Código de conducta de la Administración presupuestaria en la utilización de los medios tecnológicos

La Oficina de Informática Presupuestaria (OIP) de la Intervención General de la Administración del Estado (IGAE) pone a disposición del personal destinado en los centros directivos de la Secretaría de Estado de Presupuestos y Gastos y de la IGAE, ámbito al que se hará referencia en este documento como "Administración presupuestaria", unos medios tecnológicos, que son instrumentos de trabajo propiedad de la Administración General del Estado para el desarrollo eficaz de las funciones encomendadas a dichos centros.

Estos medios tecnológicos, que son elementos básicos para la gestión encomendada a la Administración presupuestaria (AP), están constituidos por los sistemas de información y las bases de datos, los equipos informáticos de usuario, departamentales y corporativos (PC's, impresoras, servidores …), las infraestructuras de comunicaciones y de conexión a redes internas o externas, incluido el acceso a redes externas inseguras, la infraestructura de redes corporativas y los servicios telemáticos, el software y hardware en general, y los dispositivos de movilidad disponibles en cada momento.

Este documento tiene por objetivo establecer el código de conducta y la regulación de uso de tales medios, para:

- Garantizar la disponibilidad, integridad y confidencialidad de la información,
- Evitar usos indebidos que supongan infringir los derechos de propiedad intelectual o quebrantar otros procedimientos de seguridad establecidos en la Administración presupuestaria,
- Mantener la protección de datos personales, y
- Cumplir con las medidas establecidas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).

Todo ello con una doble finalidad:

1. Facilitar y agilizar la tramitación de los procedimientos y la utilización de los servicios mediante el uso de las tecnologías de la información y de las comunicaciones.
2. Proporcionar información completa, homogénea, actualizada y fiable.

Ambos propósitos aconsejan que el uso de los medios tecnológicos del ámbito de la Administración presupuestaria responda a criterios homogéneos y normalizados, y no dependa del libre arbitrio, discrecionalidad y buen criterio de los usuarios.

El ámbito subjetivo de aplicación de este código de conducta se extiende no solamente al personal del ámbito de la Administración Presupuestaria (AP) sino también a todos aquellos usuarios ajenos a dicho ámbito que accedan o utilicen los medios tecnológicos de la AP para el ejercicio de sus funciones. Todos ellos deberán observar y cumplir obligatoriamente los criterios, pautas y medidas establecidas en este

documento, aun cuando dejen de utilizar dichos recursos.

La AP y las personas que realizan su trabajo en el ámbito de su competencia reconocen que tienen conocimiento y asumen los compromisos, normas y procedimientos para el uso de los medios tecnológicos, adoptando todas las medidas que correspondan para su estricto cumplimiento, incluso cuando finalicen su relación laboral o las funciones que justifican la utilización de la AP.

Los distintos órganos del ámbito de la AP, directamente o a través de la Oficina de Informática Presupuestaria (OIP), podrán realizar las investigaciones, accesos y controles que resulten necesarios tanto de los equipos como de las herramientas facilitadas a los usuarios, incluyendo el correo electrónico corporativo, dentro del ámbito de potestades que corresponda. Todos los controles que se establezcan serán previamente aprobados por el Comité de coordinación de seguridad de la Información (CCSI) y serán debidamente publicados en este código de conducta para general conocimiento de su existencia.

Las finalidades de los controles o/y del acceso indicados son las siguientes:

- Protección del sistema, de la red informática y de los equipos que lo conforman, a fin de garantizar la integridad del sistema y la seguridad de la información.
- Asegurar la continuidad del trabajo en el caso de que el usuario se ausente por razones de enfermedad, vacaciones, u otras similares.
- Prevención de la responsabilidad de la AP frente a terceros.
- Comprobación de la existencia del uso residual y razonable de los medios tecnológicos facilitados por la AP para usos personales.

Los usuarios, que de forma reiterada, deliberada o por negligencia infrinjan los criterios, pautas y medidas establecidas en este código de conducta, quedarán sujetos a las actuaciones técnicas o disciplinarias que correspondan.

