Anexo I - Dominio de Comunicaciones

Norma de seguridad para el acceso a Internet

1. Principios generales.

Con el despliegue de las TIC y el uso generalizado de Internet como herramienta de comunicación global, se han extendido igualmente las amenazas que ponen en peligro la confidencialidad y disponibilidad de la información y de los sistemas que le dan soporte. Para minimizar los riesgos que de ello se derivan, es imprescindible adoptar medidas de protección que propicien un correcto uso de estos medios.

El acceso corporativo a Internet desde el CSIC es un recurso que el Organismo pone a disposición de los usuarios como herramienta necesaria para el desempeño de su actividad profesional. En consecuencia, es necesario velar por su buen uso para asegurar tanto su adecuado funcionamiento en términos operativos como la seguridad de la red y de los recursos conectados a ella.

De manera más específica, se ha de garantizar un uso adecuado de los servicios de Internet, por los siguientes motivos:

a) Seguridad: para evitar, entre otros posibles riesgos, la infección por software dañino (virus, troyanos, etc.), los accesos no autorizados y el robo de información.

b) Tráfico externo de datos: con el fin de asegurar que el acceso a los contenidos necesarios para la actividad profesional no se vea perjudicado por el tráfico no ligado con el desempeño de la actividad profesional de cada trabajador en el marco de su relación laboral con el CSIC.

c) Tráfico interno de datos: como consecuencia de tráfico descargado de la web y su posterior almacenamiento en alguno de los recursos y equipos internos disponibles a tal efecto. Esta situación aconseja también regular las condiciones en las que deben realizarse las descargas y transferencias de archivos de gran tamaño, así como su movimiento a través de la red corporativa de un medio de almacenamiento a otro de manera que, en los casos en que sea necesario, se empleen los medios más adecuados para ello con el fin de evitar un deterioro de la rapidez de respuesta y calidad del servicio percibida por los demás usuarios con los que son compartidos los recursos de la red.

d) Ética y legalidad: es ineludible el compromiso que el CSIC, como institución pública, debe mantener con la sociedad, a la hora de vetar el acceso a contenidos no relacionados con el desempeño profesional de cada trabajador, y especialmente cuando éstos se encuentran alejados de determinados principios éticos, así como ejercer el control oportuno sobre el material sujeto a derechos de propiedad industrial o intelectual.

2. Acceso y uso de recursos de Internet.

Como norma general, todo el personal del CSIC y de sus Centros Mixtos dispondrá de acceso a Internet desde su equipo o equipos de trabajo, siempre que en la ubicación de su puesto de trabajo exista disponibilidad para ello. En otro caso, deberán poder acceder a Internet desde algún punto de acceso común que se habilite para tal fin; corresponde a la Gerencia de los

Institutos, Centros y Unidades (ICU) u Oficialía Mayor proporcionar tales medios comunes, en caso de existir esa necesidad.

Las conexiones que se realicen a Internet deberán obedecer, como norma general, a fines profesionales. El acceso a Internet para fines personales debe limitarse a lo mínimo imprescindible y, de ser necesario, sólo se utilizará sin interferencia en el rendimiento y desempeño de la labor profesional ni en la eficiencia de los recursos informáticos corporativos, dado el carácter compartido de éstos para todo el personal. En cualquier caso, el uso de internet para fines personales, si fuera imprescindible, se realizará también conforme a las normas de seguridad.

Al personal perteneciente a empresas contratistas u otro personal externo que durante el periodo de vigencia del contrato preste servicio en las dependencias del CSIC se le podrá habilitar el acceso a recursos, abrir puertos distintos de los habilitados por defecto o cubrir otras necesidades específicas, siempre que quede netamente justificada la necesidad para el desarrollo de su cometido en esta institución. Se precisará una petición por escrito y debidamente motivada del responsable del proyecto o servicio por parte del CSIC solicitando los correspondientes accesos para dicho contratista. Será la Secretaría General Adjunta de Informática (SGAI) en el caso de la Organización Central (ORGC) y la Gerencia, Dirección o Vicedirección de los ICU en su ámbito de responsabilidad, quienes deberán valorar y, si lo estiman procedente, autorizar los citados permisos excepcionales de acceso a este "personal externo". Las solicitudes autorizadas deberán ser conservadas por las unidades responsables mencionadas, con el fin de disponer de un registro y trazabilidad sobre la persona o unidad solicitante junto con la necesidad y la posible existencia de plazos limitados de todos aquellos permisos excepcionales otorgados.

