"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Bicentenario del Perú: 200 años de Independencia"

Miraflores, 09 de Septiembre del 2021

RESOLUCIÓN DE DIRECCIÓN EJECUTIVA N° 000150-2021-MIDIS/PNADP-DE

VISTOS:

El Memorando N.° 486-2021-MIDIS/PNADP-UTI del 28 de junio de 2021, de la Unidad de Tecnologías de la Información; el Informe N.° 300-2021-MIDIS/PNADP-UTI-CSI del Coordinador de Sistemas de la Información; el Memorando N.° 879-2021-MIDIS/PNADP-UPPM de la Unidad de Planeamiento, Presupuesto y Modernización del 07 de julio de 2021; el Informe N.° 66-2021-MIDIS/PNADP-UPPM-CMG de la Coordinadora de Modernización de la Gestión; y el Informe N.° 229-2021-MIDIS/PNADP-UAJ del 07 de septiembre de 2021 de la Unidad de Asesoría Jurídica; y,

CONSIDERANDO:

Que, mediante el Decreto Supremo N.º 032-2005-PCM, modificado por el Decreto Supremo N.º 062-2005-PCM, el Decreto Supremo N.º 012-2012-MIDIS y el Decreto Supremo N.º 002-2021-MIDIS, se crea el Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", el cual tiene por finalidad ejecutar transferencias directas en beneficio de los hogares en condición de pobreza o pobreza extrema de acuerdo con el Sistema de Focalización de Hogares (SISFOH), priorizando progresivamente su intervención a nivel nacional;

Que, mediante Resolución Ministerial N.° 278-2017-MIDIS, se aprueba el Manual de Operaciones del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", el cual constituye el documento técnico normativo de gestión institucional, que determina la estructura orgánica, describe sus funciones generales, las funciones específicas de las unidades que lo integran, así como la descripción de los procesos estratégicos, misionales y de apoyo del Programa;

Que, en mérito de las normas antes señaladas, la Dirección Ejecutiva es la máxima autoridad ejecutiva y administrativa del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", teniendo entre sus funciones la emisión de Resoluciones de Dirección Ejecutiva en asuntos de su competencia;

Que, el artículo 20 del Manual de Operaciones dispone que "La Unidad de Tecnologías de la Información es responsable de planificar, ejecutar, monitorear y evaluar el desarrollo, implementación y mantenimiento de soluciones Tecnológicas de la Información (TI) en apoyo a las Unidades del Programa, para el cumplimiento de los objetivos y en el marco de las políticas y lineamientos del MIDIS y de la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros (PCM);

Que, mediante Decreto de Urgencia N.º 006-2020 se crea el Sistema Nacional de Transformación Digital, como un Sistema Funcional del Poder Ejecutivo, conformado por un conjunto de principios, normas, procedimientos, técnicas e instrumentos para organizar, entre otros, las actividades de la administración pública, a efectos de alcanzar los objetivos del país en materia de transformación digital; habiendo establecido en su Única Disposición Complementaria Derogatoria, que para todos sus efectos, el Sistema Nacional de Transformación Digital sustituye al Sistema Nacional de Informática;

Que, con Resolución Ministerial N.° 246-2007-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática, como una guía práctica para desarrollar estándares organizacionales de seguridad y practicas efectivas de la gestión de seguridad;

Que, mediante Resolución Ministerial N.° 004-2016-PCM se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática, la cual especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización, incluyendo requisitos genéricos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las necesidades de la organización;

Que, con Resolución Ministerial N.º 002-2021-MIDIS se aprueban los "Lineamientos N.° 001-2021-MIDIS "Lineamientos de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social", considerando dentro de su alcance a los Programas Sociales, con el objetivo de establecer lineamientos para implementar la seguridad de la información, que permita proteger los recursos de la información del MIDIS y los Programas Nacionales, y tecnologías utilizadas para su procesamiento, frente a amenazas, con el fin de minimizar los riesgos de daño y asegurar la confidencialidad, integridad y disponibilidad de la información;

Que, mediante Resolución de Dirección Ejecutiva N.° 113-2015-MIDIS/PNADP-DE del 30 de setiembre de 2015, se aprueba el Instructivo de buenas prácticas sobre servicios informáticos y otros documentos normativos;

Que, la Unidad de Tecnologías de la Información ha emitido el Memorando N.° 486-2021-MIDIS/PNADP-UTI del 28 de junio de 2021, que adjunta el Informe N.° 300-2021-MIDIS/PNADP-UTI-CSI del Coordinador de Sistemas de la Información, que contiene la propuesta del Manual "Buenas prácticas sobre servicios informáticos", sustentado su aprobación;

Que, mediante Memorando N.° 879-2021-MIDIS/PNADP-UPPM del 07 de julio de 2021, la Unidad de Planeamiento, Presupuesto y Modernización, hace suyo y remite el Informe N.° 66-2021-MIDIS/PNADP-UPPM-CMG de la Coordinadora de Modernización de la Gestión, concluyendo que la propuesta normativa se encuentra acorde a la implementación del Sistema Integrado de Gestión, se articula a las normas de control interno y al macro proceso 'Gestión de Sistemas y Tecnologías de Información', proceso de 'Gestión de Tecnologías de Información' y subproceso 'Gestión de Soporte a Usuarios Finales', emitiendo opinión favorable para su aprobación;