1. Definiciones a efectos de este código de conducta.

- Medios tecnológicos: los sistemas de información y las bases de datos, los equipos informáticos de usuario, departamentales y corporativos (PC's, impresoras, servidores, …), las infraestructuras de comunicaciones y de conexión a redes internas o externas, incluido el acceso a Internet, la infraestructura de redes y los servicios telemáticos, el software y hardware en general, y los dispositivos de movilidad disponibles en cada momento puestos a disposición de los usuarios de la AP.
- Código de conducta: conjunto de criterios, pautas y medidas a los que se somete la utilización de los medios tecnológicos destinados al cumplimiento de la función asignada a la AP.
- Administrador de sistemas: responsable de la gestión y administración de los sistemas informáticos bajo su responsabilidad, realizada de acuerdo con el código de conducta de la organización en la utilización de los medios tecnológicos.
- Responsable de seguridad de la información: es la/el Responsable de la Unidad de Seguridad de la Información en los términos observados en el apartado noveno de la Resolución de 21 de diciembre de 2015, de la Secretaría de Estado de Presupuestos y Gastos, por la que se regula la política de seguridad de los sistemas de información de la Secretaría de Estado de

Presupuestos y Gastos y de la Intervención General de la Administración del Estado.

- Usuario de la AP: empleados públicos del ámbito interno de la AP, personal colaborador y empleados públicos y otro personal ajeno a dicho ámbito, que tienen a su disposición o acceden a los medios tecnológicos de la AP, ya sea desarrollando tareas permanentes u ocasionales.

2. Objetivo

El presente documento tiene como objetivos:

- Concienciar a los usuarios sobre las normas de seguridad a seguir en la utilización de los medios tecnológicos, tanto dentro como fuera de las instalaciones de la AP.
- Garantizar el uso adecuado de los medios tecnológicos, así como posibilitar la utilización eficiente de la red de comunicaciones y la distribución adecuada de los recursos colectivos, evitando prácticas incorrectas o inadecuadas en la utilización de dichos medios.
- Proporcionar criterios, pautas y medidas para que los usuarios de la AP hagan una utilización correcta de los medios tecnológicos puestos a su disposición, evitando la indebida utilización de los recursos de la Administración.

3. Ámbito de aplicación

El presente documento está dirigido y se aplica a los usuarios de la AP.

Este código de conducta es de aplicación, salvo que se disponga lo contrario, previa aprobación del CCSI, en la utilización de los medios tecnológicos puestos a disposición de los usuarios de la AP, entendiendo como tales todos los medios tecnológicos suministrados por la OIP, utilizados por los usuarios con independencia de su ubicación.

4. Utilización de los medios tecnológicos

a) Principios generales.

- Los archivos, datos y documentos recogidos en los sistemas de almacenamiento de datos se utilizarán para el desarrollo de las funciones encomendadas, es decir con fines profesionales en el ámbito público.

  No obstante, se permite un uso restringido y prudencial del sistema de almacenamiento de los dispositivos de uso personal a efectos de cumplir con obligaciones relativas a estudios académicos, o bien para atender necesidades personales razonables, siempre que se haga de manera restrictiva y sin detrimento de las responsabilidades asociadas a las funciones asignadas. El reconocimiento de este uso personal limitado del almacenamiento en dispositivos exime de obligaciones o responsabilidad a la AP respecto al mantenimiento y protección de la información personal almacenada, que corresponderá exclusivamente al usuario.

- Con carácter general se utilizará el almacenamiento compartido de archivos que proporciona la organización para guardar información corporativa que deba tener un carácter permanente en el tiempo, ya que está respaldado por políticas de copiado de respaldo y debidamente sujeto a mecanismos de seguridad, en lugar del uso del

almacenamiento local de los dispositivos asignados al usuario (disco duro del equipo de escritorio).

- La información manejada en el desempeño de las funciones que se tienen encomendadas y, muy especialmente, la que contenga datos de carácter personal, o bien que por su naturaleza haya sido clasificada como confidencial, sólo podrá almacenarse utilizando los recursos permitidos oficialmente. La precitada información sólo podrá enviarse a los receptores autorizados, e incluso, a terceras personas, oficinas, unidades o centros previa aprobación del Responsable de la Información, dando cumplimiento a lo establecido al respecto por el Reglamento (UE) 679/2016 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la Protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos (RGPD), la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDPyGDD), el ENS y las futuras normas que sean de aplicación en esta materia.

