

INSTRUCCIÓN SOBRE USO DE MEDIOS, SISTEMAS INFORMÁTICOS Y REDES DE COMUNICACIONES, QUE CETAQUA PONE A DISPOSICIÓN DE SUS EMPLEADOS Y COLABORADORES

OBJETIVOS QUE PERSIGUE LA INSTRUCCIÓN	2
DEFINICIONES	2
AMBITO SUBJETIVO Y OBJETIVO DE APLICACIÓN DE LA INSTRUCCIÓN	3
NORMAS DE ACTUACIÓN	3
NORMAS DE USO DE LOS RECURSOS INFORMÁTICOS	3
NORMAS SOBRE ALMACENAMIENTO DE LA INFORMACIÓN	5
NORMAS DE USO DE APLICACIONES INFORMÁTICAS Y SOFTWARE	5
NORMAS DE USO DEL ACCESO A INTERNET	6
NORMAS DE USO DEL CORREO ELECTRÓNICO	8
NORMAS SOBRE ACCESO Y USO DE SISTEMAS DE INFORMACIÓN Y DATOS TRATADOS	9
MONITORIZACIÓN Y CONTROL DEL CUMPLIMIENTO DE ESTA NORMATIVA	10
NO EXPECTATIVA DE PRIVACIDAD	11
EXIGENCIA DE RESPONSABILIDADES	11
DIFUSIÓN Y CONOCIMIENTO DE LA INSTRUCCIÓN	12

OBJETIVOS QUE PERSIGUE LA INSTRUCCIÓN

La presente instrucción tiene por objeto desarrollar los principios y las directrices de conducta expresados en la política de *CETAQUA de seguridad de la información y uso de las tecnologías de la información y la comunicación ("TIC")*. Estas instrucciones deberán ser difundidas, conocidas y aplicadas por todos los empleados y colaboradores de CETAQUA cuando hagan uso, directa o indirectamente, de los medios y sistemas informáticos y de las redes de comunicación puestos a su disposición por la Fundación para el desempeño de su actividad.

Como advierte la Política, los recursos informáticos constituyen un instrumento imprescindible para la realización de la actividad laboral. CETAQUA los concibe y pone a disposición, única y exclusivamente, para cumplir con las funciones asignadas a cada empleado. El uso con fines personales ajenos al desempeño laboral está expresamente prohibido, sea o no adicionalmente probable desde un punto de vista ético o legal.

Los objetivos perseguidos son varios. El uso eficiente de los medios y recursos informáticos resulta imprescindible para un adecuado y productivo desempeño profesional, lo que constituye un legítimo objetivo de cualquier organización. Adicionalmente, un uso controlado y seguro protege la integridad de los sistemas de información de la entidad frente a riesgos propios y/o de terceros ajenos a la organización. Y la integridad de tales sistemas constituye un activo esencial para el cumplimiento de sus fines fundacionales. También de este modo se protege la misma información corporativa, resulte o no sensible.

Por lo demás, la inadecuada e incontrolada utilización de los medios informáticos suscita un riesgo, por remoto que sea, de comprometer a la Fundación, bien por la posibilidad de atentar contra el derecho a la intimidad de las personas, a la integridad de los sistemas informáticos de terceros, al secreto de las comunicaciones, a los secretos corporativos propios o ajenos o a los derechos de propiedad intelectual e industrial. También, por improbable que resulte la hipótesis, se trata de evitar que los recursos de la entidad estén involucrados en los accesos, descargas o transferencias de materiales de algo riesgo (pornografía infantil, incitación al odio y discriminación, o exaltación del terrorismo).

Considerando los estrictos estándares éticos y de cumplimiento normativo que rigen en CETAQUA, es necesario establecer directrices precisas y fijar del modo más comprensible posible los mecanismos de control que la Fundación puede utilizar para asegurarse un uso adecuado de tales medios. No se trata sólo de prevenir prácticas inapropiadas, abusivas o ilegales, que incluso podrían dar lugar a responsabilidad penal de la misma entidad desde la reforma de 2010. Se trata también de asegurar un uso racional, eficiente y eficaz de los recursos de la entidad, en términos de productividad laboral.

