INSTRUCCIONES DE LA DIRECCIÓN GENERAL DE RELACIONES CON LA ADMINISTRACIÓN DE JUSTICIA RELATIVAS A LA IMPLANTACIÓN CON CARÁCTER TEMPORAL DE LA PRESTACIÓN DE TRABAJO MEDIANTE LA MODALIDAD DE "TELETRABAJO" EN EL ÁMBITO DE LA ADMINISTRACIÓN DE JUSTICIA EN LA COMUNIDAD AUTÓNOMA DE CANARIAS DURANTE LA VIGENCIA DEL ESTADO DE ALARMA Y DURANTE EL PERIODO DE REACTIVACIÓN MOTIVADO POR EL COVID-19.

Las autoridades gubernativas y sanitarias de todos los países afectados por la pandemia mundial originada por el COVID-19 han dictado medidas preventivas y de salud pública, así como de carácter laboral y económico para paliar los graves efectos en la economía general y en la salud de la población de dicha pandemia, planteando el teletrabajo y la flexibilidad del horario de trabajo como alternativas u opciones razonables de contención de las posibilidades de propagación del virus en el marco de las relaciones de trabajo.

En el ámbito de la prestación de servicio en la Administración de Justicia en nuestro país, la prestación de los servicios esenciales fijados por el Consejo General del Poder Judicial durante la pandemia COVID-19 deben guiarse por las pautas y recomendaciones formuladas por la autoridad sanitaria, como competente para fijar las determinaciones sanitarias y de salud pública de interés general con motivo de las limitaciones de movilidad adoptadas durante el estado de alarma derivado de la crisis sanitaria. La autoridad sanitaria ha dictado la Orden SND/261/2020, de 19 de marzo, que encomienda al Ministro de Justicia la coordinación de la actividad profesional de los miembros de los cuerpos de funcionarios regulados en el Libro VI de la LO 6/1985, de 1 de julio, del Poder Judicial, en todo el territorio nacional.

En este contexto, la Resolución del Ministro de Justicia de 13 de abril de 2020 por la que se adapta la prestación del servicio público de Justicia al Real Decreto 487/2020, de 10 de abril, de aplicación a todo el territorio nacional, prevé la atención del servicio público de justicia a través de las siguientes modalidades:

- **Modalidad de trabajo presencial por turnos :** el personal contemplado en las dotaciones de personal fijadas en el ámbito de nuestra Comunidad Autónoma en virtud de la Resolución n.º 403 de 14 de abril de 2020 prestará el servicio público en un régimen de turno presencial en su centro de trabajo.

- **Modalidad de plena disponibilidad :** el personal al que no le corresponda por turno asistir a su puesto de trabajo puede ser requerido para la prestación del servicio que no pueda ser realizado a distancia o para cualquier incidencia que pudiera presentarse en relación con los servicios esenciales, para lo cual debe estar disponible y plenamente localizable por vía telefónica durante toda la jornada laboral.

- **Modalidad de teletrabajo :** el personal que disponga de dispositivos con accesos securizados a sistemas y aplicaciones de gestión procesal proporcionados por la administración prestacional, o que en su defecto pueda prestar voluntariamente el servicio en similares condiciones con dispositivos personales podrá realizar sus funciones desde su domicilio, previa solicitud y autorización por parte del Centro Directivo.

Estas modalidades de prestación del servicio deben atender la totalidad de las funciones ordinarias correspondientes al puesto de trabajo, en la medida en que lo permitan los medios materiales y humanos disponibles, dando preferencia a los servicios declarados esenciales, y sin perjuicio de las limitaciones impuestas por la suspensión de términos y la suspensión e

interrupción de los plazos procesales.

Por lo que respecta a la modalidad de teletrabajo, cuya implantación temporal debe realizarse en atención a las circunstancias concurrentes y a la excepcionalidad de la situación en la cual se encuentra el país y con el objetivo de minimizar al máximo los riesgos de contagio y de exposición del personal al servicio de la Administración de Justicia, procede regular aquellas actuaciones judiciales que en el momento actual, con los medios tecnológicos existentes son susceptibles de realización a través de dicha modalidad.