  Por consiguiente, el envío de dispositivos de almacenamiento con información sobre los trabajos que se estén realizando, o procedente de las bases de datos de la AP deberá estar autorizado por el Responsable de la Información.

  Por tanto, los usuarios que tengan acceso a dichos archivos o documentos, deberán extremar las precauciones para evitar cualquier fuga o divulgación de información de los mismos que pueda hacer a la AP o al usuario, incurrir en algún tipo de responsabilidad. Asimismo, deberán tenerse en cuenta todas las medidas de seguridad adoptadas en relación con los archivos que contengan, o no, datos personales.
- Todo usuario de la AP está obligado a cumplir las medidas de seguridad establecidas por el Comité (CCSI), de acuerdo con lo previsto en la Resolución de 21 de diciembre de 2015, de la Secretaría de Estado de Presupuestos y Gastos, por la que se regula la política de seguridad de los sistemas de información de la Secretaría de Estado de Presupuestos y Gastos y de la Intervención General de la Administración del Estado, que se difunden en la Intranet corporativa.

b) Propiedad y especificaciones de los sistemas operativos

Los usuarios se comprometen a respetar la integridad de los recursos y sistemas de información del ámbito de la AP, a los que tengan acceso para la realización de sus tareas, de forma que se garantice:

- El mantenimiento del estado en el que la OIP entrega los componentes hardware y software, así como de las configuraciones de los sistemas operativos de los equipos informáticos asignados al mismo usuario o a otros usuarios a no ser que se disponga de la debida autorización.
- La ejecución de aplicaciones informáticas diseñadas y dimensionadas para la utilización adecuada de las redes o los servidores, el funcionamiento apropiado de los equipos informáticos y la monitorización de la actividad de las redes, de los equipos, de las aplicaciones o de los usuarios de acuerdo con lo dispuesto en la normativa de seguridad y en este código de conducta.

- La autorización del responsable de la Información o del responsable del servicio para realizar modificaciones de privilegios o permisos, atendiendo siempre a la naturaleza de los mismos.
- El uso adecuado y diligente de los medios tecnológicos con objeto de evitar daños físicos o lógicos de los mismos.
- El desarrollo o uso de programas cuya ejecución facilite solamente el acceso a los recursos autorizados por el administrador del Sistema.
- La custodia, con la debida diligencia, de las credenciales de acceso de cualquier índole que pudieran facilitarse al usuario para utilizar o acceder a cualquiera de los medios tecnológicos de la AP.

c) Instalación de programas

Los programas informáticos instalados en los equipos informáticos son propiedad de la AP. Sólo está permitida su utilización, copia o reproducción para fines profesionales, salvo autorización expresa para ello, y siempre observando los procedimientos establecidos por la OIP, a fin de controlar el número de licencias y, en su caso, preservar los derechos de autor de los mismos.

Todos los programas que se instalen o ejecuten en equipos informáticos que pertenezcan a la AP deben contar con la debida licencia. Los programas que se consideren necesarios para el desarrollo de las funciones, que se reciban de otras unidades de la Administración General del Estado o de otras Administraciones, o de los que se haya tenido conocimiento por cualquier otro medio, deben remitirse a la OIP, con el fin de que sean analizados para garantizar su compatibilidad con los sistemas de información corporativos, para que, si procede, sean distribuidos por los procedimientos establecidos a efectos de su mantenimiento y control.

d) Descarga, copia, almacenamiento y distribución de material protegido

Las copias o descargas siempre deberán ajustarse a la normativa vigente. Por consiguiente, la presencia de material protegido en los soportes de almacenamiento corporativos o en dispositivos de almacenamiento particulares utilizando los medios tecnológicos proporcionados por la OIP, así como, la transmisión de música, películas y obras de otras personas es considerada como una infracción contra el derecho de la propiedad intelectual y, por lo tanto, el usuario que así proceda estará incurriendo en las responsabilidades que correspondan de acuerdo con la normativa vigente.

e) Almacenamiento externo de información

La información procedente de las bases de datos de la AP sólo podrá almacenarse en sitios de Internet que ofrecen este tipo de servicios si han sido objeto de una contratación expresa por la OIP.

f) Inicio de la relación laboral con la Administración presupuestaria

Se habilitará un procedimiento para informar a todo el personal sobre las obligaciones impuestas por este código de conducta y de conocer las normas y procedimientos de seguridad en el ámbito de la AP, incluyendo su responsabilidad exclusiva en el mantenimiento y protección de la información personal derivada del uso limitado de dispositivos de almacenamiento y del correo electrónico. Así como la de notificar cualquier situación anómala que comprometa la seguridad de la organización.

g) Finalización de la relación laboral con la Administración presupuestaria.