Salvo excepciones debidamente justificadas y autorizadas expresa y formalmente por parte del CSIC, los medios físicos para efectuar dicho acceso a Internet y, con un carácter más general, para el desarrollo de las labores propias del contrato en base al cual están prestando servicio en las dependencias del CSIC, deberán ser aportados por las empresas contratistas. Los equipos que pudieran aportar deberán cumplir tanto las normas de seguridad establecidas por el CSIC como las complementarias definidas por el ICU.

El personal sujeto a estancia temporal en algún ICU para la realización de proyectos o actividades de duración limitada, por defecto, podrá disponer de acceso a Internet. En función de las características específicas del proyecto o actividad, y previa solicitud motivada del responsable de dicho proyecto o actividad en el ICU dirigida a la Dirección, Vicedirección o Gerencia, según determine reglamentariamente el ICU, podrá acceder bajo las mismas consideraciones que el personal propio o el personal externo, según el caso.

De manera preferente, y salvo que existan sólidos impedimentos de carácter físico o tecnológico, el acceso a la red interna y, por extensión, a Internet se realizará por medios cableados desde el equipo del usuario hasta una roseta RJ-45 de conexión de cable de datos próxima, si bien podrá efectuarse por medios inalámbricos cuando sea pertinente mediante la infraestructura de red Wifi.

2.1. Acceso a Internet a través de redes inalámbricas (Wifi)

En aquellos casos en los que la conexión a Internet deba realizarse por medios inalámbricos, y siempre que la infraestructura lo permita, al personal interno del CSIC y de sus centros mixtos, así como al personal externo de las categorías anteriormente mencionadas (empresas contratadas y estancias breves) se le habilitará un acceso a Internet con equivalentes permisos de acceso y recursos al que se tiene por medios cableados.

Por su parte, en el caso de proporcionar a terceros (asistentes a reuniones, visitantes, etc.) un acceso puntual a Internet como un servicio de cortesía, éste deberá ser ofrecido siempre que sea posible desde una red habilitada para tal uso, con acceso y permisos restringidos, que permitan exclusivamente la navegación estándar por Internet sin acceso a los recursos internos de la red del ICU o de la ORGC.

En aquellos centros en los que se disponga de acceso inalámbrico a Internet a través de la red *Eduroam*, el personal "invitado" con acceso a Eduroam deberá acceder a través de la correspondiente red de "invitados" habilitada al efecto empleando los mecanismos de autenticación que en cada caso se indiquen.

En función de las características y configuración efectuada en cada ICU o en la ORGC, el acceso de personal "invitado" deberá efectuarse mediante los procedimientos definidos para la conexión a la red Wifi "Invitados", cuyas credenciales de acceso y conexión se podrán obtener por alguno de los medios que se indique en cada ICU a los usuarios interesados.

2.2. Descargas de contenido

Salvo por necesidades estrictamente ligadas al desempeño profesional, no podrá llevarse a cabo la descarga de archivos que superen los tamaños que cada ICU o la SGAI determine en su respectivo ámbito, especialmente en horarios coincidentes con el horario habitual de trabajo. El tamaño máximo de los ficheros podrá ser determinado por la Gerencia de cada ICU en base a la capacidad de su red, con el posible apoyo de la SGAI.

Como regla general, el tamaño máximo de descarga (expresado en GB) no deberá superar en 100 veces el ancho de banda disponible del enlace a Internet del ICU (expresado en Gbps). A modo de ejemplo: un ICU con un ancho de banda de 1 Gbps debería limitar los tamaños máximos de descarga de archivos a un tamaño de 100 GB.

Aquellos casos que lo requieran dentro del ámbito profesional deberán ser comunicados al Centro de Atención a Usuarios en el caso de la ORGC, y a la Unidad TIC o Gerencia de los ICU en su ámbito de responsabilidad, para que se lleven a cabo las configuraciones que, en la medida de lo posible, permitan tal descarga masiva de información sin perjudicar el rendimiento de la red y su uso normal por parte del resto de usuarios.

2.2.1. Descarga de archivos mediante técnicas extremo a extremo (P2P)

No se podrán descargar ficheros, cualquiera que sea su naturaleza y temática, mediante sistemas P2P dado que suponen un riesgo importante de seguridad, y cuya ejecución pone en peligro los recursos conectados a la red corporativa. Podrán exceptuarse de esta norma las descargas que respondan a imperativos técnicos o de ámbito investigador y sean

debidamente solicitadas y autorizadas por el Comité Corporativo de Seguridad de la Información.

El acceso a contenido externo, así como la descarga y la ejecución del mismo en equipos conectados a la red corporativa, habrá de efectuarse mediante los mecanismos y herramientas que indiquen al efecto las unidades TIC.