Que, con Informe N.° 229-2021-MIDIS/PNADP-UAJ del 07 de septiembre de 2021, la Unidad de Asesoría Jurídica estima viable la emisión de la Resolución de Dirección Ejecutiva que apruebe el Manual "Buenas prácticas sobre servicios informáticos" del Programa Juntos;

Con el visado de la Unidad de Tecnologías de la Información, la Unidad de Planeamiento, Presupuesto y Modernización, y la Unidad de Asesoría Jurídica;

De conformidad con lo dispuesto por el Decreto Supremo N.° 032-2005-PCM, modificado por el Decreto Supremo N.° 062-2005-PCM, el Decreto Supremo N.° 012-2012-MIDIS y el Decreto Supremo N.º 002-2021-MIDIS; la Resolución Ministerial N.° 002-2021-MIDIS; la Resolución Ministerial N.° 068-2020-MIDIS, y estando a lo establecido por el Manual de Operaciones del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS" aprobado por Resolución Ministerial N.° 278-2017-MIDIS;

SE RESUELVE:

Artículo 1.- Aprobar el Manual 'Buenas prácticas sobre servicios informáticos' del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", que en anexo forma parte integrante de la presente Resolución.

Artículo 2.- Dejar sin efecto el Instructivo de buenas prácticas sobre servicios informáticos, aprobado en el punto iii del Artículo 1 de la Resolución de Dirección Ejecutiva N.° 113-2015-MIDIS/PNADP-DE del 30 de septiembre de 2015.

Artículo 3.- Encargar a la Unidad de Tecnologías de la Información la implementación y socialización del documento aprobado en el artículo 1 de la presente Resolución, y que las Unidades del Programa realicen las acciones necesarias para la aplicación y cumplimiento del documento aprobado.

Artículo 4.- Disponer que la Unidad de Comunicación e Imagen publique la presente Resolución en el Portal de Transparencia Estándar y en el Portal Institucional del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS" (www.gob.pe/juntos), en el plazo de dos (02) días desde su emisión.

Regístrese y comuníquese.

PROGRAMA NACIONAL DE APOYO DIRECTO A LOS MÁS POBRES "JUNTOS"

Ministerio de Desarrollo e Inclusión Social

MANUAL

Buenas Prácticas sobre Servicios Informáticos

Elaborado por:	Revisado por:	Aprobado por:
Ángel Enrique Hinostroza Camarena **Coordinador de Tecnologías de la Información** Luis Gerardo Castro Lema **Oficial de Seguridad Digital**	Edwing Pinedo Añazgo Jefe de la Unidad de Tecnologías de la Información	Jéssica Cecilia Niño de Guzmán Esaine Directora Ejecutiva

1. Objetivo

Definir y establecer las indicaciones necesarias que permita a los/las usuarios/as del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", hacer uso correcto de los recursos informáticos y de comunicaciones de los que dispone la entidad, orientados a las buenas prácticas de Seguridad de la Información.

2. Alcance

Las disposiciones establecidas en el presente documento son de aplicación en todas las Unidades de la Sede Central y las Unidades Territoriales del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS".

3. Base legal

3.1. Ley N.° 28716, Ley de Control Interno de las Entidades del Estado.
3.2. Ley N.° 29792, Ley de creación, organización y funciones del Ministerio de Desarrollo e Inclusión Social.
3.3. Decreto Legislativo N.° 1412, que aprueba la Ley de Gobierno Digital.
3.4. Decreto Supremo N.º 032-2005-PCM por el que se crea el Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS", modificado por Decreto Supremo N.º 062-2005-PCM, Decreto Supremo N.º 012-2012-MIDIS y Decreto Supremo N.° 002-2021-MIDIS.
3.5. Resolución de Contraloría N.° 146-2019-CG, que aprueba la Directiva N° 006-2019-CG/INTEG "Implementación del Sistema de Control Interno en las Entidades del Estado" y modificatorias.
3.6. Resolución Ministerial N.º 246-2007-PCM "Aprueban uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información. 2ª. Edición" en las entidades integrantes del Sistema Nacional de Informática.
3.7. Resolución Ministerial N.° 04-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da Edición", en todas las entidades integrantes del Sistema nacional de Informática.
3.8. Resolución Ministerial N.° 278-2017-MIDIS, que aprueba el Manual de Operaciones del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS".
3.9. Resolución Ministerial N.° 002-2021-MIDIS, que aprueba los "Lineamientos de Seguridad de la Información del Ministerio de Desarrollo e Inclusión Social".
3.10. Resolución de Dirección Ejecutiva N.° 187-2019-MIDIS/PNADP-DE, que reconforma el Comité de Gobierno Digital del Programa Juntos.
3.11. Resolución de Dirección Ejecutiva N.° 065-2020-MIDIS/PNADP-DE, que aprueba el "Procedimiento para la atención de servicios informáticos del Programa Nacional de Apoyo Directo a los Más Pobres "JUNTOS".
3.12. Resolución de Dirección Ejecutiva N° 081-2021-MIDIS/PNADP-DE, que designa al Oficial de Seguridad Digital del Programa Juntos.