Cuando una persona finalice su relación laboral con cualquiera de los órganos de la AP o, en general, con alguno de los órganos a los que la OIP proporciona servicio informático a través de su red, o se traslada a otro puesto de trabajo, deberá dejar intactos todos los archivos y documentos que contengan los dispositivos de almacenamiento que ha utilizado: disco duro del equipo, unidad departamental, espacio de colaboración o escritorio remoto.

El usuario deberá gestionar el traspaso de todos los archivos y documentos que hayan tenido un fin profesional de acuerdo con lo que disponga el responsable del órgano en el que estuviera asignado.

En el supuesto de que en alguno de los dispositivos corporativos de almacenamiento que haya utilizado existan archivos que no sean de utilidad profesional, él mismo deberá gestionar su traspaso a un dispositivo de almacenamiento de su propiedad o su eliminación (si no afectara al desempeño profesional de la unidad), poniéndose en contacto, en caso de duda sobre el modo y carácter de la eliminación, con su administrador de centro. El administrador de centro seguirá las instrucciones de la Unidad de Coordinación de Incidencias (en adelante, UCI) para realizar un borrado seguro de la información contenida en los dispositivos corporativos de almacenamiento que haya utilizado el usuario implicado.

En el caso de que exista información personal en alguno de los dispositivos corporativos de almacenamiento que haya utilizado, debe ser eliminada por el propio usuario antes de seguirse el procedimiento explicado en los párrafos precedentes.

Si el responsable del órgano lo considera necesario designará la persona que hubiera de gestionar, con el usuario que causa baja o se traslada, el traspaso de la información profesional. En este caso, este último introducirá sus credenciales de acceso y permitirá que la persona designada por el responsable del órgano salve en algún dispositivo corporativo de almacenamiento los documentos y archivos relacionados con el trabajo, borrando después el resto de los documentos y archivos. Según el procedimiento aplicable en cada momento se concederán permisos de acceso a la información profesional copiada en los dispositivos corporativos de almacenamiento, al responsable del órgano o a la persona que designe.

En el caso de que el usuario decline su asistencia al acto descrito en el párrafo precedente o en caso de deceso, el responsable del órgano designará a una persona de la unidad en que prestaba servicio el usuario para que, junto con el administrador de centro, revise la información almacenada por si fuera necesaria para la continuidad del servicio, efectuando su traspaso. En todo caso, posteriormente se ha de realizar un borrado seguro de los dispositivos corporativos de almacenamiento utilizados, de acuerdo al procedimiento establecido por la OIP.

h) Controles sobre la utilización de los medios tecnológicos

Con el objetivo de garantizar las condiciones establecidas por este código de conducta para el uso de los medios tecnológicos de la AP, la OIP, en la medida en que los recursos y la técnica lo permitan, establecerá controles, previamente acordados por el CCSI.

Para el establecimiento de estos controles sobre la utilización de medios tecnológicos de la AP se emplearán las herramientas disponibles en cada momento que pueden consistir en software específico, herramientas de monitorización, de control de tiempo o de sitios visitados, programas de captura periódica de imágenes de la pantalla del ordenador, diarios de la actividad en la navegación por Internet, etc….

El alcance de estos procedimientos de control o inspección será recogido en este código de conducta, para general conocimiento por todos los usuarios de los medios tecnológicos de la AP, de forma que quede constancia pública de la existencia de los mismos.

Actualmente se podrán implementar los siguientes controles sobre la actividad de los usuarios:

- Control de las impresiones y copias efectuadas. Los Responsables de centro pueden obtener un informe con las impresiones y copias efectuadas por cada usuario, distinguiendo si es en blanco y negro y color. Pudiéndose llegar hasta el nombre y tipo de fichero impreso.
- Los controles referidos a la utilización del servicio de mensajería y de navegación por internet se incluyen en su correspondiente apartado.

