POLÍTICA DE LA TECNOLOGÍA DE LA INFORMACIÓN

ASOCIACIÓN EDUCACIÓN Y CULTURA

Cuadro Gestión Documental de Revisiones

Versión	Fecha	Cambios	Autor	Revisado por	Aprobado por	Nombre del Documento
1.00	31/102025	Creación	MARIA CONCEPCION MARTINEZ MARTINEZ Firmado digitalmente por MARIA CONCEPCION MARTINEZ MARTINEZ Fecha: 2026.02.19 11:46:39 +01'00' Fdo: M Concepción Mtnez Mtnez	08994333E NURIA ANGULO (R: B87060109) Firmado digitalmente por 08994333E NURIA ANGULO (R: B87060109) Fecha: 2026.04.22 10:12:56 +02'00' Fdo: ADcuatro	25988017H MARÍA DOLORES CARRILLO (R: G28375574) Firmado digitalmente por 25988017H MARÍA DOLORES CARRILLO (R: G28375574) Fecha: 2026.02.19 11:45:42 +01'00' Fdo: Junta Directiva	POLÍTICA TIC_31oct25_V01.00

ÍNDICE

1. Introducción

La presente política recoge la normativa y procedimientos de la Asociación Educación y Cultura, (en adelante "la AEC"), en relación con las herramientas que utiliza el personal en el desarrollo de sus actividades en la AEC, con el objetivo de crear una cultura de actuación acorde a la legalidad y evitar así cualquier tipo de conductas delictivas que pudieran darse en relación con dichos medios.

Debido a que en las entidades es cada vez mayor la utilización de las nuevas tecnologías, es necesario el control de estas herramientas. No obstante, ello puede suponer una quiebra de la intimidad del personal constitutivo de un delito contra la intimidad. Aun así, este derecho a la intimidad del personal debe conciliarse con los derechos e intereses legítimos de la AEC, como el derecho a velar por la eficacia de la entidad y protegerse del perjuicio que pudiera ocasionar a la misma las acciones del personal.

Es necesario hacer una breve referencia a la normativa y jurisprudencia existente en esta materia:

1. **El Convenio Europeo para la Protección de los Derecho Humanos** establece que toda persona tiene derecho al respeto de la vida privada y familiar y prohíbe la injerencia que no esté prevista en la ley y que no se justifique por razones de seguridad, bienestar económico, defensa del orden, prevención de las infracciones penales, protección de la salud, de la moral o de los derechos y libertades de los demás.
2. **La Constitución Española,** recoge como derecho fundamental el derecho a la intimidad personal y familiar y a la propia imagen, así como el secreto de las comunicaciones.
3. **El Estatuto de los Trabajadores en su art. 20** dispone que el empleador podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad humana y teniendo en cuenta la capacidad real de los trabajadores disminuidos, en su caso.

Los Tribunales han interpretado esta cuestión y, como ejemplo, la sentencia del Tribunal Supremo de 26 de septiembre de 2007 (Sala de lo Social) establece lo siguiente:

"...las medidas· de control sobre los medios informáticos puestos a disposición de los trabajadores se encuentran, en principio, dentro del ámbito normal de esos poderes: el ordenador es un instrumento de producción del que es titular el empresario como propietario o por otro título y éste tiene, por tanto, facultades de control de la utilización, que incluyen lógicamente su examen. Por otra parte, con el ordenador se ejecuta la prestación de trabajo y, en consecuencia, el empresario puede verificar en él su correcto cumplimiento, lo que no sucede en los supuestos del artículo 18, pues incluso respecto a la taquilla, que es un bien mueble del empresario, hay una cesión de uso a favor del trabajador que delimita una utilización por éste que, aunque vinculada causalmente al contrato de trabajo, queda al margen de su ejecución y de los poderes empresariales del artículo 20 del Estatuto de los Trabajadores para entrar dentro de la esfera personal del trabajador.... Se trata de medios que son propiedad de la Institución y que ésta facilita al trabajador para utilizarlos en el cumplimiento de la prestación laboral, por lo que esa utilización queda dentro del ámbito del poder de vigilancia de empresario que, como precisa el artículo 20.3 del Estatuto de los Trabajadores , implica que éste "podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales", aunque ese control debe respetar "la consideración debida" a la "dignidad" del trabajador".