DEFINICIONES

A los efectos previstos en esta instrucción, se entenderá por:

Aplicación informática: Programa o conjunto de programas informáticos que tienen por objeto el tratamiento electrónico de la información.

Red de comunicación: Infraestructura de telecomunicación accesible por los usuarios, tanto de acceso a red interna o intranet como de acceso a red externa o extranet, correo electrónico o email o cualquier otro instrumento de transmisión telemática o acceso a la información, mediante la conexión de medios informáticos, que sean propiedad de la Fundación o sobre los que ostente derechos de uso y control.

Recursos informáticos: cualquier medio o instrumento que interviene en los sistemas de información y en las redes de comunicaciones de la Fundación.

Sistemas de información: los vinculados con la recolección, recuperación, procesamiento, almacenamiento y distribución de los datos relevantes para los procesos implicados en la organización, actividad y funcionamiento de la Fundación.

Usuario: toda persona física que tenga autorizado el acceso a los sistemas de información o redes de comunicaciones de la Fundación, con independencia de la vinculación que tengan con la misma.

AMBITO SUBJETIVO Y OBJETIVO DE APLICACIÓN DE LA INSTRUCCIÓN

La presente instrucción será de aplicación a directivos, empleados y colaboradores de la Fundación y en general a cualquier usuario autorizado a acceder a sus sistemas de información o redes de comunicación, con independencia de la función que ejerza y el tipo de vinculación que tenga con la entidad (laboral, becario, prestación de servicios, etc.)

La presente instrucción será de aplicación para todo uso de los sistemas de información, redes de comunicación, telefonía fija o móvil de la Fundación.

NORMAS DE ACTUACIÓN

NORMAS DE USO DE LOS RECURSOS INFORMÁTICOS

1. Las siguientes normas se aplicarán a todos los ordenadores personales facilitados y configurados por CETAQUA para su utilización por parte de los usuarios, incluyendo equipos de sobremesa, portátiles y dispositivos móviles con capacidades de acceso a los Sistemas de Información de la organización.
2. CETAQUA pone a disposición de los usuarios que así lo precisen los equipos informáticos y dispositivos de comunicaciones, tanto fijos como móviles, necesarios para el desarrollo de su actividad profesional. Así pues, los datos, dispositivos, programas y servicios informáticos dispuestos deben utilizarse para el desarrollo de las funciones encomendadas. Cualquier uso de los recursos con fines distintos a los autorizados está estrictamente prohibido.
3. El ordenador personal (PC) es el recurso informático que permite ordinariamente el acceso de los usuarios a los Sistemas de Información y servicios informáticos de la Fundación constituyendo un elemento esencial en la cadena de seguridad de los sistemas de información. En consecuencia, se velará especialmente por el cumplimiento de las normas respecto a este recurso.
4. Existirá un inventario actualizado de los equipos informáticos, gestionado por la unidad competente. A cada nuevo usuario que se incorpore a la organización y así lo precise, la Fundación le facilitará el alta de nuevo usuario, con configuración de acceso a los servicios y aplicaciones que resulten necesarias para su concreta actividad. La ficha de alta incluirá nombre, apellidos, NIF, área, teléfono y dirección de correo electrónico, servicios a los que requiere acceso, aplicaciones y perfiles, y los datos que adicionalmente resultaren precisos.