3. Malware y fraudes en Internet.

El concepto de malware se corresponde con un abanico de variantes, cada vez más sofisticadas, de lo que en los orígenes de la popularización del uso de Internet se conocía como virus. El malware persigue distintos fines que, por lo general, se pueden encuadrar en dos tipologías generales: por un lado el fraude, robo o el uso de otros mecanismos que se suelen materializar de forma directa en la obtención de dinero por parte de los ciberdelincuentes (creadores o usuarios del malware); y por otro, el robo de información sensible, que indirectamente también conllevará la desestabilización o la obtención de beneficios económicos para los ciberdelincuentes con la consiguiente pérdida por parte de los usuarios afectados (personas físicas, organismos públicos, empresas privadas, etc.).

Dado que el malware puede estar oculto en muy diversas fuentes, tales como enlaces y barras publicitarias en páginas web, documentos adjuntos y enlaces incluidos en correos electrónicos, ventanas emergentes, etc., se deberán extremar las medidas de precaución tanto a la hora de visitar páginas web de dudosa fiabilidad como a la hora de ejecutar archivos adjuntos o abrir enlaces incluidos en correos electrónicos, aunque provengan de remitentes conocidos y de confianza.

Las personas que reciban algún correo electrónico que entiendan puede ser malicioso por su contenido o por su origen, o bien las que detecten cualquier tipo de comportamiento anómalo en su ordenador de trabajo, deberán ponerse en contacto con el CAU o con el personal del servicio TIC correspondiente a su ICU.

3.1 Phishing

Dentro de las distintas variantes de malware y de las distintas técnicas de fraude a través de Internet, una de las más extendidas y, por sus consecuencias, peligrosa, es el *phishing*.

Se conoce como *phishing* a todas aquellas técnicas utilizadas para tratar de obtener de los usuarios información confidencial, entre las que habitualmente se encuentran las credenciales y claves de acceso a diferentes sitios. Entre ellas cabe destacar como las más habituales las credenciales de acceso a páginas web de bancos, claves (PIN) de firma de una tarjeta de crédito/débito, contraseña de acceso al ordenador del usuario, credenciales de acceso a redes sociales, etc.

Para ello suelen emplearse técnicas de *ingeniería social*, que tienen como denominador común el solicitar esa información confidencial al usuario haciéndole creer que la está proporcionando a alguien confiable (el propio banco, la propia red social, el propio servicio informático del trabajo, etc.) cuando en realidad se está produciendo una suplantación de identidad, bien con un enlace falso incluido en un correo, con un banner publicitario o cualquier otro método que dirige a una falsa página web con aspecto muy similar a la auténtica, y en la que el usuario introduce voluntariamente la información solicitada.

También es habitual el empleo de correos con supuestas alertas de seguridad, de necesidad de cambio de contraseña, de verificación o confirmación de datos personales entre otros que, bajo la confianza de que el sitio en cuestión es el auténtico, hace al usuario proporcionar por sí mismo su información confidencial a los ciberdelincuentes.

En este sentido, conviene destacar que el personal del CSIC nunca va a solicitar a los usuarios ninguna clave, contraseña ni información confidencial de otra índole mediante correo electrónico, teléfono ni ningún otro medio, por lo que no deberán ser proporcionadas a nadie bajo ningún concepto ni en ninguna situación. En el caso de que el CAU o servicio informático del ICU requiriese acceder al equipo del usuario para realizar cualquier actuación, siempre será el propio usuario quien deberá introducir su contraseña en caso necesario, no debiendo tampoco en este caso facilitarla al personal TIC que esté atendiendo su solicitud.

Es de suma importancia acceder a las páginas web deseadas tecleando directamente su Dirección (por ejemplo www.csic.es), en vez de hacerlo a través de enlaces de cualquier tipo recibidos en un correo electrónico o encontrados en cualquier otra página web, barra publicitaria, o lugar similar.

En caso de que un usuario perciba por algún medio algún intento de *phishing* relacionado con cualquier página web deberá ponerlo en conocimiento de forma inmediata con el CAU o con el servicio informático de su ICU, el cual deberá hacer un primer análisis de la situación y poner en conocimiento del Área de Comunicaciones y Seguridad de la SGAI tal situación para que, si procede, se adopten las medidas oportunas.

La SGAI publicará una Guía con recomendaciones y buenas prácticas para la navegación segura por Internet, en la que aparecerán recogidas las principales técnicas y amenazas conocidas en su conjunto como *malware*, así como las principales precauciones a tener en cuenta al respecto.

4. Autenticidad y seguridad de la conexión.

Para aquellos usos de Internet que impliquen realizar un intercambio de información especialmente sensible, como información personal, datos bancarios u otra de índole similar (por ejemplo, en el acceso a bancos por parte de los habilitados pagadores, u otro personal que lo requiera como parte de su desempeño profesional) se deberá, como norma general, introducir manualmente en la barra de direcciones la dirección de la página a la que se desea acceder. De esta forma se asegura el acceso a la página deseada y no a otra que pueda tratar de suplantar a la original.