4. Siglas y definiciones

4.1. Activo de Información: Se refiere a todo lo que tiene un valor para el Programa en cuanto a la información, hardware y software, servicios relacionados para la transmisión de datos y los/as servidores/as que están relacionados a su control.

4.2. Centro de Datos: Denominado también Centro de Procesamiento de Datos - CPD (en inglés: data center o data centre), es el espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización.
4.3. CTI: Coordinación de Tecnologías de la Información.
4.4. Dispositivo de almacenamiento: Instrumentos utilizados para contener y respaldar información, los cuales pueden ser transportados por un usuario o se encuentran formando parte de los equipos servidores institucionales.
4.5. Equipos de comunicación: Dispositivos que permiten el acceso a la red, permiten la conectividad a los distintos sistemas institucionales, protegen el sistema de correos o la conectividad de la red de JUNTOS a la red de internet.
4.6. Equipos de red: Todo dispositivo que intercambia información por medio de una red de datos sea este cableado o inalámbrica.
4.7. Equipos Informáticos: En el presente documento se entenderá como equipo informático a todo dispositivo utilizado en su mayoría por los usuarios finales, tales como computadoras, escáneres, impresoras, entre otros.
4.8. FTP (Protocolo de Transferencia de Archivos): Medio por el cual un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.
4.9. GI: Gestor de Información
4.10. Página Web: Documento que se despliega al entrar a la internet. Puede contener archivos de texto, imágenes, videos, entre otros o redireccionar a otro documento(s).
4.11. Recursos Informáticos: Se entenderá como cualquier aplicación, herramienta, componente o dispositivo que se puede agregar a una computadora o sistema; por lo tanto, puede ser un recurso de hardware como de software.
4.12. Seguridad de la Información: Conjunto de medidas que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.
4.13. Sistema de Mesa de ayuda: Aplicativo informático que permite la gestión de incidentes de TI.
4.14. Soportes removibles: Son dispositivos que contienen información y que pueden instalarse o retirarse de un equipo.
4.15. SPAM: Se llama a los mensajes electrónicos no solicitados y que se envían a una gran cantidad de recipientes.
4.16. Usuario: Persona que hace uso de los recursos informáticos del Programa JUNTOS, teniendo para tal efecto credenciales para el acceso a los sistemas informáticos o de red.
4.17. UTI: Unidad de Tecnologías de la Información.

5. Disposiciones

5.1. Disposiciones Generales

5.1.1. La Unidad de Tecnologías de la Información revisa de manera periódica el cumplimiento del presente manual, y emite las alertas necesarias para las correcciones que sean pertinentes para el uso del equipamiento informático y de comunicación.
5.1.2. La Unidad de Tecnologías de la Información, realiza el control de las claves a las diferentes plataformas del Programa Juntos.
5.1.3. El Oficial de Seguridad Digital vela por el cumplimiento del presente manual, así como de gestionar las incidencias y/o vulnerabilidades relacionadas a la seguridad de la información.

5.1.4. El usuario es responsable del cumplimiento de todas las medidas estipuladas en el presente documento y de informar sobre cualquier incidencia o vulnerabilidad identificada a través de los mecanismos establecidos.

5.1.5. La Unidad de Administración brinda el soporte para realizar la disposición de equipos en desuso.

5.1.6. Todos los bienes informáticos y de comunicaciones que son asignados por la entidad deben ser cuidados y utilizados de manera correcta.

5.2. Disposiciones Específicas

5.2.1. Uso de Correo Electrónico

5.2.1.1. El usuario debe revisar y depurar los correos electrónicos almacenados en las carpetas no deseados, spam o papelera de reciclaje a fin de liberar espacio en su casilla de correo.

5.2.1.2. El contenido, manejo y reserva de la información del buzón de correo, es de responsabilidad exclusiva del usuario de la cuenta; debe realizar el cambio de su contraseña de correo con una frecuencia máxima de noventa (90) días calendario.

5.2.1.3. El usuario debe comunicar a la UTI, sobre la recepción de mensajes inusuales internos o externos, a fin de que tome las medidas correctivas del caso.

5.2.1.4. No se permite a los usuarios facilitar y/u ofrecer su cuenta y contraseña de correo a cualquier otra persona, ni el uso inadecuado del mismo. Si la UTI detecta el uso indebido del servicio de correo electrónico, bloqueará la cuenta del usuario como medida preventiva, por un periodo de treinta (30) días calendario. Si se comprueba que la falta es grave, se anulará definitivamente, sin perjuicio de las sanciones correspondientes.

5.2.1.5. El usuario debe depurar los correos antiguos y que no son necesarios almacenarlos, a fin de liberar espacio de su casilla de correo.

5.2.1.6. En ese sentido, sobre el buzón de entrada de los correos electrónicos, los usuarios deben discriminar la información relevante de la que no lo es, a fin de no saturar dicho buzón, y de ser el caso, retirarlos del servidor de correo y respaldarlos en archivos con extensión pst (el apoyo en esta actividad lo pueden solicitar al equipo de Soporte Técnico y Helpdesk). Considerar que dichas actividades favorecen al buen funcionamiento del servidor de correos y del cliente Outlook.

5.2.1.7. El usuario es responsable de la información transmitida o compartida a través de cualquier media asignado, como es el correo electrónico u otro medio de difusión empleado por el Programa.