5. Los ordenadores personales y demás medios deben utilizarse únicamente para fines propios del desempeño de la función asignada y como herramienta de apoyo a las competencias profesionales de los usuarios autorizados. Únicamente el personal autorizado por CETAQUA podrá distribuir, instalar, desinstalar software y hardware, o modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que puedan repercutir en la seguridad de los Sistemas de Información de la Fundación. Cuando se precise instalar dispositivos no provistos por CETAQUA, deberá solicitarse autorización previa.
6. Está prohibido alterar, sin la debida autorización, cualquiera de los componentes físicos o lógicos de los equipos informáticos y dispositivos de comunicación, salvo autorización expresa de CETAQUA. En todo caso, estas operaciones sólo podrán realizarse por el personal de soporte técnico autorizado.
7. Salvo autorización expresa de la Fundación, los usuarios no tendrán privilegio de administración sobre los equipos.
8. Los usuarios deberán facilitar al personal de soporte técnico el acceso a sus equipos para labores de reparación, instalación o mantenimiento. Este acceso se limitará únicamente a las acciones necesarias para el mantenimiento o la resolución de problemas que pudieran encontrarse en el uso de los recursos informáticos y de comunicaciones, y finalizará completado el mantenimiento o una vez resueltos aquellos.
9. Si el personal de soporte técnico detectase cualquier anomalía que indicara una utilización de los recursos contraria a la presente Instrucción, lo pondrá en conocimiento del Compliance Officer de la Fundación, que tomará las oportunas medidas correctoras.
10. Los ordenadores personales, portátiles y demás medios de la organización habrán de mantener actualizados los parches de seguridad de todos los programas que tengan instalados. Se deberá prestar especial atención a la correcta actualización, configuración y funcionamiento de los programas antivirus y cortafuegos.
11. Los usuarios deberán notificar a la Fundación, a la mayor brevedad posible, cualquier comportamiento anómalo del ordenador que estén utilizando, especialmente cuando existan sospechas de que se haya producido algún incidente de seguridad.
12. El usuario deberá participar en el cuidado y mantenimiento del equipo que utilice, lo tenga o no personalmente asignado, dando cuenta de cualquier circunstancia anómala.
13. El usuario debe ser consciente de las amenazas provocadas por malware. Muchos virus y troyanos requieren la participación de los usuarios para propagarse, ya sea a través de disquetes, CDs/DVDs, memorias USB, tarjetas de memoria flash, discos duros externos o cualquier medio de almacenamiento externo, mensajes de correo electrónico o instalación de programas descargados desde Internet. Es imprescindible, por tanto, vigilar el uso responsable los equipos para reducir este riesgo.
14. El usuario se hace responsable de toda la información extraída con autorización fuera de la organización a través de cualquier sistema de almacenamiento externo que le haya sido asignado. Es imprescindible un uso responsable de los mismos, especialmente cuando se trate información sensible, confidencial o protegida.
15. El cese de actividad de cualquier usuario debe ser comunicada de forma inmediata a la Fundación, al objeto de que le sean retirados los recursos informáticos que en su caso le hubieren sido asignados y darle de baja de credenciales y privilegios de acceso. En caso de que la persona tenga asignado personalmente algún recurso informático (portátil, Tablet, etc.) deberá devolverlo sin demora a la entidad cuando finalice su vinculación con dicho puesto o función.

16. Salvo autorización, está prohibida la ejecución remota de archivos de tipo audiovisual ajena al desempeño profesional.
17. Está igualmente prohibida la conexión a la red informática corporativa de cualquier equipo o dispositivo no facilitado por la Fundación o sin su previa autorización.
18. La utilización de conexiones mediante cable y medios inalámbricos con tecnologías WiFi, Bluetooth o infrarrojos que no estén debidamente autorizados por la Fundación, queda igualmente prohibida.

Los usuarios en ningún caso podrán acceder físicamente al interior de los PC que tengan asignados para el ejercicio de sus funciones, sólo personal autorizado podrá realizarlo para labores de reparación, instalación o mantenimiento.

Los usuarios deberán abstenerse de manipular los mecanismos de seguridad instalados en los PC.