Asimismo, la mencionada sentencia estableció que existe un hábito social generalizado de tolerancia con ciertos usos personales moderados de los medios informáticos y de comunicación facilitados por la AEC al personal. Esta tolerancia crea una expectativa de confidencialidad que debe ser tenida cuenta. Por ello, dispone a continuación que las entidades deben fijar previamente las reglas de uso de los instrumentos de trabajo (p. ej.: estableciendo prohibiciones absolutas o parciales, o permitiendo el uso personal por parte del personal) y se debe informar al personal de cuáles son esas reglas, de los controles y medidas aplicables por parte de la AEC. De este modo desaparece la expectativa de intimidad del personal sobre esos medios y su control no debería generar un posible delito contra la intimidad.

Aunque esta doctrina se ha flexibilizado en virtud de sentencias posteriores del Tribunal Supremo y del Tribunal Constitucional, es recomendable que las entidades jurídicas dispongan de un protocolo de actuación en materia de uso de Tecnologías de la Información y Comunicación (en adelante "TIC").

2. Objetivo y alcance

La política de uso de las herramientas TIC de la AEC persigue garantizar la seguridad en la utilización de los sistemas de información y de las comunicaciones, establecer los sistemas de control y las consecuencias que el incumplimiento de esta tiene para el personal.

Las normas contenidas en el presente protocolo son de obligado cumplimiento por parte de todo el personal de la AEC y su vulneración podrá conllevar acciones disciplinarias.

La AEC implementará las medidas necesarias para llevar a cabo un adecuado control sobre el cumplimiento y respeto de la política de uso de las herramientas TIC.

3. Políticas

La AEC es una entidad concienciada con la seguridad de sus sistemas de información y vela por el mantenimiento de su seguridad. Asimismo, pretende estar alineada con el cumplimiento de la legalidad y, en concreto:

- Todos los datos procesados por los equipos, infraestructuras, aplicaciones y sus resultados son propiedad de la AEC.
- El uso de las TIC será controlado tanto por motivos de seguridad como por motivos de control de la actividad que realiza el personal.
- El sistema de control se basará en un sistema proporcional basado en herramientas y medios que permitan sistemas de control lo menos invasivos posible.
- Se podrán adoptar las medidas legales oportunas frente al incumplimiento de estas políticas y, en general, frente al incumplimiento de la legalidad vigente.

Esta política se basa en las siguientes premisas:

- ✓ Respeto a las normas vigentes en materia de protección de datos. Desarrollo de procedimientos y adopción de medidas para el cumplimiento de las obligaciones que afectan a datos personales.
- ✓ Diseño de un plan de mejora continua de los procedimientos adoptados.
- ✓ Mediante la presente política la AEC pretende establecer un sistema de uso y control del conjunto de las tecnologías de la información que se utilizan por parte del personal de la AEC.

Asimismo, se pretende regular el control por parte de la AEC para que se produzca sin quebranto de la intimidad del personal y del derecho al secreto de las comunicaciones, esto es, su esfera de privacidad, para evitar la comisión de delitos contra la intimidad.

4. Principios generales

Este apartado regula cuales son los principios sobre la vigilancia, control del correo electrónico y el uso de internet en la AEC. Para que la actividad de control por parte de la AEC y esté justificada deben respetarse los principios de protección de datos personales. Estos serían:

1º.- Necesidad: La AEC, antes de proceder a realizar esta actividad de control, debe comprobar si el mecanismo de vigilancia que ha de llevar a cabo es necesario para el caso concreto. Siempre será más apropiado, de ser posible, la utilización de medios más comunes y de menor injerencia en la privacidad del personal, debiendo recurrir a la vigilancia del correo electrónico o uso de internet en circunstancias excepcionales.

2º.- Finalidad: Debe existir un objetivo o fin determinado previo al inicio de la actividad de control y recogida de datos, y este fin debe ser legítimo. Los datos obtenidos deberán utilizarse única y exclusivamente para este fin concreto.

Ej. El tratamiento de los datos puede realizarse a efectos de seguridad del sistema, pero estos datos no podrán utilizarse para supervisar el comportamiento del personal.

3º.- Transparencia: La AEC debe indicar de forma clara y abierta sus actividades. Ello implica que la AEC debe:

- Haber informado al personal de la política existente relativa a la vigilancia del correo electrónico y de la utilización de Internet.
- Debe comunicar a su personal en qué medida pueden utilizar los sistemas de comunicación con fines privados o personales.
- Determinar en qué circunstancias la AEC puede adoptar medidas de vigilancia.
- Informar al personal de las medidas de vigilancia adoptadas.
- Debe informarse al personal de quien se trate, de cualquier abuso de las comunicaciones electrónicas detectado, salvo que las circunstancias justifiquen la continuación de la vigilancia.