5. Custodia y almacenamiento de la información puesta a disposición de los usuarios

La información manejada en el desempeño de las funciones que se tienen encomendadas sólo podrá almacenarse utilizando los recursos permitidos oficialmente.

Muy especialmente, la que contenga datos de carácter personal, o bien que por su naturaleza haya sido clasificada como confidencial.

La precitada información sólo podrá enviarse a los receptores autorizados, o a terceras personas, oficinas, unidades o centros previa aprobación del Responsable de la Información, dando cumplimiento a lo establecido al respecto por el Reglamento (UE) 679/2016 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la Protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de estos datos (RGPD), la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDPyGDD), el ENS y las futuras normas que sean de aplicación en esta materia.

Por consiguiente, el envío de dispositivos de almacenamiento con información sobre los trabajos que se estén realizando, o procedente de las bases de datos de la AP deberá estar autorizado por el Responsable de la Información.

Por tanto, los usuarios que tengan acceso a dichos archivos o documentos, deberán extremar las precauciones para evitar cualquier fuga o divulgación de información de los mismos que pueda hacer a la AP o al usuario, incurrir en algún tipo de responsabilidad.

Asimismo, deberán tenerse en cuenta todas las medidas de seguridad adoptadas en relación con los archivos que contengan, o no, datos personales.

6. Caso especial del uso del correo electrónico.

El correo electrónico es un recurso informático para el intercambio de información. Para evitar que se convierta en una herramienta de envío masivo e indiscriminado de información y garantizar su utilización de forma segura, se deben observar unas reglas mínimas de conducta.

Abuso en la utilización del correo electrónico

Se considera abuso la utilización del correo electrónico para actividades que trasciendan los objetivos habituales del servicio de correo y perjudiquen directa o indirectamente a los usuarios o al funcionamiento normal de la AP.

Tipos de abuso

Cabe considerar al menos los siguientes tipos de abuso en la utilización del correo electrónico:

- Envío de contenido inadecuado

  Contenido que por su naturaleza sea susceptible de ser tipificado como ilegal o atentatorio a la dignidad, intimidad o confidencialidad de las personas. Envío de programas informáticos (software) sin licencia, de alerta de virus falsos o difusión de virus reales o que puedan perjudicar a la AP, o a las Administraciones públicas.

  Envío de contenidos con derechos de autor y, por tanto, sujetos a la Ley de propiedad intelectual.

- Envío a través del buzón asignado a otra persona.

  Aunque el contenido del mensaje a enviar sea legítimo, no se puede utilizar el buzón asignado a otra persona, a no ser que ésta haya dado su consentimiento por escrito indicando que no tiene información personal o, en caso de que la haya, haciéndose responsable de una posible divulgación de la misma.

- Envíos masivos no autorizados

  El envío masivo de publicidad, felicitaciones o de otro tipo de correos utilizando el buzón propio u otro ajeno. Se entenderá como "masivo" cuando el número de destinatarios del mismo o su contenido sea desproporcionado en relación con los objetivos profesionales inherentes al propio mensaje.

- Ataques con el objetivo de imposibilitar o dificultar el servicio.

  Es indiferente que vaya dirigido a un usuario concreto o a todo el sistema. Este tipo de ataques consiste en el envío de un número alto de mensajes, que tenga por objeto paralizar el servicio a todos o a un usuario, disminuir la capacidad de proceso del servidor, o de almacenamiento de un servidor o usuario.

- **El correo corporativo se utilizará para fines profesionales.** En ningún caso su utilización podrá dar lugar a los siguientes supuestos:
    - Para la propagación de cartas encadenadas.
    - Para recoger correo de buzones que no pertenecen a la AP, sino a proveedores de correo de Internet.
    - Para uso con fines lucrativos o comerciales, para uso recreativo o cualquier otro que no tenga relación con la actividad laboral.
    - Para la inscripción a "newsletter", grupos de noticias, o similares que no estén directamente relacionadas con la función asignada al usuario y que resulten de plena confianza.
    - Para utilizar las listas de distribución de correo para fines distintos de los propios de la AP, y nunca para fines publicitarios, comerciales o de índole personal que no estén relacionados con el desempeño de la función asignada.