NORMAS SOBRE ALMACENAMIENTO DE INFORMACIÓN

1. La información almacenada de forma local en los ordenadores de los usuarios (disco duro local, por ejemplo) puede ser objeto de salvaguarda mediante procedimiento corporativo de copia de seguridad. En caso contrario, se recomienda que la información almacenada relevante sea asegurada mediante realización periódica de copias de seguridad.
2. CETAQUA puede poner a disposición de ciertos usuarios unidades de red compartidas para contener las salvaguardadas periódicas de sus unidades locales. Debe tenerse en cuenta que tales unidades corporativas son un recurso compartido por todos los usuarios, por lo que sólo deberá salvaguardarse la información que se considere estrictamente necesaria.
3. No está permitido almacenar información privada, de cualquier naturaleza, en los recursos de almacenamientos compartidos o locales, salvo autorización previa y excepcional de la Fundación.

NORMAS DE USO DE APLICACIONES INFORMÁTICAS Y SOFTWARE

1. Cuando utilicen los equipos de la Fundación, los usuarios deben hacer uso exclusivamente de las aplicaciones informáticas o versiones de software instalados en sus equipos, debiendo seguir las instrucciones o normas que la misma establezca para su empleo. Las aplicaciones informáticas tienen una finalidad profesional, por lo que no deben ser utilizadas para uso personal o privado.
2. La Fundación será la responsable de configurar el sistema operativo, definir las aplicaciones informáticas de uso estandarizado y proceder a su instalación o desinstalación. Sólo con autorización expresa, dadas las características o naturaleza de las aplicaciones informáticas, podrán los usuarios efectuar directamente su instalación.
3. En ningún caso podrán los usuarios borrar o desinstalar las aplicaciones informáticas legalmente instaladas en sus equipos por la Fundación.
4. Queda estrictamente prohibida la instalación de aplicaciones informáticas sin la correspondiente licencia o no adecuándose a la legislación vigente.

5. Las aplicaciones informáticas están protegidas por la propiedad intelectual, por lo tanto, queda terminantemente prohibido el uso, reproducción, modificación, transformación, cesión o comunicación sin la debida autorización, con finalidad ajena a la propia de la Fundación.
6. Queda prohibida cualquier actuación que pueda tener consideración de provocadora o intimidatoria en el trabajo, de tal manera que debe excluirse la instalación o visualización de salvapantallas, fotos, vídeos, comunicaciones u otros medios con contenidos ofensivos, violentos, amenazadores, obscenos o, en general, aquellos que agredan la dignidad de la persona.
7. Los usuarios están obligados a cumplir las medidas de seguridad diseñadas por la Fundación, así como las prevenciones que al efecto se establezcan. Por tanto, no podrán desactivar los programas antivirus ni sus actualizaciones, y tampoco podrán introducir voluntariamente programas, virus, macros o cualquier otro dispositivo lógico o secuencia de caracteres, que causen o sean susceptibles de causar alteración o daño en los recursos informáticos de la Fundación o en los de terceros.
8. Los usuarios están obligados a utilizar exclusivamente los programas antivirus y sus respectivas actualizaciones u otros sistemas de seguridad, destinados a la prevención de la entrada en los Sistemas de Información de cualquier elemento destinado a alterar o dañar los recursos informáticos, que sean instalados por la Fundación.