4ª.- Legitimidad. La operación de vigilancia y control de los datos únicamente puede realizarse si la finalidad es legítima. Por ejemplo; control del personal por parte de la AEC para evitar la transmisión de información confidencial.

5ª.- Proporcionalidad. Los datos que se utilicen deben ser adecuados, pertinentes y no excesivos en relación con los fines para lo que se han recabado, teniendo en cuenta el tipo y grado de riesgo al que se enfrenta la AEC.

6ª.- Exactitud y conservación de los datos. Los datos recopilados deben ser precisos y no almacenarse más del tiempo estrictamente necesario. Se establece un periodo de conservación de los mensajes electrónicos por un periodo de 1 año.

7º.- Seguridad. Es necesario que la AEC adopte medidas técnicas y organizativas adecuadas para proteger todos los datos personales que se hallen en su poder de toda intromisión exterior. La persona que durante las operaciones de control acceda a los datos personales del personal debe estar sometida a una obligación estricta del secreto profesional respecto a la información confidencial a la que va a acceder.

5. Control del correo electrónico

5.1. Normas de uso

Se considera correo electrónico corporativo tanto el interno, entre terminales de la red corporativa, como el externo, dirigido o proveniente de otras redes públicas o privadas y, especialmente, internet. En la utilización del correo electrónico, la AEC adopta un modelo de uso no abusivo o desmedido.

Este servicio, en todo caso, no deberá ser utilizado para realizar las siguientes actividades:

1. Enviar mensajes con contenidos o ficheros adjuntos ofensivos o inapropiados que puedan considerarse, para quien los recibe, un atentado contra su intimidad personal, honor o dignidad, absteniéndose de efectuar referencias peyorativas de carácter personal en relación con la ideología, religión, creencias, afiliación política o sindical, o realizar comentarios basados en el género, edad, raza, preferencias sexuales, discapacidades físicas o psíquicas, o en la apariencia de las personas.
2. Enviar mensajes y/ o documentos corporativos a cuentas privadas del personal para uso no vinculado a su actividad, o a cuentas externas de sus familiares o amigos.
3. Enviar o reenviar mensajes de correo en cadena o de tipo piramidal, sin permiso del Órgano de representación.

Se establecen las siguientes normas:

1. El correo electrónico sea cual fuese la dirección asignada, se configura como una herramienta de trabajo no exclusiva, colectiva y de libre acceso, asignada al proyecto o centro que titula la AEC. No se atribuirá con el nombre del personal.
2. Queda prohibido el uso de este para fines no relacionados con las funciones que tiene encomendadas el personal.
3. El empleo del nombre o apellidos del personal junto al dominio de la AEC en la dirección de correo no significa la asignación por la AEC de un correo personal.

4. Se podrá realizar copia de seguridad de los emails y acceder al contenido de estos ante problemas técnicos o de seguridad o cuando existan sospechas de que no se cumplen estas normas.
5. No se permiten el uso de cuentas de correo distintas a las proporcionadas por la AEC.
6. No está permitido manipular las cabeceras de los correos electrónicos con la finalidad de ocultar o falsear la identidad del remitente del mensaje.
7. El correo electrónico es una de las fuentes más importantes de difusión de virus, por lo que se recomienda no abrir mensajes sospechosos, ni clickear sobre enlaces cuyo origen pueda ser sospechoso.

5.2. Controles

La AEC podrá controlar el uso del correo electrónico mediante un sistema de dos niveles:

- Un primer nivel de control de tráfico y de archivos adjuntos.
- Un segundo nivel de control de contenidos.

La AEC podrá utilizar también sistemas de control de correos basados en palabras clave u otros sistemas que estime oportunos siempre que esté justificado. Para que la AEC pueda proceder al control del correo electrónico del personal, éstos deben haber otorgado su consentimiento. No obstante, este consentimiento no puede ser utilizado como medio general para legitimar estos controles.

El personal tiene el derecho fundamental, reconocido en la Constitución, al secreto de la correspondencia. Si el personal dispone de cuentas de correo electrónico personal o correo web, el acceso a los mismos por parte de la AEC solo podría justificarse en circunstancias muy limitadas, pues prevalecería el derecho fundamental al secreto de correspondencia. Si la AEC fomentara la utilización del correo web para asuntos personales, se facilitaría la distinción entre el correo de uso profesional y el correo de uso privado, y reduciría el riesgo de intromisión de la AEC en la vida privada del personal, siempre que los servidores de correo web cuenten con un sistema adecuado

de protección de datos de carácter personal. Por lo tanto, deberá analizarse caso por caso.

