Contingencia para el resguardo y protección de personas, bienes e información, todos los elementos necesarios para asegurar la continuidad del funcionamiento de los sistemas informáticos y el resguardo de la información del ICJ ante cualquier situación o evento no previsible.

2.1.10. Políticas específicas para el mantenimiento a sistemas de legado

2.1.10.1. Cada sistema que utilice tecnología anterior deberá tener un técnico DTDI asignado para su mantenimiento.

2.1.10.2. Se podrá actualizar información en la base de datos de sistemas de legado, previa solicitud realizada por el Jefe de la Unidad Organizativa, a través de los canales de comunicación establecidos por el DTDI.

2.1.10.3. La actualización directa a la base de datos de sistemas de legado será exclusiva para aquellos casos donde el módulo informático no cuente con los mecanismos de actualización o porque no sea posible su adecuación, procurando que dichos sistemas sí tengan esa funcionalidad.

2.1.10.4. El técnico informático asignado, deberá registrar las acciones realizadas a cualquier actualización a la base de datos de sistemas de legado en el formulario indicado, detallando las tablas afectadas con sus respectivos campos.

2.1.11. Políticas específicas para el uso de contraseñas o password

2.1.11.1. El manejo seguro de toda contraseña o password es responsabilidad del empleado público.

2.1.11.2. La contraseña o password deberá ser actualizada periódicamente por el empleado público, empleando el mecanismo del sistema operativo del equipo informático que utilice.
2.1.11.3. La contraseña o password debe cumplir los requerimientos de seguridad establecidos por el DTDI en atención a los softwares a utilizar.

2.1.12. Políticas específicas para el uso de correo electrónico

2.1.12.1. Las cuentas de correo electrónico que se asignen a los empleados públicos serán para uso oficial, y se formarán utilizando el nombre y apellido del empleado público a la que será asignado.
2.1.12.2. Está prohibido abrir archivos adjuntos de correo electrónico recibidos de remitentes desconocidos, ya que pueden contener virus u otros códigos dañinos, que pueden poner en riesgo la fidelidad de la información almacenada en los equipos.
2.1.12.3. Los empleados públicos no deberán enviar mensajes no solicitados de correo electrónico (correo SPAM), ni cadenas de mensajes, correo basura o materiales publicitarios o de carácter erótico.
2.1.12.4. Está prohibido utilizar el correo institucional para suscribirse a sitios como periódicos, moda, deportes, viajes, entretenimiento y/o todos aquellos sitios que no tienen ninguna relación con el quehacer del Instituto, ya que podrían ser fuente de correo SPAM.
2.1.12.5. Toda solicitud de creación de una cuenta de correo electrónico podrá ser autorizada por la Jefatura de Unidad Organizativa, quien justificará y explicará el uso que se dará a dicho servicio, debiendo solicitarlo al DTDI.

2.1.13. Políticas específicas para la adquisición de recurso informático

2.1.13.1. La adquisición de bienes informáticos se apegará a los procedimientos establecidos por la Ley de Compras Públicas, así como a la Ley del Presupuesto de Egresos del Estado para el Ejercicio Fiscal correspondiente.
2.1.13.2. Las tecnologías de información que se planeen adquirir deberán ser congruentes con los servicios que se pretenden prestar y apegarse a las medidas de racionalidad y disciplina presupuestal vigentes.
2.1.13.3. Toda adquisición de recurso informático deberá contar con la validación técnica correspondiente, consistente en las especificaciones y configuraciones de los bienes informáticos solicitados por las diferentes unidades organizativas, por lo que será requisito indispensable contar previamente con ésta a fin de iniciar con el proceso de adquisición correspondiente.
2.1.13.4. No se autorizará la compra de bienes informáticos usados o remanufacturados.
2.1.13.5. Toda adquisición de bienes informáticos deberá estar amparada por una garantía por parte del fabricante, o en su defecto del distribuidor (proveedor).
2.1.13.6. El ICJ en lo posible procurará efectuar compras conjuntas, para obtener mejores precios de compra, salvo en casos emergente y justificados, se podrá efectuar compras independientes.
2.1.13.7. El ICJ renovará sus equipos informáticos basados en los siguientes criterios:

- Tiempo de uso del equipo.
- Insuficiencia de las especificaciones técnicas para el uso designado del equipo.