Igualmente sería una utilización indebida, además de las posibles implicaciones legales:

- El acceso a un buzón distinto al propio sin consentimiento, por escrito o por delegación autorizada expresamente en el sistema de la persona que lo tiene asignado, pues, en este caso, se estaría incurriendo en delito de violación de correspondencia.
- El envío, sin autorización, de datos procedentes de las bases de datos de la AP a las que se tiene autorización de acceso, a personas destinadas dentro o fuera de la AP y que carecen de autorización de acceso a las bases de datos de las que proceden los datos extraídos.
- El uso del correo electrónico como contenedor o almacén de información afectando negativamente a la disponibilidad del espacio asignado al resto de usuarios de la AP.
- El envío de correos en los que el remitente no sea el propietario del buzón, sino que se utilice otro nombre suplantando la identidad de otra persona.

Información que debe incluirse en el mensaje y firma

Todos los correos electrónicos emitidos desde cualquier cuenta electrónica corporativa, deberán ser identificados bajo un título relacionado con el contenido e incluir la siguiente información de acuerdo con las directrices establecidas desde la Subsecretaría del Ministerio de Hacienda y Función Pública:

- Nombre completo del emisor.
- Puesto de trabajo que ejerce el emisor.
- Código DIR3 que tiene asociado el puesto de trabajo.
- Centro directivo en el que el emisor está destinado.
- Dirección postal corporativa.
- Teléfono oficial.
- Cuenta electrónica de correo corporativa

- Logotipo del Ministerio de Hacienda y Función Pública.

Medidas preventivas

En el supuesto en que un usuario no observe alguna de las normas, reglas y recomendaciones o incurra en alguno de los abusos señalados en el presente documento en relación con el correo electrónico, sin perjuicio de las acciones disciplinarias o legales que procedieran, el CCSI o la persona en quien delegue podrá acordar la supresión de la asignación del buzón de correo o, en su caso, de alguna de sus funcionalidades, o la limitación del espacio de almacenamiento asignado al buzón en el servidor de correo.

Controles establecidos

Mensualmente se podrá elaborar un informe para cada centro o unidad en el que se relacionarán para cada usuario el número de mensajes enviados y recibidos, clasificados por tamaño y día del mes.

7. Uso del correo electrónico no corporativo

En ningún caso la información interna que el usuario maneje en el ejercicio de las funciones asignadas o durante los servicios de apoyo que preste en Órganos que están fuera del ámbito de la AP podrá enviarse a través de un buzón de correo externo.

8. Caso especial de la navegación por Internet

Las conexiones que se produzcan a través de Internet tienen que obedecer a fines profesionales en el ámbito público, con el propósito de obtener el mayor aprovechamiento de los recursos informáticos. No obstante, se permite un uso restringido y prudencial a efectos de cumplir con obligaciones relativas a estudios académicos, o bien para atender necesidades personales razonables, siempre que se haga de manera restrictiva y ocasional, y sin detrimento de las responsabilidades asociadas a las funciones asignadas.

La navegación por sitios web, el envío de mensajes, registros, altas, relleno de formularios y cualquier otra actividad realizada vía Internet, serán completa responsabilidad del usuario emisor y en todo caso deberá asumir las consecuencias que emanen de su actuación.

En ningún caso deberá accederse a direcciones de Internet con contenido ilegal o atentatorio a la dignidad, privacidad o confidencialidad de las personas.

Es obligación de las Administraciones Públicas dar cumplimiento al contenido de las normas que protegen la propiedad intelectual o industrial, por lo que los usuarios deberán comprobar cuidadosamente, antes de utilizar información procedente de Internet, si la misma se encuentra protegida por las citadas normas.

Bajo ningún concepto se debe publicar, almacenar o poner a disposición de terceros copias no autorizadas de material con derechos de autor, o de soportes de almacenamiento de la AP, a través de la red de comunicaciones o de Internet utilizando los equipos y sistemas de información de la AP, salvo que se haya obtenido expresamente autorización por escrito de los titulares de los derechos.

