Unidad de Protección de Datos
Colegio de Santo Tomás
Plaza de Cervantes, 10
28801 Alcalá de Henares – Madrid
Tfno. 91 885 6473
protecciondedatos@uah.es

CIRCULAR INFORMATIVA

Sobre la Autenticación por Múltiple Factor (MFA) para asegurar los sistemas, servicios e información que maneja la Universidad

19-12-2022

Desde los Servicios Informáticos llevan varios meses anunciando la puesta en marcha de la Autenticación por Múltiple Factor (MFA) como uno de los medios a utilizar, entre otros, para asegurar todos los sistemas, servicios e información que maneja la Universidad de Alcalá. La UAH debe tomar las decisiones necesarias para protegerse de los ciberataques, que desgraciadamente, son cada día más usuales y que ya han sufrido algunas Universidades de nuestro país, como la UCLM o la UAB, u otros organismos como el SEPE, por ejemplo.

La utilización del MFA, como se explicaba, es una de estas medidas de seguridad utilizadas para proteger a la UAH. La necesidad de utilizar la MFA o simplemente el doble factor de autenticación (2FA) viene determinado por el **Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad** que establece, en lo relacionado con los mecanismos de autenticación para usuarios de la organización [op.acc.6], que para el acceso a sistemas de nivel medio –que es el que tienen los sistemas de información de la Universidad– desde o a través de zonas no controladas, se requerirá de un doble factor de autenticación [op.acc.6.r8.1]. Las personas usuarias de la organización a estos efectos son todo el personal del organismo, ya sea propio o contratado, estable o circunstancial, que pueda tener acceso a información contenida en los sistemas.

La seguridad de la información y los sistemas debe mantenerse dentro del entorno de la Universidad, que ya posee los medios de ciberseguridad necesarios –aunque hay que advertir que cada día se necesitan más, puesto que la ciberdelincuencia tienen progresivamente más medios y están más preparados–, pero la UAH también tiene que disponer de una política de protección de la información para situaciones de movilidad, como sería el trabajo a distancia, normalmente el domicilio u otras instituciones universitarias y/o centros de investigación. Este trabajo “en casa” –en ubicación diferente al lugar habitual de trabajo– puede entenderse como el teletrabajo para el PAS o el trabajo del PDI.

Unidad de Protección de Datos
Colegio de Santo Tomás
Plaza de Cervantes, 10
28801 Alcalá de Henares – Madrid
Tfno. 91 885 6473
protecciondedatos@uah.es

Para conseguir que la 2FA funcione tanto dentro como fuera del entorno de la Universidad, es necesario utilizar un teléfono para enviar el código de autenticación que se usará como doble factor de autenticación además del uso del usuario/contraseña. Se ha solicitado el teléfono móvil, pero también funcionará en el teléfono fijo del trabajo. Por tanto, **si no se quiere proporcionar el teléfono móvil, hay otra posibilidad para usar la 2FA.** Cuando se quiera utilizar el correo fuera del entorno del trabajo, se podrá hacer uso del teléfono fijo utilizando (a su vez) el teléfono software o softphone, que tendría que instalarse en el ordenador o Tablet del personal [medios propios o titularidad de la UAH]. Mediante el softphone se pueden mantener las llamadas telefónicas entrantes y salientes dirigidas al teléfono fijo del puesto de trabajo, y también se podrá realizar la doble autenticación ya que, en el caso de que el mensaje que se reciba en el softphone, pida pulsar una tecla (normalmente "#") el softphone y el móvil deberían generar el mismo código, según nos indican desde los Servicios Informáticos[1].