- Condiciones de funcionamiento del equipo, el cual se revisará en forma anual durante el servicio de mantenimiento de este.

2.1.14. Políticas específicas para la utilización de servicios de internet

2.1.14.1. El ICJ proveerá el servicio de acceso a Internet, para ser utilizado para fines institucionales.

2.1.14.2. EL DTDI, deberán de controlar y restringir el acceso a los sitios WEB de las siguientes categorías: pornografía y entretenimiento.

2.1.14.3. Los empleados públicos deberán evitar el acceso para ver Televisión a través de Internet y descargar de Internet: Música, Películas y Juegos.

2.1.14.4. La utilización de las diferentes redes sociales podrá autorizarse, si se justifica la utilización para fines laborales

2.1.15. Políticas específicas para la gestión de usuarios institucionales

2.1.15.1. Para acceder a los sistemas informáticos institucionales, deberá contarse con una cuenta del empleado público, exceptuando los casos en que el software implementado tenga sus propios usuarios de administración.

2.1.15.2. Cuando existan empleados que finalicen la relación laboral con el ICJ, se deberá "inhabilitar" al usuario en un máximo de un mes posterior al retiro, generando los respaldos de información correspondientes.

2.1.16. Políticas específicas para el resguardo de la sala de servidores informáticos y de sistemas especializados administrados por el DTDI

2.1.16.1. Únicamente el personal del DTDI, podrán ingresar a la Sala de Servidores Informáticos y Cuartos de Sistemas Especializados que estén siendo administrados en forma directa por el DTDI.

2.1.16.2. Se prohíbe que el personal del ICJ, ajeno al DTDI, ingrese donde se encuentran físicamente los equipos informáticos y de comunicaciones, sin antes haber presentado una solicitud al DTDI en donde se explique la razón por la cual desea ingresar y esta haya sido aprobada.

2.1.16.3. En caso de que la Jefatura del DTDI, haya aprobado la solicitud de ingreso a las salas administradas, de aquellos empleados que lo hayan solicitado para fines laborales, se delegará un Técnico que acompañe al visitante mientras éste permanece en dicha sala.

2.1.16.4. Se deberá registrar el ingreso a la sala de servidores y de comunicaciones que administre el DTDI, para lo cual deberá llevarse una "bitácora" de ingresos a la misma.

2.1.16.5. Todos los elementos que se encuentren dentro de las salas de servidores informáticos y de comunicaciones que se administren, son responsabilidad del DTDI, por lo que deberán contar con las llaves de acceso a dichas áreas, y de ser posible, habilitar accesos electrónicos, pero siempre limitando el acceso al personal interno del DTDI que se designen. Estas medidas ayudan a lograr lo siguiente:

- Evitar ingresos no autorizados.
- Evitar que personal no autorizado, manipule el cableado de red y este pierda la configuración ya establecida.
- Asegurar el buen estado de la red.

- Proteger la integridad de los equipos.
- Asegurar la comunicación entre todas las empresas.
- Garantizar que los empleados públicos dispongan siempre de los servicios de acceso a los diferentes sistemas informáticos, correo electrónico, consultas web y páginas web.