Alternativamente, y especialmente cuando no se haya efectuado el acceso por el mecanismo señalado, se deberá intentar verificar la autenticidad de la página visitada, es decir, que la página que se visita es realmente la que dice ser. Existen distintas formas de llevar a cabo dicha verificación, las cuales a su vez van cambiando y evolucionando conforme aparecen nuevas versiones de los navegadores de internet, y a su vez presentan matices diferenciadores entre unos navegadores y otros.

Esta cuestión es especialmente importante cuando se utilizan credenciales de acceso a algún recurso corporativo o vinculado directamente con el CSIC (dominio, intranet, o bancos con cuentas corrientes, activos y servicios bancarios propios del Organismo, en el caso del personal habilitado para ello). De igual forma debe ampliarse el ámbito de precaución a aquellos otros sitios en los que, a pesar de no ser una

práctica recomendada, se empleen las mismas credenciales que las utilizadas para el acceso a recursos corporativos.

En la Guía de recomendaciones y buenas prácticas para la navegación segura por Internet se mostrarán, entre otras cuestiones, las principales formas de efectuar dicha verificación.

Adicionalmente a la verificación de la autenticidad de la entidad que se encuentra tras una página web, los mismos medios indicativos servirán para asegurar que la comunicación entre el equipo del usuario y la página web a la que está conectado se realiza de forma cifrada de extremo a extremo. Esto asegura que, aunque alguien pudiera interceptar la información, la misma no sería inteligible y por tanto carecería de utilidad y valor su interceptación.

En general, la información transmitida por Internet no circula de manera cifrada. Sin embargo, en la transmisión de información sensible, confidencial o protegida se deberá asegurar su cifrado mediante los mecanismos de comprobación oportunos recogidos en la citada Guía, u otros distintos que la propia evolución tecnológica de los navegadores vaya convirtiendo en habituales.

5. Confidencialidad de la información.

No está permitido difundir sin autorización cualquier tipo de información de carácter confidencial, reservada o sensible, tanto sobre la propia institución y de su actividad científico-técnica o administrativa como sobre cualquier empleado, grupo o unidad sin perjuicio de los límites que marca la legislación vigente y sin menoscabo del derecho a la libertad de expresión.

6. Suspensión de derechos de acceso.

El Responsable de Seguridad Informática, en coordinación con el Responsable del Sistema y, en su caso, con el responsable de la información que se encuentre en riesgo, podrá acordar la suspensión de los derechos de acceso de los usuarios del CSIC, siempre que obedezca a alguna causa que suponga una vulneración de la Norma General de Seguridad Informática para la utilización de los recursos y sistemas de información del Consejo o de alguna de las Normas Específicas que la acompañan.

Asimismo se podrá limitar temporalmente el acceso a Internet y, por extensión, la conexión a la red corporativa, en aquellos equipos de usuario en los que, a través de las herramientas de seguridad instaladas al efecto, se detecten comportamientos y actividades de riesgo para la seguridad de los recursos de la red, tales como intentos de conexión reiterados a determinados destinos tanto internos como externos, intentos repetitivos de acceso desde equipos externos al equipo de un usuario o la falta de instalación de las herramientas corporativas de seguridad, entre otras.

La suspensión del acceso a Internet finalizará cuando las razones objetivas que dieron lugar a la misma hubieran desaparecido.

7. Condiciones técnicas del acceso seguro a Internet.

Los servicios utilizables por defecto, con sus puertos habituales asociados en el acceso a Internet para los usuarios internos, son los siguientes:

a) Servicios http y https: 80 y 443

b) Servicio ssh: 22

c) Servicios Tomcat: 8080, 8443

d) Servicios proxy

e) Servicios de acceso a VPN más habituales: OpenVPN, Cisco IPSec, VPN over TCP, PPTP VPN

f) Servicios de sistemas de videoconferencia habituales

En el caso de necesitar otros servicios adicionales a los indicados o a los que el usuario percibe como operativos durante su navegación por Internet, se deberá solicitar al CAU de la SGAI, en el caso de la ORGC, o al personal TIC de cada ICU, las necesidades y servicios adicionales que se precisasen junto con la justificación de los mismos. Dichos servicios informáticos analizarán cada situación con los responsables que corresponda en cada caso y determinarán la conveniencia o no de ampliar el abanico de servicios disponibles, de acuerdo a criterios de eficacia en el uso de la red y tratando de salvaguardar la seguridad de los recursos a ella conectados.