5.2.1.8. El usuario debe activar la opción de fuera de oficina de su correo electrónico, cuando este se encuentre de vacaciones, descanso médico o licencia.

5.2.2. Uso de Servicios de Red, FTP, Internet

5.2.2.1. La UTI se hace cargo de restringir y controlar el uso de recursos por parte de los servidores, con potencial de invalidar los controles de los sistemas y software.

5.2.2.2. El usuario se encuentra prohibido de instalar o ejecutar programas no autorizados, que sean obtenidos a través de internet, correo electrónico u otro medio y/o instalar servidores y clientes de correo electrónico, GOPHERS o WWW, u otros que puedan utilizarse con fines no lícitos o no autorizados y dañinos tanto para el Programa como para sus propietarios.

5.2.2.3. En el caso que se necesite descargar archivos de ofimática o imágenes de la red o internet, éstos no deben ser mayores a 10 MB de tamaño, a fin de no generar congestión en la red. En caso se requiera la descarga de archivos de mayor capacidad se deberá comunicar a la UTI.

5.2.2.4. Los usuarios no están autorizados a conectar equipos de red ajenos al Programa, a los puntos de red de la entidad. De requerirse por razones de trabajo deberán ser autorizados por la Unidad donde labora mediante el formato correspondiente o en su defecto mediante correo remitido por el jefe de unidad ambos remitidos a la UTI, donde se evalúa la necesidad del acceso y se dará el VoBo de ser el caso.

5.2.2.5. Los usuarios no están autorizados a manipular los componentes de red, como gabinetes de comunicación, canaletas de cableado estructurado, cajas toma datos, Access Point, etc.; ni realizar extensiones de la red de datos, usando Switch, puntos de acceso inalámbrico u otro dispositivo sin la previa solicitud mediante formato de accesos o correo electrónico por parte de su Jefatura de Unidad y posterior validación y aprobación de la UTI.

5.2.2.6. Está prohibido conectar a la toma eléctrica estabilizada que son parte del Cableado Estructurado, equipos como cargadores de celulares, horno microondas, dispensadores, lustradoras, ventiladores, hervidores o cualquier otro equipo que no sea de uso informático.

5.2.2.7. El usuario se encuentra prohibido de decodificar el tráfico en la red o cualquier intento de obtención de información de correo confidencial u otro tipo de información que se transmita a través del mismo.

5.2.2.8. No está permitido colocar extensiones de tomas eléctricas por parte de los usuarios. En caso se requiera de puntos adicionales de toma corrientes deberá la Jefatura correspondiente solicitar dicha instalación a la Unidad de Administración para la evaluación correspondiente.

5.2.2.9. Los archivos o información a transferir por el servicio FTP deben ser de carácter estrictamente relacionado a las labores del trabajador y objetivos del Programa, y por lo tanto se encuentra prohibido el transferir o compartir archivos de contenido musical, lúdico, o de cualquier otra índole ajena a las labores del Programa.

5.2.2.10. De encontrarse archivos de las características no permitidas en el punto anterior, la UTI procederá de oficio la eliminación de dichos archivos.

5.2.2.11. Cada unidad de JUNTOS cuenta con carpetas compartidas, las cuales son de uso exclusivo de los colaboradores integrantes de cada unidad conforme al perfil de acceso solicitado por su Jefatura, por lo que se recomienda almacenar en ellas la información sensible a sus labores desarrolladas.

5.2.2.12. El uso de servicio de internet es exclusivamente para el desarrollo de las actividades y consecución de fines del programa; en ese sentido, si se requiere acceso a alguna página web restringida por encontrarse en una categoría no permitida, deberá contar con la autorización de la Jefatura pertinente, mediante formato o correo remitido por ella.

5.2.3. Uso de Código Telefónico

5.2.3.1. El código telefónico es de uso personal y exclusivo del usuario asignado, por lo tanto, no puede dar a conocer este código ni ser usada por otros trabajadores o terceros. Se considera mal uso del código telefónico, realizar llamadas de propósito personal, comercial, financiero o lúdico, ajeno al Programa JUNTOS.

5.2.3.2. Para el cambio del código telefónico, el usuario debe enviar su requerimiento vía correo electrónico al área de soporte técnico de la UTI, esta debe ser reemplazada y comunicada personalmente, o caso particular remitido por correo electrónico al usuario solicitante.

5.2.4. Uso de los equipos informáticos

5.2.4.1. Antes de insertar un dispositivo de almacenamiento externo (USB, disco externo u otros) a una PC, deberá revisarse a través del Sistema de Antivirus Corporativo instalado en la PC a fin de evitar contagio de virus y su propagación en la red.

5.2.4.2. El usuario está prohibido de abrir los equipos informáticos, cambiar componentes, alterar o eliminar software instalado por el Programa JUNTOS.

5.2.4.3. En caso de interrupción de fluido eléctrico el usuario deberá desenchufar el cable alimentador de energía a fin de evitar descargas que dañen física o lógicamente el equipo. Restablecido el fluido eléctrico, esperar aproximadamente 5 minutos para encender los equipos.