Dicha implantación, como se ha indicado, se realiza con carácter temporal durante la vigencia del estado de alarma y durante el periodo de reactivación motivado por el Covid-19, reduciendo los desplazamientos físicos del personal funcionario, sin perjuicio de que se proceda a su implantación definitiva fuera de la vigencia del estado de alarma, previa negociación con los sindicatos integrantes de la Mesa de Negociación del Sector Justicia.

En su virtud, esta Dirección General en cumplimiento de las competencias atribuidas por el artículo 90.1.h) del Decreto 382/2015, de 28 de diciembre, por el que se aprueba el Reglamento Orgánico de la extinta Consejería de Presidencia, Justicia e Igualdad, vigente en virtud de la Disposición transitoria primera del Decreto 203/2019, de 1 de agosto, por el que se determina la estructura central y periférica, así como las sedes de las Consejerías del Gobierno de Canarias, y previa negociación con las organizaciones sindicales integrantes de la Mesa Sectorial de Justicia de Canarias celebrada en la sesión del día 23 de abril de 2020,

RESUELVE

Primero.- Se implanta la modalidad de teletrabajo en el ámbito de la Administración de Justicia, de carácter voluntario y temporal durante la vigencia del Estado de Alarma y periodo de reactivación motivado por el COVID.19.

Para acogerse a la citada modalidad se deberá presentar solicitud a través del registro electrónico de la de la Consejería de Administraciones Púbicas, Justicia y Seguridad (https://sede.gobcan.es/apjs/cpji/menu_lateral/registro_electrónico), así como correo electrónico dirigido a la siguiente dirección: pmmlp.justicia@gobiernodecanarias.org (para el personal funcionario destinado en la provincia de Las Palmas) o pmmtfe.justicia@gobiernodecanarias.org (para los destinados en la provincia de Santa Cruz de Tenerife)..

El personal funcionario que preste su consentimiento a la modalidad de teletrabajo podrá, en cualquier momento, presentar solicitud para revocar dicho consentimiento a través de los mismos medios señalados para acogerse a dicha modalidad de prestación de trabajo, revocación que será considerada efectiva una vez que la Administración acuse recibo de la misma. En caso de revocación del consentimiento, si la Administración hubiera facilitado la herramienta informática quedará bajo custodia del personal teletrabajador hasta que se concrete con el mismo su retirada.

Segundo.- La persona que voluntariamente realice la modalidad de teletrabajo tendrá los mismos derechos (horario, jornada, descansos durante la jornada, retributivos, etc) y obligaciones existentes hasta la fecha y reconocidos al resto de personal funcionario que exclusivamente desempeñen sus funciones en régimen presencial y de disponibilidad, si bien se refuerza la obligación de confidencialidad y sigilo sobre toda la documentación e información

que por razón de su trabajo pueda manejar, dentro del entorno familiar o de terceras personas ajenas a su desempeño laboral, recordando la imposibilidad de traslado de expedientes judiciales fuera de las Sedes Judiciales a los domicilios del personal funcionario que se acoja a la Modalidad de teletrabajo.

Tercero.- El acceso seguro a la red corporativa requerirá disponer de un certificado VPN, usando el cliente de VPN Global Protect, lo que permitirá estar conectado a la red corporativa de forma segura. Una vez establecida la VPN podrá efectuarse una conexión vía Escritorio Remoto al PC del puesto de trabajo, desde el que podrá acceder a las aplicaciones corporativas, como por ejemplo Atlante, Inforeg, etc y demás aplicaciones a las que tiene acceso en su puesto de trabajo.

