RESOLUCIÓN DE LA DIRECTORA GENERAL DE ECONOMÍA DIGITAL E INNOVACIÓN, POR LA QUE SE ADOPTAN MEDIDAS EN LA EJECUCIÓN DE LAS POLÍTICAS DE SEGURIDAD DIGITAL PARA LA IMPLEMENTACIÓN DEL TELETRABAJO COMO CONSECUENCIA DE LA PANDEMIA DEL VIRUS COVID-19.

Vista la Resolución de 12 de marzo de 2020 de la Secretaría General para la Administración Pública por la que se adoptan medidas respecto a todo el personal la Administración de la Junta de Andalucía con motivo del COVID-19, y en atención a los siguientes,

ANTECEDENTES DE HECHO

Primero.- Con fecha 11 de marzo de 2020, el Director General de la Organización Mundial de la Salud declaró el brote del nuevo coronavirus 2019 (nCoV) como una Pandemia. En su declaración, el Comité de Emergencias instó a los países a estar preparados para contener la enfermedad pues todavía es posible interrumpir la propagación del virus, siempre que se adopten medidas firmes para detectar la enfermedad de manera precoz, aislar y tratar los casos, hacer seguimiento de los contactos y promover medidas de distanciamiento social acordes con el riesgo.

Segundo.- Con fecha 14 de marzo de 2020, es publicado el Real Decreto 463/2020, por el que se declara el estado de alarma para la gestión de la crisis sanitaria ocasionada por el COVID-19, y en el que se establecen limitaciones de la libertad de circulación de las personas, así como medidas de contención en diferentes ámbitos.

Tercero.- Con fecha 15 de marzo de 2020, el Consejero de la Presidencia, Administración Pública e Interior dicta Orden por la que se determinan los servicios esenciales de la Administración de la Junta de Andalucía con motivo de las medidas excepcionales adoptadas para contener el COVID-19, estableciendo con carácter general la modalidad no presencial para la prestación de servicios en el ámbito de la Administración General de la Junta de Andalucía y sus entidades instrumentales y consorcios adscritos, con la vigencia indicada en la misma Orden, esto es, del 16 al 30 de marzo de 2020, ambos inclusive, sin perjuicio de las prórrogas que se puedan acordar.

Cuarto.- En virtud del Decreto del Presidente 2/2019, de 21 de enero, de la Vicepresidencia y sobre reestructuración de Consejerías, y de acuerdo con el Decreto 104/2019, de 12 de febrero, por el que se regula la estructura orgánica de la Consejería de Economía, Conocimiento, Empresas y Universidad, a este Departamento le corresponden las competencias relativas a la dirección e impulso de la política de telecomunicaciones y seguridad de los sistemas de información de la Administración de la Junta de Andalucía y del sector público andaluz. En concreto, según el artículo 9.1.m) del Decreto 104/2019, de 12 de febrero, le corresponde la "Coordinación y ejecución de las políticas de seguridad de los sistemas de Información y telecomunicaciones de la Administración de la Junta de Andalucía."

Quinto.- El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, establece en su artículo 7, entre los principios básicos en materia de seguridad de la información, los de prevención, reacción y recuperación, fija los conceptos de "gestión de personal", "autorización y control de los accesos", "protección de información almacenada y en tránsito" y "prevención ante otros sistemas de información interconectados" entre los requisitos mínimos

(artículos 14, 16, 21 y 22) y establece directrices generales para el acceso remoto (medida op.acc.7, apartado 4.2.7, anexo II).

Sexto.- Ante la activación de la modalidad no presencial para la prestación de servicios en el ámbito de la Administración General de la Junta de Andalucía y sus entidades instrumentales y consorcios adscritos, resulta necesaria la definición de requisitos para la seguridad en los equipos de acceso, las conexiones a la red de la gestión de la información, el uso de las aplicaciones corporativas y otros aspectos, de forma que se minimice su vulnerabilidad frente a posibles ataques o errores de uso.

Por todo lo anterior, se hace necesario desarrollar medidas para la ejecución de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

FUNDAMENTOS DE DERECHO

Primero.- La Dirección General de Economía Digital e Innovación, es competente para dictar esta Resolución de conformidad con lo establecido en el artículo 9.1.m) del Decreto 104/2019, de 12 de febrero, por el que se regula la estructura orgánica de la Consejería de Economía, Conocimiento, Empresas y Universidad, en el que se le atribuyen facultades en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía.