5.2.4.4. Antes de salir de refrigerio, retirarse temporalmente de su estación de trabajo, el usuario deberá realizar lo siguiente:

a) Bloquear el equipo para impedir el acceso de otros usuarios.

b) Poner el equipo en estado “Hibernar” o “Suspender” a fin de cumplir con los lineamientos de austeridad y racionalidad, y protección del medio ambiente.

5.2.4.5. Al culminar las labores diarias el usuario deberá apagar adecuadamente el equipo de cómputo y demás equipos asignados, a fin de evitar pérdida de información o que se dañe el sistema operativo.

5.2.4.6. Se encuentra prohibido acceder a páginas web no relacionadas con las actividades laborales (redes sociales, mensajería instantánea, salas de chat, páginas pornográficas, juegos, programas musicales, deportes, películas, etc.). Para el caso de acceso a redes sociales, se podrá gestionar eventualmente el acceso solo a personal autorizado mediante los formatos de acceso a los servicios informáticos establecidos por la UTI y remitidos por el sistema Mesa de Ayuda. El documento referido debe contener la justificación resumida y debe estar firmado por el Jefe de Unidad.

5.2.4.7. Si el usuario encuentra alguna irregularidad en los equipos de cómputo, recursos o servicios informáticos, debe comunicarlo inmediatamente al Gestor de Información de su Unidad Territorial o la UTI, a fin de que se adopten las acciones necesarias para regularizar su estado y operatividad.

5.2.4.8. Cada usuario que haga uso de los sistemas a los que se le ha dado acceso, se hará responsable de la información que se manipule durante su uso.

5.2.4.9. Los usuarios no deben compartir credenciales de ningún sistema, bajo responsabilidad conforme al numeral precedente.

5.2.4.10. Cada usuario debe contar con los accesos a los sistemas propios de su labor, lo cual debe ser solicitado por el Jefe de área.

5.2.4.11. El usuario será responsable de la información de la entidad que se encuentre en los equipos informáticos y de comunicaciones, asignados a su persona para el desarrollo de sus actividades, por lo que deberá realizar periódicamente copia de seguridad de la información más importante o crítica en medios externos para salvaguardar la información en caso de robo o pérdida de información.

5.2.4.12. En caso se encuentre o detecte que un usuario está haciendo mal uso de los equipos y recursos informáticos o maltratando estos equipos, será sujeto de las sanciones disciplinarias que correspondan conforme a la normativa aplicable. De igual manera, en los casos que se encuentre que el usuario esté haciendo mal uso de los sistemas informáticos, la Unidad de Tecnologías de la Información podrá bloquear el uso de los programas o aplicaciones identificadas, y se comunicará el hecho al Jefe de Unidad correspondiente.

5.2.4.13. Ningún usuario puede utilizar o distribuir software no autorizado en los equipos de cómputo o la red del Programa, debido a que éste podría

poner en riesgo la integridad y la seguridad de las computadoras y servidores del Programa.

5.2.4.14. En caso la UTI detecte o encuentre software no autorizado, o software no licenciado, en alguna computadora de la institución, procederá de oficio con la desinstalación, para luego comunicar a la Jefatura correspondiente del hecho indicado.

5.2.4.15. El personal designado por la UTI debe respetar la confidencialidad de los accesos de otros trabajadores de la entidad, así como garantizar la confidencialidad e integridad de los datos publicados y obtenidos.

5.2.4.16. Cuando el usuario traslade un equipo informático debe tener los cuidados necesarios para que la información contenida en él no se pierda o deteriore. Las acciones pertinentes que debe desarrollar el servidor para dicho fin son, entre otras:

- Emplear micas y archiveros para proteger los documentos físicos.
- Emplear cajas para proteger los activos de información, ya sean documentos, computadoras, impresoras, equipos móviles, entre otros.
- Tomar inventario de los activos de información a trasladar.

5.2.4.17. Todas las unidades del Programa, deben resguardar y hacer uso adecuado de los activos de información, en coordinación con las unidades responsables de la aplicación de controles de seguridad correspondientes.

5.2.4.18. Los usuarios deben tratar la información y los activos de información asociados, estrictamente para los fines y objetivos definidos por el MIDIS.

5.2.4.19. Los usuarios deben cumplir con el cuidado de los equipos y recursos informáticos del Programa. En caso se presente algún daño o incidente que afecte la integridad de las mismas se adoptará las medidas pertinentes. Asimismo, el usuario es responsable del uso adecuado de los recursos informáticos que le son asignados.

5.2.4.20. Los usuarios deberán de tomar las medidas del caso al momento del traslado de sus equipos informáticos asignados, a fin de que terceros no puedan acceder a la información contenida en ellos.

5.2.4.21. Los usuarios no podrán instalar ningún software o aplicativo en los equipos informáticos asignados toda instalación debe de ser coordinada con la UTI.

5.2.5. Uso de dispositivos móviles

5.2.5.1. La UTI, o personal asignado, realiza la configuración de los equipos móviles asignados a los usuarios. Los usuarios no deberán instalar aplicaciones que no estén relacionados con sus funciones.

5.2.5.2. Los usuarios a los cuales se les asigne un dispositivo móvil, son responsables de su custodia, cuidado y uso adecuado; así mismo, debe salvaguardar la información almacenada en dicho dispositivo y realizar un uso adecuado de este.