Los requisitos técnicos para el correcto funcionamiento del cliente Global Protect son los siguientes:
• Sistema Operativo:
- Windows 8.1 y Windows 10.
- Apple macOS versión 10.11 o posterior

• Para poder proveer el servicio de VPN, el PC desde donde se vaya a instalar y utilizar este software, deberá disponer de acceso a Internet, además de tener instalado un antivirus actual

Sin perjuicio de los cursos formación que se impartan a través del Instituto Canario de Administración Pública, a través de la pagina web https://www.gobiernodecanarias.org/administracionespublicas/cibercentro/conexionremota/documentacion/vpn/index.html se podrá acceder a manuales y videos de ayuda para la configuración de la vpn y la conexión remota.

Cuarto.- Teniendo en cuenta siempre la disponibilidad de medios técnicos, y especialmente de equipos informáticos, la Dirección General de Relaciones con la Administración de Justicia los facilitará al personal que lo precise y desee acogerse voluntariamente a la modalidad de teletrabajo. En este sentido, la Administración, teniendo en cuenta las circunstancias personales y familiares de la persona interesada, dará preferencia en la entrega de equipos a quienes se encuentren en situación de cumplimiento de un deber inexcusable por cuidado de hijos o personas mayores dependientes, así como con el personal considerado especialmente sensible, sin descartar a los funcionarios que se encuentren en plena disponibilidad que voluntariamente lo soliciten, para cuando no deban atender turnos de trabajo presencial.

Quinto.- Las actuaciones y puestos de trabajo susceptibles de realizar en la modalidad de teletrabajo son los siguientes:

1. Decanatos: funcionarios/as de los Cuerpos de GPA y TPA para funciones de registro y reparto.
2. Registro Civil : funcionarios/as de los Cuerpos de GPA y TPA (acceso a Inforeg, expedición de licencias de enterramiento, certificados de fe de vida, inscripción de nacimientos y defunciones etc).
3. Juzgados de Paz : Acceso a Inforeg, Expedición de licencias de enterramiento, certificados de fe de vida, inscripción de nacimientos y defunciones.
4. Funcionarios de los cuerpos de GPA y TPA adscritos a la Secretaría de Gobierno y Audiencias Provinciales para realizar funciones de registro y reparto de asuntos.

- El personal funcionario que se encuentre en situación de cumplimiento de un deber inexcusable por cuidado de hijos o personas mayores dependientes, así como el personal que haya solicitado la exención por ser trabajador/a considerado/a especialmente sensible prestará servicios a través de la modalidad de teletrabajo, cuando voluntariamente lo soliciten y cuando las circunstancias personales y técnicas lo permitan.

Asimismo, previo estudio y negociación con las organizaciones sindicales integrantes de la Mesa Sectorial de Justicia de Canarias, se podrán incluir nuevos puestos que se consideren que reúnen los requisitos para ser realizados mediante la modalidad de teletrabajo durante la vigencia del Estado de Alarma y durante el periodo de reactivación posterior motivado por el COVID-19.

Sexto.- En Anexo a las presentes instrucciones se establecen una serie de recomendaciones en materia de seguridad que deberán ser adoptadas durante la prestación de servicio en la modalidad de teletrabajo.

ANEXO

RECOMENDACIONES DE SEGURIDAD PARA LA PRESTACIÓN DE SERVICIO A TRAVÉS DE LA MODALIDAD DE TELETRABAJO EN EL ÁMBITO DE LA ADMINISTRACIÓN DE JUSTICIA EN LA COMUNIDAD AUTÓNOMA DE CANARIAS

1. Utilización de los servicios y herramientas corporativas

En la medida de lo posible, para el ejercicio de las tareas y actividades correspondientes a las funciones del puesto de trabajo, se deberán utilizar los recursos y las herramientas que la Administración Pública pone a disposición de sus usuarios.
El acceso remoto se articulará mediante una conexión VPN, que establecerá un canal de comunicación seguro entre el equipo que esté utilizando y la red de justicia. La Administración Pública de la Comunidad Autónoma de Canarias facilita los componentes necesarios, previa solicitud en el siguiente formulario de Sírvete: "Solicitud / Renovación VPN Empleado Público".
El ordenador personal, portátil o dispositivo móvil utilizado para el teletrabajo y el acceso remoto a los servicios y herramientas corporativas, estará bajo la custodia de la persona usuaria que los utilice, que deberá adoptar las medidas necesarias para evitar los accesos no autorizados a la información. Asimismo, con el fin de minimizar las amenazas de seguridad, estos equipos deberán mantenerse actualizados, en la medida de lo posible, tanto su sistema operativo como su antivirus.