Segundo.- Las directrices en materia de seguridad TIC en el ámbito de la Administración de la Junta de Andalucía, sus entidades instrumentales y los consorcios, a los que se refiere el artículo 12.3 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, se determinan en el Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía (modificado por el Decreto 70/2017, de 6 de junio).

Tercero.- Por su parte, la Orden de 9 de junio de 2016, por la que se efectúa el desarrollo de la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, articula el desarrollo de dicha política mediante resoluciones de la Dirección General competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones de la Administración de la Junta de Andalucía.

Cuarto.- Entre los ámbitos de desarrollo de la política de seguridad TIC que establece la Orden de 9 de junio de 2016 se encuentra el acceso y uso de aplicaciones corporativas, servicios de Internet y otros recursos de uso colectivo o individual, así como la protección lógica de equipos, electrónica de red, comunicaciones y servicios.

Vistos los antecedentes de hecho, los fundamentos de derecho, y demás normas de general aplicación y atendiendo a razones de interés público y de protección de la salud pública, esta Dirección General,

RESUELVE

Primero.- Ámbito de aplicación.

La presente Resolución será de aplicación a la Administración de la Junta de Andalucía y la totalidad de sus entidades instrumentales, así como a los Consorcios regulados en el artículo 12.3 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, todas ellas, entidades comprendidas en el ámbito de aplicación del Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía.

Segundo.- Requisitos de seguridad en los equipos de acceso.

- Con carácter general, todos los empleados que teletrabajen deberán utilizar equipos portátiles corporativos configurados para garantizar el cumplimiento de los criterios de seguridad que se exponen a continuación.
- En caso de que no haya suficientes equipos portátiles corporativos, se priorizará la asignación de éstos a usuarios que participen en la prestación de los servicios esenciales establecidos en el anexo de la Orden del Consejero de la Presidencia, Administración Pública e Interior de 15 de marzo de 2020.
- A criterio de las entidades, se podrán utilizar equipos de sobremesa corporativos, con las mismas características de seguridad que los portátiles, que serán retirados de las instalaciones bajo autorización escrita, y con compromiso de buen uso firmado por el usuario.
- Para el resto de usuarios, a criterio de las entidades y de forma extraordinaria, se podrán emplear equipos privados de éstos, siempre que cumplan una serie de requisitos mínimos y bajo declaración responsable de los usuarios indicando que se implantarán las medidas de seguridad indicadas por esta Resolución.
- En caso de que se usen equipos propios de los usuarios, se podrán emplear sobre los mismos sistemas operativos autoarrancables desarrollados por la Administración de la Junta de Andalucía.
- En cualquiera de los casos anteriores, las medidas de seguridad mínimas a aplicar en los equipos de acceso serán las siguientes:
    - Se instalarán y mantendrán actualizados, en el sistema operativo y en los programas de aplicación, los parches de seguridad distribuidos por el fabricante/desarrollador del producto.
    - Se instalará y mantendrá actualizado un sistema de protección frente a código malicioso (antivirus, por ejemplo).
    - Se vigilará el cumplimiento de la legislación en materia de propiedad intelectual, evitando la instalación y uso de programas sin la correspondiente licencia y la reproducción de contenidos sin autorización.
- Para equipos corporativos, adicionalmente, se aplicarán las siguientes medidas:
    - Se reducirá en lo posible la instalación de aplicaciones, limitándose a las estrictamente necesarias, y obteniéndolas siempre del fabricante original.
    - Se deshabilitarán los programas de sincronización con la nube que no sean corporativos.

- Se habilitará en los usuarios del equipo el nivel de acceso mínimo necesario, y solo se permitirán privilegios de administración de forma justificada.
- Se habilitará el bloqueo automático de la pantalla por inactividad, requiriendo contraseña para volver a la sesión.

- En caso de uso de equipos propios de los usuarios, se intentará que el acceso a los mismos para teletrabajo se haga con un usuario separado, específico para esa finalidad, protegido por contraseña, con bloqueo de sesión por inactividad y no accesible por el resto de usuarios de dicho equipo.

Tercero.- Requisitos de seguridad en las conexiones a la red de la entidad.