5.2.5.3. El acceso al dispositivo deberá de estar protegido con las medidas de seguridad necesarias para evitar el acceso de terceros a la información contenida en el dispositivo, tales como; pin de seguridad, huella dactilar, reconocimiento facial, entre otros.

5.2.5.4. Los usuarios no podrán divulgar la información sensible a la que tengan acceso a través de los aplicativos o archivos en sus equipos móviles, bajo responsabilidad.

5.2.5.5. Se debe realizar copias de seguridad de los archivos o información almacenada en sus equipos, para afrontar casos de pérdida o deterioro del mismo.

5.2.5.6. No se podrá asignar dispositivos móviles a personal tercero o externo al Programa, tal como lo dispone los Lineamientos de Seguridad de la Información.

5.2.5.7. Evitar acceder a enlaces de dudosa procedencia o a sitios no seguros desde sus dispositivos a fin de no afectar la seguridad del equipo.

5.2.5.8. De presentarse alguna falla o daño, el dispositivo no deberá ser manipulado por el usuario ni por terceros, deberá comunicarse con mesa de ayuda de la UTI o el Gestor de Información para que le indiquen las acciones a realizar.

5.2.5.9. En caso de pérdida o robo, el usuario deberá alertar inmediatamente al personal a cargo de Control Patrimonial de la Sede Central o la UT, así como a la mesa de ayuda de la UTI, a fin de realizar las acciones correspondientes que permitan salvaguardar la información contenida en el dispositivo.

5.2.6. Uso de impresoras

5.2.6.1. Evitar manipular las partes de la impresora cuando ésta se encuentre imprimiendo. De ocurrir atasco de papel, deberá comunicar de inmediato al personal de Mesa de Ayuda de la UTI o Gestor de Información en caso de la Unidad Territorial. No deberá jalar ni arrancar el papel.

5.2.6.2. Se deberá mantener el cuidado respectivo, en el sentido que se debe evitar que en sus partes internas se queden papeles de anotaciones, clips, residuos de grapas, tinta de corrector líquido, etc. en el momento de escaneos o fotocopiado. Asimismo, la impresora debe permanecer apagada y sin papel (el cual debe ser guardado en su paquete original), en caso no sea utilizada en un largo periodo, como por ejemplo los fines de semana.

5.2.6.3. En caso de interrupción de fluido eléctrico el usuario a cargo deberá desenchufar el cable alimentador de energía a fin de evitar descargas que dañen física o lógicamente el equipo. Restablecido el fluido eléctrico, esperar aproximadamente 5 minutos para encender los equipos.

5.2.6.4. En caso de pérdida o robo debe informar a la Unidad de Administración (UA) y a la Unidad de Tecnologías de la Información (UTI). En el caso el traslado sea fuera de la institución deberá coordinarlo con el personal a cargo de Control Patrimonial.

5.2.6.5. El usuario no debe dejar documentos que contienen información sensible, sea esta interna o confidencial, en las impresoras o fotocopiadoras.

5.2.6.6. En caso se imprima hojas que no son necesarias, deberán desecharse con la característica que la información que contienen no sea legible o recuperable.

5.2.7. Disposición de los soportes removibles

5.2.7.1. El Programa JUNTOS dispone de distintos soportes removibles: discos duros internos, discos duros externos, discos compactos, cintas de respaldo, teléfonos celulares, los cuales son usados por los distintos servidores del programa en sus diferentes actividades.

5.2.7.2. Los referidos dispositivos almacenan información de distintos tipos y niveles de necesidad, en ese sentido corresponde al usuario que lo emplea o administra calificar dicha información, teniendo en cuenta su criticidad.

5.2.7.3. Cuando los soportes removibles ya no son requeridos ya sea por cumplir su vida útil desaparece la necesidad para utilizarlos, se ha completado la capacidad de almacenamiento, o requiere ser reemplazado, se realizan las siguientes tareas:

a) Cuando cumple su vida útil, sea por reemplazo o inoperatividad, el soporte removible es desechado previa eliminación de toda la información contenida en él, a fin de que no pueda ser recuperada por terceros.

b) Cuando desaparece la necesidad para utilizarlo, se realiza la eliminación de toda la información contenida y se resguarda hasta que se requiera el uso nuevamente.

c) Cuando se ha completado la capacidad de almacenamiento, el soporte removible es reemplazado por otro de similar característica. Para el caso de cintas de respaldo se remite para su respectivo resguardo con la empresa contratada para tal fin.

d) Cuando requiere ser reemplazado, se realiza el respaldo de la información del soporte a reemplazar y se traslada al nuevo, para luego eliminar toda información del soporte reemplazado y proceder a desecharlo.

5.2.8. Inicio de sesión segura

5.2.8.1. Los usuarios deben acceder a los sistemas o plataformas del programa a través de los medios autorizados.

5.2.8.2. Los usuarios deben poseer credenciales para acceder a los sistemas institucionales, los cuales son brindados por la UTI previa solicitud de la Jefatura correspondiente según sea el caso.

5.2.8.3. El usuario debe considerar como contraseña las siguientes reglas:

a) No tener menos de ocho (8) caracteres; se recomienda que tenga al menos un carácter numérico y uno alfabético, combinar números y letras (en mayúscula y minúscula).

b) No tener más de tres caracteres consecutivos iguales, en cualquier posición, a los de una clave usada anteriormente.

c) Una contraseña ya utilizada no puede ser usada hasta después de por lo menos cinco (05) cambios.