No se debe contribuir o participar en cualquier infracción de los derechos de propiedad intelectual utilizando o conectándose a una red de intercambio de ficheros, o servidor P2P, con los equipos y sistemas de la AP.

En caso de detectar un uso inadecuado de Internet por parte de un usuario, sin perjuicio de las acciones disciplinarias o legales que procedieran, el CCSI o la persona en quien delegue podrá tomar medidas orientadas a restringir el acceso a determinadas direcciones de Internet.

Controles establecidos

Dado el riesgo que supone para la AP los servicios de acceso a Internet, se monitorizará e inspeccionará el tráfico, con el fin de poder detectar y corregir cualquier anomalía o uso no adecuado que se esté produciendo o pueda producirse.

La inspección podrá realizarse sobre el tráfico generado durante la navegación personal con acceso a Internet, incluyendo aquel que utilice protocolos de navegación segura.

Los registros resultantes de la actividad de la monitorización e inspección no podrán almacenarse indefinidamente y tendrán restringido su acceso exclusivamente al personal autorizado.

Mensualmente se podrá elaborar un informe para cada centro o unidad en el que se recoja para cada usuario el tiempo que ha dedicado en el mes a la navegación por internet y la categoría de las páginas visitadas.

9. Custodia y mantenimiento de los recursos informáticos puestos a disposición de los usuarios

a) Recursos informáticos móviles.

Este tipo de dispositivos estarán bajo la custodia del usuario que los utilice, o del administrador de centro asignado por el responsable de centro. Es responsabilidad de ambos adoptar las medidas necesarias para evitar el acceso a ellos de personas no autorizadas, así como su sustracción o que sufran daños por manipulaciones incorrectas.

En caso de sustracción se ha de poner inmediatamente en conocimiento del responsable de la seguridad del edificio y del responsable de personal de la Unidad para la adopción de las medidas que correspondan (por ejemplo, presentar la correspondiente denuncia en la comisaría de policía), así como de la División de Explotación de la OIP de la IGAE a efectos de baja en el inventario.

Cuando cambien las circunstancias laborales (por ejemplo: término de una auditoría, cese en el cargo, etc.) que originaron la entrega de un recurso informático móvil se deberá proceder a su devolución al administrador de centro del centro para que borre la información que tenga almacenada y deje el recurso en su estado original para que pueda ser asignado a un nuevo usuario. En caso de que haya información personal del usuario que haya tenido asignado el ordenador éste será responsable de borrar la información del dispositivo. Si la información personal fuese divulgada o accedida por terceros debido a la inadecuada diligencia de la persona propietaria de la misma, no podrá imputársele ningún tipo de responsabilidad a la AP.

b) Recursos informáticos de sobremesa.

Igualmente, la persona a la que se le haya asignado un puesto de sobremesa deberá adoptar las medidas necesarias para evitar que usuarios no autorizados tengan acceso al equipo, bloqueando la sesión en toda ausencia de su puesto de trabajo, por breve que sea.

c) Dispositivos internos y externos de almacenamiento. Se incluye dentro de este apartado cualquier tipo de documento o soporte de Información en cualquier tipo de soporte registral o de almacenamiento, incluidos los de distribución de software de fabricantes, listados de programas, datos de pruebas, documentación de los sistemas, dispositivos de almacenamiento extraíbles.

Al terminar la jornada laboral o ausentarse del puesto de trabajo debe evitarse dejar en lugar visible los dispositivos externos de almacenamiento de información. Esta medida también es de aplicación a las salidas de información de los sistemas de información y bases de datos de la AP en soporte papel.

Asimismo, es recomendable establecer una contraseña de acceso a los dispositivos de almacenamiento extraíbles.

Todos los elementos de equipos que contengan dispositivos corporativos de almacenamiento de datos, por ejemplo, discos duros fijos, deben comprobarse antes de su reutilización o eliminación para asegurar que todo dato sensible, y software bajo licencia, han sido borrados o sobrescritos. En el caso de que se almacene información personal, la responsabilidad de que se produzca su acceso por otras personas o su divulgación será del propio usuario, no

pudiéndose imputar responsabilidad alguna a la AP como se ha indicado anteriormente.