2. Utilización de conexiones a Internet de confianza o conocidas

Con el fin de minimizar el riesgo de comprometer la seguridad de los sistemas corporativos, se evitará el uso de conexiones WiFi abiertas y redes públicas.
Como medida de seguridad, la conexión a través de una red WiFi de confianza se recomienda que esté protegida por una contraseña lo más compleja y larga posible y con una combinación de caracteres mayúsculas, minúsculas, números y símbolos.

3. Uso de Contraseñas y procedimientos de autenticación

Siempre que sea posible, se recomienda el acceso a los sistemas de información con certificado digital y la utilización de contraseñas robustas, basadas en caracteres especiales, números y letras en mayúsculas y minúsculas y, preferiblemente, evitando el uso de información que pueda ser inferida del conocimiento de la persona o de la organización a la que pertenece.
Las contraseñas corporativas deben mantenerse en secreto y no deben ser compartidas con ningún otro usuario y, en caso de que se le requiera para que comunique su contraseña o considere que ha quedado expuesta a personal no autorizado, se deberá poner en conocimiento del personal responsable, de forma que esta circunstancia pueda ser tratada como un incidente de seguridad.

4. Phishing

El phishing es un tipo de ciberdelito que consiste en la comunicación de mensajes fraudulentos enviados por correo electrónico, teléfono, SMS, WhatsApp, etc., mediante el cual un atacante, suplantando la identidad de un usuario o de una entidad fiable, contacta con una víctima de una forma aparentemente legítima, para tratar de que acceda a diversas peticiones:

- Proporcionar ciertos datos sensibles.
- Instalar una aplicación.
- Abrir un archivo adjunto.
- Acceder a un enlace.
- Realizar un pago, etc.

Es una de las estafas más utilizadas por los delincuentes informáticos y tiene como objetivo obtener datos de un usuario: claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc.

El funcionamiento del phishing es sencillo: se recibe un correo electrónico, con una apariencia legítima que pide actualizar, validar o confirmar información mediante un enlace. Tras pulsar en él, se redirige al usuario a una página web falsa, en la que se procede al robo de la contraseña u otros datos.

Para identificar un posible ataque de phishing, la Dirección General de Telecomunicaciones y Nuevas Tecnologías del Gobierno de Canarias recomienda las siguientes medidas:

- Detectar si en el correo o la llamada telefónica se solicita algún tipo de información sensible.
- Comprobar la dirección del correo electrónico, tanto el nombre del remitente como del dominio (parte de la dirección del correo electrónico que sigue a la "@").
- Buscar fallos gramaticales y tipográficos, y analizar si en el lenguaje usado se utiliza contenido emocional como miedo, curiosidad, avaricia, etc.
- Las llamadas telefónicas fraudulentas suelen provenir de números internacionales o de extensión larga.
- Algunos correos de phishing contienen enlaces a supuestas web oficiales donde se piden los datos a los usuarios, o ficheros adjuntos que puedan contener malware o código de explotación.
- A veces el ataque se inicia mediante una notificación de error o advertencia informática, mostrando un número de teléfono de una empresa de soporte, como Microsoft. En este sentido, se debe tener en cuenta que, en el Gobierno de Canarias, los problemas informáticos los gestiona CiberCentro o los servicios informáticos de cada Consejería o Área. Por lo que, ningún usuario debe ser contactado directamente por una empresa de servicios informáticos.

No se deben hacer clics en enlaces, ni descargar ningún documento adjunto de correos electrónicos sospechosos. Se sospechará de aquellos correos electrónicos o llamadas que pidan hacer actuaciones no habituales (solicitud de datos personales o credenciales, por ejemplo).