NORMAS DE USO DEL ACCESO A INTERNET

1. El acceso a internet por los usuarios por medio de ordenador o cualquier otro dispositivo de la Fundación se realizará únicamente empleando los medios y a través de la red establecida a estos efectos por la Fundación. No está permitido acceder directamente por cualquier medio de conexión directa a la red a través de un proveedor de servicio de acceso.
2. Las conexiones a internet que se produzcan a través de la red de la entidad tendrán una finalidad profesional. El usuario empleará estas conexiones exclusivamente para el ejercicio de las tareas y actividades que corresponden a las funciones de su puesto de trabajo.
3. Está prohibido el acceso a direcciones de internet que tengan un contenido ofensivo o atentatorio de la dignidad humana. A estos efectos, la Fundación podrá restringir el acceso a determinados servidores de contenidos en internet.
4. Está prohibido el acceso a redes de internet profunda o deep web, tales como la red Tor.
5. La Fundación podrá controlar los accesos a internet. En este sentido, se podrá proceder a monitorizar las direcciones de acceso y el tiempo de conexión de los usuarios a internet, así como la limitación de su uso en razón de las funciones que ejerza, por motivos de seguridad o rendimiento de la red.
6. La Fundación podrá registrar todos los accesos a servidores de la red incluyendo, al menos, la información de: direcciones de páginas visitadas, fecha y hora, ficheros descargados, usuario y puesto desde el que se ha efectuado la conexión.
7. Está prohibida la configuración o utilización sin autorización previa de sistemas proxy, VPN, o cualquier elemento de acceso a internet a través de un intermediario por los usuarios.
8. Las transferencias de datos desde o a internet se realizarán exclusivamente cuando lo exija el ejercicio de las funciones del puesto de trabajo. En todo caso, los usuarios

deberán tener en cuenta, antes de utilizar la información proveniente de la red, si dicho uso es conforme a las normas que protegen la propiedad intelectual e industrial.

9. Está estrictamente prohibido el uso abusivo de internet.

Se considerará abusivo:

- 9.1. El acceso a otras redes de información o a otros equipos, con el propósito de violar su integridad o seguridad, entendiéndose desde la mera búsqueda de vulnerabilidades hasta la intrusión efectiva.
- 9.2. El acceso o visualización de contenidos inapropiados desde el punto de vista ético (pornografía, incitación de la violencia, discriminación, odio, denigración de víctimas del terrorismo y otras).
- 9.3. La realización de cualquier actividad de promoción de intereses personales del usuario.
- 9.4. La publicación o envío de información no solicitada.
- 9.5. La publicación o envío de información sensible, confidencial, protegida o propiedad de la Fundación a personas, empresas o sistemas de información externos no autorizados. En este sentido, los usuarios se comprometen a garantizar la privacidad de estos datos y contraseñas de acceso, así como a evitar la difusión de los mismos.
- 9.6. La publicación o envío de mensajes a través de Internet que contengan amenazas, ofensas o imputación de hechos que puedan lesionar la dignidad personal, así su utilización para acosar y hostigar a compañeros y/o a terceros y, en general, la utilización del servicio de Internet de manera ilegal o infringiendo cualquier norma interna que pudiera resultar de aplicación.
- 9.7. El Empleo de utilidades de intercambio de información en Internet no autorizadas (tales como redes P2P, Torrent, FTP).
- 9.8. El Uso de Internet para propósitos que puedan influir negativamente en la imagen de CETAQUA, de sus patronos, directivos y empleados y de los organismos públicos o privados con los que se mantiene relación.
- 9.9. El acceso a Internet para el uso de mensajería instantánea (Whatsapp Web, Messenger, Skype, etc.) por motivos no profesionales. Esto aplica también a dispositivos móviles facilitados y propiedad de CETAQUA.
- 9.10. La descarga o transferencia de ficheros no relativa a las actividades profesionales del usuario (tales como programas, juegos, ficheros de sonido, fotos, videos o películas, libros, etc.).
- 9.11. Sin perjuicio de todo lo anterior, las consultas no esporádicas, sino prolongadas o recurrentes en internet sin justificación profesional.
- 9.12. El juego on line y la participación en foros, chats, y secciones de comentarios u opinión
- 9.13. El uso de redes sociales sin autorización expresa de la Fundación
- 9.14. El acceso a máquinas terceras sin autorización, por ejemplo, a través de servicios como SSH, FTP, escritorio remoto, y otros