2.2. Procedimientos

2.2.1. Procedimiento para la adquisición de recurso informático

No de acción	Responsable	Descripción
01	Altas Autoridades / Jefaturas de Unidades Organizativas	Determinan las necesidades de recursos informáticos con base en las necesidades institucionales
02	DTDI	Recibe solicitud y elabora requerimiento de compra con base en: 1. Especificaciones del equipo solicitado. 2. Satisfacción de sus necesidades a corto y mediano plazo. 3. Especificaciones técnicas vigentes establecidas por el DTDI 4. Procedimientos vigentes de la Unidad de Compras Públicas -UCP-
03	Encargado de Activo Fijo	Reciben equipos informáticos por parte de proveedores y notifica al DTDI, la recepción del equipo adquirido.
04	DTDI	Retira los equipos informáticos y/o accesorios de la Sección de Activo Fijo.
		Verifica que el equipo informático cumpla con los requerimientos técnicos detallados en el requerimiento de compra
		Si todo está correcto lo instala, prueba el equipo informático en el lugar indicado por la unidad solicitante y lo configura. Instala el software correspondiente y activa las licencias de software si es necesario.
		Registra el software instalado, en el formulario respectivo (Cuando aplica)
05	Unidades Organizativas	Firman acta de entrega, y los formularios correspondientes de Inventario de activo fijo
06	Técnico del DTDI	Entrega copias de actas en formato digital al empleado público responsable.

2.2.2.Procedimiento para la modificación a los sistemas informáticos desarrollados.

No de acción	Responsable	Descripción
01	Jefatura de Unidad Organizativa	Solicita la modificación del sistema, a través de los medios de comunicación, a la jefatura del DTDI.
02	Jefe del DTDI	Asigna técnico DTDI para que efectúe el análisis de impacto de los cambios solicitados y la factibilidad de desarrollarlos e implementarlos. Si es factible, continua a paso 03. Si no es factible, explica el motivo de la no procedencia a la Unidad Organizativa.
03	Técnico del DTDI	Con la autorización de la Jefatura DTDI, realiza modificación de sistema desarrollado.

2.2.3.Procedimiento para la administración de perfiles y usuarios

No de acción	Responsable	Descripción
01	Jefatura de Unidad Organizativa	Solicita habilitación o deshabilitación de usuarios a través de los medios puestos a disposición por el DTDI.
02	Jefatura DTDI	Asigna a técnico DTDI
03	Técnico del DTDI	• Recibe el formulario y verifica si existe el usuario dentro de la configuración existente. • Si el usuario no existe, lo adiciona al catálogo de usuarios • Si existe el usuario y se requiere "habilitación" de opciones, lo habilita según lo requerido. • Si lo requerido es "inhabilitación" de opciones de menú, se revisa a qué perfiles pertenece el usuario y se elimina de dichos perfiles, o se "inhabilitan" las opciones ya no requeridas • Informa a la Jefatura de Unidad Organizativa, la actualización del perfil
04	Jefatura de Unidad Organizativa	Verifica lo requerido e informa su conformidad.

2.2.4. Procedimiento para soporte técnico de recursos informáticos

No de acción	Responsable	Descripción
01	Servidor Público	Informa de problemas en el uso del recurso informático que tiene asignado y solicita apoyo en forma directa al Técnico DTDI.
02	Técnico del DTDI	• Verifica la falla o asesorías necesarias y da soporte técnico para solucionarlo. • Registra servicio realizado en el formulario correspondiente. • Solicita al empleado público atendido la conformidad del servicio proporcionado. • Si existe no conformidad en el servicio, busca información técnica del problema, para solventar el inconveniente al empleado público. • Informa los resultados del soporte técnico brindado al Jefe del DTDI o Encargado de Sección, según corresponda

2.1. Control de formatos y anexos.

El control de los formatos y anexos se realizará en un documento complementario al presente documento normativo. La codificación de los formatos y las versiones originales serán administradas por la UPDI.

CAPITULO III
VIGENCIA

El presente documento normativo, entrará en vigencia a partir de su aprobación en el acta de acuerdo de Dirección Ejecutiva correspondiente.

COMUNÍQUESE. –

Instituto crecer Juntos

AÑO 2024

GOBIERNO DE EL SALVADOR