En fin, respecto del uso del teléfono personal (móvil) antes señalado, hay que decir que la normativa legal no prevé expresamente que el empresario pueda obligar –o no pueda hacerlo– a sus trabajadores y trabajadoras a aportar un dispositivo propio[2]**.** Sin embargo, la Jurisprudencia sí ha señalado en doctrina reiterada[3] que, por una parte, la empresa no puede obligar (salvo pacto individual en contrario) a su personal a aportar un móvil propio que contravenga la ajenidad [en los

[1] Para solicitar el softphone o teléfono virtual e instalarlo en el equipo informático o tablet, deberán seguirse las instrucciones recogidas en la página web de los SSII (https://www.uah.es/es/conoce-la-uah/organizacion-y-gobierno/servicios-universitarios/servicios-informaticos/catalogo-de-servicios/otros-servicios/trabajo-en-remoto/), que es el procedimiento que hasta la fecha ya ha seguido el PAS que teletrabaja. Para responder cualquier duda o atender posibles problemas hay que ponerse en contacto directamente con el CAU de la UAH: cau@uah.es

[2] Los artículos 87 y 88 de la LOPDGDD regula el derecho a la intimidad y el uso de dispositivos digitales en el ámbito laboral. Con la aprobación de la Ley Orgánica en 2018 se introdujeron (nuevos) derechos sobre desconexión digital e intimidad/honor, etc.

[3] Entre otras, Sentencia del Tribunal Supremo (social) de 21 de septiembre de 2015 [Rec. Núm. 259/2014]. El Supremo entiende entonces que el número de teléfono y el correo electrónico personal no forman parte de los datos que deben considerarse *imprescindibles* para el desarrollo del trabajo ya que las relaciones laborales funcionaban sin ellos hace unos años. Ahora bien, también señala que sería deseable que en la actualidad [ya en 2015, antes de promulgarse el RGPD y la LOPDGDD] "de progresiva pujanza telemática en todos los ámbitos" se facilitasen esos datos a la empresa, siempre de forma voluntaria; el correo y el móvil no son necesarios para el mantenimiento o el cumplimiento del contrato de trabajo y, por tanto, no pueden ser de cesión obligatoria, y de ahí que estén especialmente amparados por la normativa de protección de datos. Por todas, más recientemente, STS de 8 de febrero de 2021 (Rec. Núm. 84/2019) y SAN de 27 de junio de 2022 (Rec. Núm. 128/2022).

Unidad de Protección de Datos
Colegio de Santo Tomás
Plaza de Cervantes, 10
28801 Alcalá de Henares – Madrid
Tfno. 91 885 6473
protecciondedatos@uah.es

medios de producción] que caracteriza las relaciones laborales subordinadas/asalariadas[4]. Y, por otro lado, tampoco se puede someter el dispositivo móvil personal al control empresarial habitual como sí podría hacerse cuando la empleadora proporciona los medios necesarios para el trabajo. En todo caso, en cualquiera de los dos supuestos, entra en conflicto el poder empresarial de control y supervisión (poderes de dirección, organización y disciplinario) y el derecho a la intimidad de la persona trabajadora; en el caso de dispositivos móviles particulares, siempre se va a requerir el consentimiento del personal para acceder a ellos y a la información relativa al trabajo.

En suma, los dispositivos móviles [portátiles, tablets y smartphones] ya son parte de las relaciones laborales y herramientas que puestas al servicio del personal para que desempeñen su trabajo. A tal fin, para evitar dudas (problemas o malentendidos) sobre la utilización de estos dispositivos en el puesto de trabajo –sean facilitados por la universidad o propiedad de la persona trabajadora– se recomienda establecer una **Política de uso de dispositivos móviles**, **que toda la plantilla debe conocer.**

Cualquier duda, consulta o comunicación en relación con las medidas aquí planteadas podrán formularse escribiendo al correo protecciondedatos@uah.es

[4] Según la Agencia Española de Protección de Datos el personal no está obligado a facilitar a su empresa su número de teléfono o un correo electrónico personal, salvo que la recogida de estos datos fuera de cumplimentación voluntaria y con el consentimiento expreso del trabajador o de la trabajadora, que podrían oponerse posteriormente a su tratamiento.