NORMAS DE USO DEL CORREO ELECTRONICO

1. La Fundación suministrará a cada usuario una dirección individual de correo electrónico, procediéndole a instalar y configurar una cuenta de correo. El acceso a dicha cuenta de correo se efectuará mediante una clave personal.
2. Los usuarios tienen prohibido el uso en las redes de comunicación propias de la entidad de otras cuentas de correo electrónico distintas a las facilitadas por la Fundación.
3. El uso por los usuarios del correo electrónico habilitado por la Fundación es estrictamente profesional, vinculado con el ejercicio de las funciones que corresponde al puesto de trabajo que desempeñe.
4. Los usuarios tienen prohibido expresamente el acceso a cuentas de correo que no le hayan sido asignadas. Para que un usuario distinto pueda acceder a una cuenta de correo será preciso que el titular de ésta lo autorice por escrito, salvo los supuestos de cuentas de correo asociadas a puestos singulares.
5. Los usuarios no deben interceptar, leer, borrar, copiar o modificar el correo electrónico dirigido a otros usuarios.
6. Con la finalización de la relación del usuario con la Fundación se interrumpirá el acceso a la cuenta de correo del usuario.
7. Está estrictamente prohibido el uso abusivo del correo electrónico.
Se considerará uso abusivo de correo electrónico.
 - 7.1. El uso recurrente del correo para fines personales, distintos a los derivados de las actividades profesionales del usuario.
 - 7.2. En todo caso, el envío de correos electrónicos con contenido inadecuado, ilegal, ofensivo, difamatorio, inapropiado o discriminatorio por razón de sexo, raza, edad, discapacidad, o de cualquier otro modo atentatorio de la dignidad
 - 7.3. En todo caso el envío deliberado de ficheros con software no licenciado, virus y códigos maliciosos, de alerta de virus falsos o cualquier otro contenido que pueda perjudicar a los usuarios.
 - 7.4. La difusión de la cuenta de correo corporativa del usuario en listas de distribución, foros, servicios de noticias, etc., que no sean consecuencia de la actividad profesional del usuario, así como la realización de cualquier actividad de promoción de intereses profesionales personales ajenos a la Fundación.
 - 7.5. El uso de cualquier la cuenta de correo de la Fundación para enviar mensajes o cartas en cadena y/o correos basura o spam (correo electrónico no solicitado).
 - 7.6. El uso de cualquier cuenta de correo de la Fundación para enviar mensajes que contengan amenazas, ofensas o imputación de hechos que puedan lesionar la dignidad personal y, en general, la utilización del correo electrónico de manera ilegal o infringiendo cualquier norma que pudiera resultar de aplicación.
 - 7.7. Revelar a terceros el contenido de cualquier dato reservado o confidencial propiedad de la Fundación o de terceros, salvo que tal actuación fuera realizada en cumplimiento de fines estrictamente profesionales con el previo consentimiento de los afectados.
 - 7.8. Utilizar el correo para propósitos que puedan influir negativamente en la imagen de la Fundación, de su patronato, directivos, empleados, o de los organismos públicos o privados con los que se mantiene relación.

8. No está permitido el uso del correo corporativo para recoger correo de buzones que no pertenezcan a la Fundación, así como el reenvío automático del correo corporativo a buzones ajenos a la organización, salvo que se cuente con autorización expresa.
9. No está permitido el envío de mensajes de correo a múltiples usuarios sin proteger debidamente la identidad de los receptores, mediante la ocultación de las direcciones de recepción usando los campos CCo (con copia oculta)
10. Las acciones realizadas desde una cuenta de usuario o desde una cuenta de correo electrónico de usuario son, salvo prueba en contra, responsabilidad de su titular.