Los dispositivos corporativos de almacenamiento extraíbles con información sensible deben contener la información cifrada o, al menos, protegida con una contraseña. Una vez que no sea necesaria, se deben destruir físicamente o sobrescribirse o borrarse de manera segura y no simplemente usando la función normalizada de borrado.

10. Trabajo no presencial

El trabajo a distancia o teletrabajo facilita el ejercicio de las competencias de la AP cuando el trabajador no pueda acceder presencialmente a las oficinas, ahora bien, también la hace más vulnerable.

Por consiguiente, además de observar todas las medidas mencionadas en las secciones anteriores se deben introducir controles adicionales con objeto de evitar suplantaciones de identidad de las personas que trabajan en la AP, indisponibilidad de los sistemas debido a ataques por denegación de servicio, intentos de acceso en tramos horarios no habituales, escaneos de la red interna y todos aquellos ataques que se presenten en el futuro.

La conexión a la red corporativa desde cualquier ubicación física se puede realizar utilizando la solución de movilidad proporcionada por la OIP o dispositivos personales, en todo caso bajo los procedimientos técnicos habilitados por dicha Oficina.

La solución de movilidad corporativa está conformada por un ordenador portátil configurado con las medidas de seguridad implementadas por la OIP y la conexión se realiza a través de una VPN[1] o de ER[2] por Internet.

Con objeto de que un usuario pueda trabajar como si estuviera en la oficina utilizando la solución de movilidad corporativa es clave que se tenga en consideración lo siguiente:

- Conectar el portátil a la red corporativa en la propia oficina al menos cada 30 días, al objeto de garantizar la actualización de la última versión de las herramientas de seguridad. No obstante, en caso de que se presente una situación excepcional como la pandemia debida al COVID19, u otras similares que pudieran presentarse en un futuro, el número de días indicado se revisará con objeto de evitar un impacto negativo en el ejercicio del trabajo encomendado.

  En caso de obviar lo indicado en el párrafo anterior al intentar conectar el portátil a la red corporativa, a través de la VPN, el sistema detectará que el dispositivo tiene desactualizadas las medidas de seguridad y temporalmente el usuario sólo tendrá habilitado el acceso a un número limitado de funcionalidades. Este periodo transitorio depende del tiempo que necesite el portátil para actualizarse.

Actualmente están implantados los siguientes controles:

- Detección de tráfico de red muy elevado ya sea en el perímetro externo o en la red interna de la AP.

[1] Acrónimo en inglés de Red Privada Virtual.
[2] Escritorio Remoto.

- Registro de las conexiones y desconexiones de los usuarios, de forma que, cuando un usuario se conecta a la red, se le informa de cuando realizó la última conexión.
- Obtención de informes de conexiones y desconexiones de los usuarios a disposición de la unidad responsable de personal y, en su caso, de los responsables de las unidades.

El trabajo no presencial implica el uso de redes cuya administración es ajena a la AP, por lo tanto, todo acceso remoto se hace securizando el canal de transmisión a través de técnicas de virtualización del canal y cifrado del contenido transmitido. Es responsabilidad del usuario mantener la seguridad de las comunicaciones en tales circunstancias evitando:

- permitir que personas ajenas a la organización pueda acceder a la información tratada ya sea por cesión directa de la información o bien revelación voluntaria o accidental de credenciales que permitan el acceso a la organización. Se deberán cambiar inmediatamente las contraseñas si se sospecha que han podido ser sustraídas o reveladas.
- el uso de equipos asignados por la AP para actividades ajenas a la función para la cual están destinados, en especial aquellas actividades que implican el uso de canales de comunicación con terceros que puedan acceder al equipo e instalar software malicioso.
- dejar cualquier documentación confidencial o contraseñas al descubierto, esto incluye abandonar el puesto de trabajo de forma provisional dejando el esquipo desbloqueado.
- utilizar redes inalámbricas de uso público a las que se pueda acceder sin el uso de una contraseña robusta.
- utilizar medios para compartir información en la nube que no cuenten con un control de accesos adecuada.
- abrir correos de fuentes desconocidas que contengan ficheros o enlaces a sitios extraños.
- utilizar medios no cifrados para videoconferencias donde la confidencialidad de las sesiones de audio o video no estén garantizadas.