5.2.8.4. La solicitud de accesos informáticos es realizada mediante los formatos de Solicitud de Acceso a los Servicios Informáticos – Usuario Interno (PNADP-UTI-GTI-F-001) o Solicitud de Acceso a los Servicios Informáticos – Usuario Externo (PNADP-UTI-GTI-F-002), establecidos en el Procedimiento para la atención de servicios informáticos.

5.2.8.5. Los accesos a los sistemas o plataformas del programa se brindan según la Tabla 01: Perfiles para el acceso a los servicios informáticos, establecidos en el Procedimiento para la atención de servicios informáticos.

5.2.8.6. El usuario a quien se le crea recientemente sus credenciales, deberá cambiar las contraseñas de cada sistema periódicamente.

5.2.8.7. La persona que no tenga credenciales de autentificación de JUNTOS, no podrá hacer uso de ningún sistema, ni usar las computadoras institucionales. En ese sentido, no tiene acceso a ningún servicio del programa.

5.2.8.8. Solo se podrá acceder a los sistemas institucionales con las credenciales de autentificación brindadas por la UTI y se harán desde una computadora institucional o desde una fuera de la sede, pero contando con la autorización del caso.

5.2.8.9. Solo se podrá acceder desde fuera de la red de JUNTOS a algunos sistemas, principalmente los que se encuentran vía WEB, pero con las credenciales autorizadas.

5.2.9. Uso de Escritorios y pantallas limpias

5.2.9.1. El usuario no debe mantener papeles en el escritorio ni adheridos en pantallas de los equipos que revelen información confidencial, de acuerdo con la clasificación de la información establecida en la Directiva del proceso de Gestión Documental.

5.2.9.2. En caso que el usuario deje su puesto de trabajo o se encuentre en cualquier otro lugar por un tiempo prolongado, no debe dejar documentos sobre el escritorio que puedan ser hurtados o analizados por personas no autorizadas.

5.2.9.3. El usuario no debe dejar el computador, equipo de escritorio o máquina virtual sin bloqueo de pantalla protegido por una contraseña al retirarse de su escritorio por cualquier motivo.

5.2.9.4. La Unidad de Tecnologías de la información velará porque las estaciones de trabajo y equipos portátiles tengan aplicado protector de pantalla, que se active de forma automática ante un período de inactividad. Para acceder nuevamente a la información del computador asignado se debe exigir una clave.

5.2.9.5. El usuario debe resguardar la información contenida en archivos físicos, la cual debe guardarse bajo llave cuando no se está utilizando.

5.2.9.6. El usuario debe tomar las medidas necesarias para impedir el acceso de terceros no autorizados a información Interna y Confidencial; así como información relacionada con su trabajo.

5.2.9.7. Las pantallas del computador, debe tener los iconos básicos y/o necesarios. Se recomienda no colocar como iconos de acceso rápido documentación o carpetas que contengan información sensible.

5.2.9.8. El usuario luego del uso de salas de reuniones u otros espacios donde se ejecuten reuniones de trabajo, debe dejar limpio todo el material utilizado, una vez finalizado el uso de las mismas. Esto incluye el borrar el pizarrón y/o eliminar el material escrito que se haya usado. Junto con lo anterior, cualquier equipamiento, propiedad del Programa que haya sido utilizado en la sala debe ser devuelto a su lugar de origen.

5.2.9.9. Los equipos informáticos utilizados en reuniones no deben contener información de los temas de las reuniones en las pantallas de los mismos, en ese sentido si se copian archivos en ellos para su fácil acceso se deben borrar finalizada la reunión. Recordar que los equipos de reuniones tienen esa finalidad y son empleados por diversos colaboradores e inclusive por personal externo que colabora con los objetivos institucionales en compañía de colaboradores de JUNTOS.

5.2.10. Transferencia de información

5.2.10.1. La transferencia de información puede ser de manera interna o externa.

5.2.10.2. En el caso interno, la transferencia de información se puede realizar a través de los servidores de archivos (file server) mediante carpetas compartidas o a través de los correos electrónicos hasta 10MB. En ambos casos, se debe contar con las credenciales de acceso para poder realizarla. En el caso en que la información a transferir se requiera realizar entre las distintas sedes con el Centro de Datos del Programa JUNTOS, se deberá realizar por ftp a través de los enlaces de datos que interconectan estas sedes.

5.2.10.3. En el caso externo, la transferencia de información puede realizarse por correo electrónico hasta 10 MB, FTP seguro o conexión VPN, los cuales para el acceso se utilizan credenciales y perfiles determinados: lectura o escritura y previa autorización de la UTI.

5.2.10.4. El uso de los servicios de almacenamiento en la nube, así como los programas de transferencia de archivos están restringidos, pues se desconoce la accesibilidad que terceros puedan tener a ellos. En caso se requiera su uso, deberá contarse con la autorización de la Jefatura de la Unidad correspondiente, bajo responsabilidad y solicitarse a la UTI para habilitar el acceso cuando no se haya podido realizar por las otras formas anteriores indicadas.