NORMAS SOBRE ACCESO Y USO DE SISTEMAS DE INFORMACIÓN Y A DATOS TRATADOS

1. Los datos gestionados por CETAQUA y tratados por cualquier Sistema de Información de la Fundación, deben tener asignado un responsable, que será el encargado de conceder, alterar o anular la autorización de acceso a dichos datos por parte de los usuarios.
2. Para acceder a los recursos informáticos es necesario tener asignada previamente una cuenta de usuario y estar dado de alta en los servidores de dominio. La autorización del acceso establecerá el perfil necesario con el que se configuren las funcionalidades y privilegios disponibles en las aplicaciones según las competencias de cada usuario, adoptando una política de asignación de privilegios mínimos necesarios para la realización de las funciones encomendadas.
3. Es responsabilidad del usuario hacer buen uso de su cuenta de usuario. La cuenta se podrá desactivar en caso de mala utilización.
4. Los usuarios tendrán autorizado el acceso únicamente a aquella información y recursos que precisen para el desarrollo de sus funciones. El acceso a la información será personal y las credenciales de acceso, intransferibles.
5. Cuando un usuario deje de atender un PC durante un cierto tiempo, es necesario bloquear la sesión de usuario, para evitar que ninguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlo. Deberá salvaguardar cualquier información, documento, soporte informático, dispositivo de almacenamiento extraíble, etc., que pueda contener información confidencial o protegida frente a posibles revelaciones o robos de terceros no autorizado
6. La baja de los usuarios será inmediatamente comunicada a para proceder a la eliminación efectiva de los derechos de acceso y los recursos informáticos asignados al mismo.
7. Como medida de protección de la información propia, confiada o tratada por la Fundación, está absolutamente prohibido el envío al exterior de información, electrónicamente, mediante soportes informáticos o por cualquier otro medio, que no hubiere sido previamente autorizada por la Fundación.
8. Todo el personal de la organización o ajeno a la misma que, por razón de su actividad profesional, hubiera tenido acceso a información gestionada por CETAQUA (tal como datos personales, documentos, metodologías, proyectos, claves, análisis, programas, etc.) deberán mantener sobre ella, por tiempo indefinido, una total reserva mientras la no se autorice su divulgación.

9. En el caso de entrar en conocimiento de información que no sea de libre difusión, en cualquier tipo de soporte, deberá entenderse que dicho conocimiento es estrictamente temporal mientras dure la función encomendada, con la obligación de secreto o reserva indefinidas y sin que ello le confiera derecho alguno de posesión, titularidad o copia del mismo. Asimismo, se deberán devolver los soportes de información utilizados inmediatamente después de la finalización de las tareas que hubieren originado su uso.
10. Los usuarios sólo podrán acceder a aquella información para la que posean las debidas y explícitas autorizaciones, en función de las labores que desempeñen, no pudiendo en ningún caso acceder a información perteneciente a otros usuarios o grupos de usuarios para los que no se posea tal autorización.
11. Los derechos de acceso a la información y a los Sistemas de Información que la tratan deberán siempre otorgarse en base a los principios de mínimo privilegio posible y necesidad de conocer.
12. La información contenida en los Sistemas de Información de la CETAQUA es de su propiedad, por lo que los usuarios deben abstenerse de comunicar, divulgar, distribuir o poner en conocimiento o al alcance de terceros (externos o internos no autorizados) dicha información, salvo autorización expresa.
13. Se evitará almacenar información sensible, confidencial o protegida en medios desatendidos (tales como CDs, DVDs, memorias USB, dispositivos de almacenamiento externo en general, listados, etc.) o dejar visible tal información en la misma pantalla del ordenador.
14. Todo lo anterior se entenderá sin perjuicio del estricto cumplimiento de la normativa aplicable en materia de protección de datos de carácter personal.

MONITORIZACIÓN Y CONTROL DE CUMPLIMIENTO DE ESTA NORMATIVA

1. Con la finalidad exclusiva de asegurar el cumplimiento de dichas normas, la entidad
 - a) Revisará periódicamente el estado y seguridad de los equipos, el software instalado, los dispositivos y redes de comunicaciones de su titularidad.
 - b) Monitorizará los accesos a los equipos proporcionados, a las redes de comunicaciones, y a la información contenida en sus sistemas.
 - c) Auditará la seguridad de las credenciales de acceso proporcionadas.
 - d) Monitorizará el tráfico a los servicios de internet, correo electrónico y otras herramientas de colaboración.
 - e) Podrá bloquear la instalación de aplicaciones y programas no instalados de serie en los equipos proporcionados.
 - f) Podrá bloquear el acceso a cualquiera de las herramientas que permitan la administración de los equipos proporcionados (panel de control, terminal de comandos, etc.).