A pesar de ello es necesaria una información mínima que debe poseer el personal y que se les debe facilitar: A DETERMINAR

- Reglas sobre el acceso al contenido del correo electrónico y las finalidades específicas de este acceso.
- Indicar periodo de conservación de las copias de seguridad de los mensajes.
- Precisar cuándo se borran definitivamente los correos electrónicos del servidor.
- Cuestiones de seguridad.

6. Control de acceso a internet

Los medios técnicos que utiliza el personal, unos son propiedad de la AEC y otros, propiedad del personal.

La AEC es quien debe decidir si autoriza la utilización privada de internet y en qué medida. Si la AEC decidiera controlar la utilización de internet, implementaría medios técnicos para prevenir la utilización abusiva de internet, por ej.: limitando accesos o utilizando avisos o advertencias automáticas.

En todo caso, y cuando se lleven a cabo actividades de control, la medida de control debe ser proporcional al riesgo que corra la entidad. En muchas ocasiones, basta con llevar a cabo comprobaciones generales, por ejemplo, la elaboración de un listado de los sitios más visitados para comprobar si se está llevando a cabo una utilización abusiva de internet, sin analizar el contenido de los sitios visitados.

Si a través de comprobaciones generales se detecta la posible utilización abusiva de Internet, la AEC podría considerar la posibilidad de realizar otros controles.

En todo caso, deberá comunicarse al personal los resultados obtenidos y ofrecerle la posibilidad de defender una correcta utilización de Internet.

La información mínima que deben recibir el personal en relación a la utilización de internet es la siguiente:

- En qué condiciones se autoriza la utilización de Internet con fines privados.
- Restricciones existentes, como elementos que no pueden ser visualizados o copiados.
- Precisarse el control que puede realizar o realizará la AEC.
- En qué condiciones se autoriza el uso de internet con fines privados.
- Restricciones existentes, si existen restricciones de visualizaciones o copiados.
- Informar sobre el control que FV puede realizar o realizará.
- Uso que se llevará a cabo con los datos recogidos.

El uso a internet estará limitado exclusivamente por la necesidad de acceso que requiera el desarrollo de la función del personal. Debe entenderse que internet es una herramienta estrictamente de trabajo y no deberá ser utilizada para fines ajenos a las funciones desarrolladas por el personal y encomendadas por la AEC.

Tampoco estará permitido el uso del correo electrónico personal, redes sociales, chats o la instalación de cualquier tipo de software ajeno a la actividad desarrollada por el personal sin la debida autorización del Órgano de representación.

6.1. Normas de uso

Queda prohibido:

- El uso de este para fines no relacionados con las funciones laborales encomendadas.
- Debates en tiempo real (Chat), redes sociales, sistemas de mensajería instantánea tipo Messenger, así como la instalación de programas P2P (Peer-to-Peer) y de cualquier otro tipo de acceso a entornos o plataformas ·de intercambio de ficheros.
- Páginas de ocio, entretenimiento o webs de contenido sexual, xenófobo o que inciten a la violencia.

6.2. Controles

La AEC podrá controlar el uso del acceso a Internet proporcionado mediante un control de las páginas visitadas, almacenamiento y control de las cookies, y su utilización en procedimientos disciplinarios o en cualquier orden administrativo o judicial.

La AEC también podrá utilizar otros sistemas de control de la navegabilidad que estime oportunos.

La AEC autoriza la utilización privada de internet en la medida de uso razonable. En el supuesto que hubiera un cambio de política respecto a esta permisión, es recomendable la implementación de medios técnico para prevenir la utilización abusiva de internet, como por ejemplo limitando accesos o utilizando avisos o advertencias automáticas.

Si a través de comprobaciones generales se detecta la posible utilización abusiva de internet, la AEC podría considerar la posibilidad de realizar otros controles. En todo caso, deberá comunicarse al personal y ofrecerle la posibilidad de defender una correcta utilización de internet.

7. Dispositivos de almacenamiento externo

7.1. Normas de uso

- ✓ El personal no puede técnicamente utilizar dispositivos de almacenamiento externo, salvo en los casos en que se autorice expresamente por escrito y se adopten las debidas medidas de seguridad.
- ✓ La información que se contenga en dichos dispositivos, contenga o no, datos de carácter personal, se mantendrá cifrada.

7.2. Controles

La AEC podrá controlar el uso de los dispositivos externos, incluso el contenido de estos, mediante el sistema que estime oportuno.

8. Aplicaciones

No se podrán descargar o utilizar programas que no estén previa y expresamente autorizados por la AEC.