- La conexión del equipo de acceso a la red doméstica se realizará mediante cable de red preferiblemente.
- En caso de que se use red Wifi, ésta deberá disponer de autenticación y se evitará en lo posible el uso de redes públicas o abiertas, siendo preferible en este segundo caso, el uso de la conexión de datos del móvil corporativo, si se dispone del mismo.
- Para organismos integrados en RCJA, se configurará el acceso a través del APN corporativo en el uso de la conexión de datos móviles corporativa.
- Se utilizará una conexión de red privada virtual (VPN) con doble factor de autenticación para el acceso a la red de la entidad. En entidades integradas en RCJA, se usará el servicio corporativo de VPN.
- Una vez conectado el equipo de acceso a la red de la entidad, el acceso y uso de los recursos internos (almacenamiento de ficheros, aplicaciones, servicios de terminal y escritorio remoto, equipos de escritorio en su caso...) estará restringido y controlado, aplicándose el principio de mínimo privilegio.
- Si para mediar el acceso a la red de la entidad se usan servicios de terminal, escritorios remotos o pasarelas de salto, se habilitará en éstos la auditoría de accesos para facilitar la detección e investigación de posibles incidentes.

Cuarto.- Requisitos de seguridad en la gestión de la información.

- En general, se minimizará la salida de información corporativa de la red interna de la entidad. Si se debe trabajar con documentos, se preferirá que éstos residan en recursos de almacenamiento de la entidad.
- Si se requiere la creación de ficheros temporales con información corporativa en el equipo de acceso, se mantendrán en el mismo por el tiempo mínimo necesario y se borrarán cuando dejen de ser útiles.
- Se prohíbe el uso de servicios de almacenamiento y compartición de documentos no corporativos o no autorizados, y especialmente el uso de cuentas particulares en estos servicios para intercambiar información interna. Se usarán en su lugar herramientas corporativas como Consigna o Ficheros Junta.

Quinto.- Requisitos de seguridad en el uso de las aplicaciones corporativas.

- Sólo se habilitará el acceso a la aplicaciones corporativas estrictamente necesarias, usando segundo factor de autenticación si está disponible, y aplicando el principio de mínimo privilegio.

- Se verificará la correcta trazabilidad de las operaciones (usuarios individuales, auditoría de accesos...).

Sexto.- Detección y gestión de incidentes de seguridad.

- Las entidades mantendrán actualizado el listado de activos críticos de su organización en AndalucíaCERT, como medida preventiva ante los distintos escenarios que puedan surgir en la implantación de medidas excepcionales en el ámbito TIC, como puede ser un aumento en el número de usuarios en modalidad de teletrabajo.
- En cumplimiento de la Resolución de 13 de julio de 2018, de la Dirección General de Telecomunicaciones y Sociedad de la Información, por la que se establecen normas sobre gestión de incidentes de seguridad TIC, las entidades recordarán a sus usuarios la obligación de notificar los incidentes de seguridad que se detecten, y los canales establecidos para dicha notificación.

Séptimo.- Soporte a usuarios.

- Las entidades que dispongan de centro de atención a usuarios dimensionarán la capacidad del mismo para prever el incremento de consultas y peticiones y facilitarán el acceso para los empleados en acceso remoto.
- Dado que los usuarios aislados, trabajando en acceso remoto, pueden ser víctimas más fáciles para las técnicas de ingeniería social, se incrementará la alerta ante campañas de *phishing* que aprovechen situaciones excepcionales, y se mantendrá a los usuarios informados y preparados para notificar cualquier incidente que detecten.

Octavo.- Efectos.

La presente Resolución surtirá efectos desde el momento de su firma.

La Directora General de Economía Digital e Innovación.

Dª. Loreto del Valle Cebada

ANEXO I – Glosario

Equipo de acceso: dispositivo informático usado fuera del ámbito físico corporativo (equipo corporativo o propiedad del usuario) para conectar con la red del organismo.

VPN: Del inglés Virtual Private Network (Red Privada Virtual). Mecanismo que permite el establecimiento de una comunicación segura y flexible entre dos nodos, entre un nodo y una red o entre dos redes cuando dicha comunicación ha de atravesar un medio inseguro.

RCJA: Red Corporativa de Telecomunicaciones de la Junta de Andalucía.

APN: Del inglés Access Point Name (Nombre del Punto de Acceso). Pasarela que permite el acceso a Internet desde una red de datos móviles.