- g) Podrá bloquear el acceso a las herramientas de seguridad instaladas de serie en los equipos proporcionados (antivirus, cortafuegos, etc.).
 - h) Podrá bloquear la utilización de puertos de salida y de entrada correspondientes a servicios no autorizados mediante la configuración de los cortafuegos del equipo.
2. La Fundación llevará a cabo esta actividad de control de manera proporcional al riesgo, y de acuerdo con las cautelas legal y jurisprudencialmente exigidas, con plena observancia de los derechos de los usuarios. El acceso al contenido de los mensajes de correos electrónicos sólo procederá en casos indicios fundados de abuso grave y cuando no resulte suficiente la simple monitorización de los datos asociados al proceso de comunicación.
 3. Los sistemas en los que se detecte un uso inadecuado o en los que no se cumplan los requisitos mínimos de seguridad, podrán ser bloqueados o suspendidos temporalmente. El servicio se restablecerá cuando la causa de su inseguridad o degradación desaparezca. Todos los empleados de la Fundación velarán por el cumplimiento de la presente Instrucción e informarán al CO sobre los incumplimientos detectados, y a los responsables técnicos competentes las deficiencias de seguridad observadas, para que se tomen las oportunas medidas.
 4. El sistema que proporciona el servicio de correo electrónico podrá, de forma automatizada, rechazar, bloquear o eliminar parte del contenido de los mensajes enviados o recibidos en los que se detecte algún problema de seguridad o de incumplimiento de la presente Normativa. Se podrá insertar contenido adicional en los mensajes enviados con objeto de advertir a los receptores de los mismos de los requisitos legales y de seguridad que deberán cumplir en relación con dichos correos.
 5. El sistema que proporciona el servicio de navegación podrá contar con filtros de acceso que bloqueen el acceso a páginas web con contenidos inadecuados, programas lúdicos o páginas potencialmente inseguras. Igualmente, el sistema podrá registrar y dejar traza de las páginas a las que se ha accedido, así como del tiempo de acceso, volumen y tamaño de los archivos descargados. El sistema permitirá el establecimiento de controles que posibiliten detectar y notificar a la Fundación sobre usos prolongados e indebidos del servicio.

NO EXPECTATIVA DE PRIVACIDAD

La implantación y difusión de la presente instrucción, pretende delimitar claramente los límites que la Fundación establece en el uso de los medios, sistemas informáticos y redes de comunicaciones puestos a disposición de los usuarios, al objeto de que éstos no abriguen falsas expectativas de privacidad cuando utilizan estos medios.

EXIGENCIA DE RESPONSABILIDADES

Cuando se detecte en el uso de los medios informáticos actuaciones irregulares, ilícitas o ilegales, se procederá al ejercicio de las acciones pertinentes para las exigencias de las responsabilidades disciplinarias o incluso legales que correspondan.

DIFUSIÓN Y CONOCIMIENTO DE LA INSTRUCCIÓN

Todos los usuarios de los sistemas de información, redes de comunicaciones y medios informáticos que sean propiedad o estén bajo la supervisión de la Fundación están obligados al conocimiento y cumplimiento de las presentes instrucciones.

La Fundación asegurará la divulgación y conocimiento de la misma por parte de todos los usuarios, valiéndose para ello de cuantos medios informativos estén a su alcance.

NOTA: Estas Instrucciones de uso de los medios informáticos han sido aprobadas,

Por el Patronato de CETAqua, Centro Tecnológico del Agua, Fundación Privada en fecha 8 de noviembre de 2019.

Por el Patronato de Fundación Centro Gallego de Investigaciones del Agua en fecha 13 de noviembre de 2019.

Por el Patronato de Centro Andaluz de Investigaciones del Agua, Fundación Privada en fecha 27 de noviembre de 2019.