No se descargarán ficheros adjuntos procedentes de un correo con remitente desconocido. En la medida de lo posible, los datos adjuntos se descargarán

manualmente y se analizarán con una solución antivirus en primer lugar.
En caso de que sufra o detecte un ataque de phishing, se deberá comunicar el incidente de seguridad a CiberCentro a través de los canales habituales:

- Sírvete.
- Teléfono: 922 922 912 - 928 117 912.
- Correo electrónico: cibercentro@gobiernodecanarias.org.

5. Navegación segura por Internet

El ordenador personal, portátil o dispositivo móvil utilizado para el teletrabajo estará bajo la custodia de la persona usuaria que los utilice, que deberá adoptar una serie de medidas en relación con la navegación por Internet:

- Evitar la navegación por páginas no seguras.
- Evitar la instalación de cualquier software de contenido o procedencia dudosa o desconocida.
- Mantener actualizados los navegadores web (Internet Explorer, Google Chrome, …) con la última versión y parches de software disponibles.
- Eliminar periódicamente el historial de navegación, las cookies, las contraseñas recordadas y otros archivos temporales. Así se evitarán potenciales elementos espías.

6. Finalización de la jornada laboral

Al finalizar la jornada laboral, se cerrarán todas las conexiones a los sistemas de información, webs y servicios corporativos utilizados. La persona usuaria deberá bloquear su equipo personal, portátil o dispositivo móvil, a efectos de evitar su acceso a estos recursos por otras personas durante su ausencia.
Se deberá eliminar la información temporal generada, prestando especial atención a la carpeta de “Descargas”, a la “Papelera de reciclaje” y a la carpeta de “Mis Documentos”. La destrucción de documentación temporal en papel se deberá realizar de forma que se garantice que ningún dato sensible o protegido queda visible.
En la medida de lo posible, la documentación se generará a través de los recursos corporativos que proporciona la organización, evitando almacenar, en el equipo personal desde el que se teletrabaja, cualquier documentación o información sensible especialmente protegida.
Si fuera estrictamente necesario el uso de documentación en papel para la realización de las tareas, se deberán extremar las medidas de seguridad para su custodia, de forma que se evite el acceso no autorizado de la información contenida en ella.
Asimismo, se evitará almacenar información sensible, confidencial o protegida en medios desatendidos (tales como CDs, DVDs, memorias USB, etc.), así como dejar visible tal información en la pantalla del ordenador o en documentos impresos cuando no puedan estar custodiados por la persona usuaria.

7. Seguridad de los equipos

Para facilitar la movilidad, el modelo de teletrabajo actual utiliza en la mayoría de los

casos ordenadores portátiles, tablets, o dispositivos similares. No obstante, precisamente por el hecho de ser trasladables son más fáciles de perder, y susceptibles de ser sustraídos. Por ello deben tomarse precauciones concretas tales como:

- No dejar los equipos desatendidos, en coches (aunque no estén a la vista) y evitar sacarlos de casa si no es necesario.
- Si se trasladan entre el hogar y el trabajo, hacerlo con una funda o maletín que ofrezca una buena resistencia a caídas, golpes, aplastamientos o líquidos.
- En el lugar de teletrabajo, es recomendable ubicar el dispositivo en un espacio propio, donde se evite que pueda sufrir daños tales como derramamiento de líquidos, caídas, etcétera.
- El equipo será utilizado exclusivamente por el personal al que le sea asignado.
- Prestar atención al cableado, ya que evitará tropiezos que puedan terminar con la caída y/o rotura del equipo.
- Guardar el equipo en un lugar seguro que evite que quede al alcance de otras personas del hogar o de mascotas.

8. Protección de datos

Las plataformas e infraestructuras tecnológicas corporativas de la Administración Pública de la Comunidad Autónoma de Canarias garantizan la seguridad y la confidencialidad de los datos almacenados en ellas. En la Comunidad Autónoma de Canarias, el órgano competente en materia de tecnologías de la información y de las comunicaciones garantizará el cumplimiento de las medidas previstas en su política de seguridad y en la normativa vigente en materia de protección de datos de carácter personal.