5.2.11. Sobre Seguridad de la Información

5.2.11.1. El usuario será responsable de la información de la entidad que se encuentre en los equipos informáticos y de comunicaciones como: CPU, Tablet, Laptop y Celular, asignados a su persona para el desarrollo de sus actividades, por lo que deberá velar tanto por su seguridad como por su adecuado uso.

5.2.11.2. El tratamiento de la información, y el uso de los dispositivos asignados para ello, será estrictamente para los fines definidos por el programa.

5.2.11.3. En general, los usuarios no deberán dar acceso a otros a ninguno de los recursos informáticos asignados a su persona.

5.2.11.4. Los usuarios no deben intentar descifrar los controles criptográficos establecidos para el control de la información o acceder a la información protegida sin la autorización respectiva.

5.2.11.5. Cualquier incidente de seguridad de la información detectado, deberá ser informado a Mesa de Ayuda, mediante el aplicativo o correo electrónico, a fin de que la UTI pueda realizar las acciones necesarias.

5.2.11.6. Cuando un usuario va hacer uso de sus vacaciones, descanso médico o licencia, el usuario debe comunicar al Gestor de Información o UTI para que se proceda a bloquear los accesos a los sistemas de información que utiliza. En caso el usuario no lo realice, podrá ser desactivada por la UTI a solicitud del jefe de Unidad o la Unidad de Recursos Humanos.

5.2.11.7. Queda prohibido bajo responsabilidad del usuario la comunicación a otros usuarios, de las contraseñas y accesos que utiliza para sus labores en la entidad.

5.2.12. Copias de Respaldo de Información

5.2.12.1. Toda la información almacenada en las carpetas compartidas de las unidades es respaldada por la UTI, mas no la contenida en los equipos de los usuarios.

5.2.12.2. El usuario deberá realizar periódicamente copia de seguridad de la información más importante o crítica en medios externos para salvaguardar la información en caso de robo o pérdida de información.

5.2.12.3. Para realizar las copias de seguridad de información en un medio externo como DVD, desde la CPU o Laptop asignado se debe seguir los pasos indicados en el Anexo 01: Pasos a seguir para realizar copias de seguridad de información en DVD.

5.2.12.4. Si la información de la entidad que desea salvaguardar no es factible copiar en DVD, podrá copiar la información crítica en las carpetas compartidas de su unidad al cual tiene acceso o deberá solicitar a la UTI en caso no hubiese uno disponible. Queda prohibido copiar información como música, video o cualquier otra que no sea de interés para la entidad.

6. Control de Cambios

Versión	Fecha	Justificación	Textos Modificados	Responsable
01	28/06/2021	Versión Inicial		UTI

7. Formatos

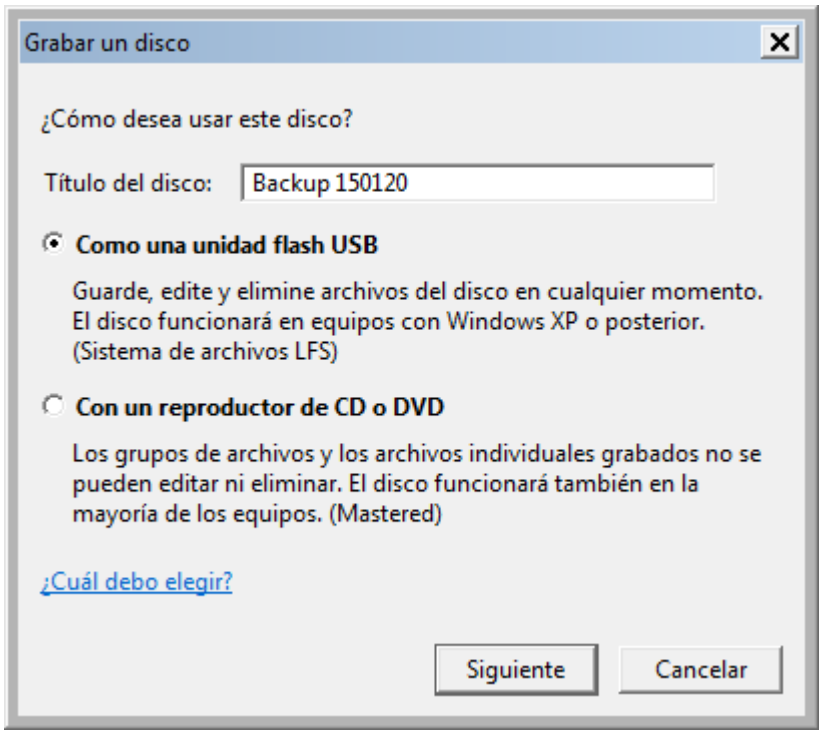
- Ninguno

8. Anexo

- Anexo 01: Pasos a seguir para realizar copias de seguridad de información en DVD

Anexo 01: PASOS A SEGUIR PARA OBTENER COPIAS DE SEGURIDAD EN DVD

1. Cargar el explorador de Windows
2. Insertar un DVD o CD vacío.
3. Dar click con el mouse en la Unidad de DVD RW
4. Ingresar el título del disco. Ej. Backup 150120



5. Dar click en siguiente
6. Seleccionar la información a realizar copia de seguridad y pegar en la Unidad de DVD RW.
7. Luego que termina de copiarse la información y mostrarse en el DVD, puede proceder a retirar el DVD.