DEFENSOR UNIVERSITARIO
Plaza San Diego s/n
28801 Alcalá de Henares (Madrid)
Teléfonos: 91 885 4178 /4162
Fax: 91 8856499
defensor@uah.es

RECOMENDACIÓN

ASUNTO: Implantación del sistema de autenticación por múltiple factor (MFA) para acceder a los servicios de Office 365 de la UAH

Motivación.

Ante la Defensoría Universitaria se han presentado diferentes consultas y reclamaciones relacionadas con la manera en la que se está llevando a cabo la implantación del sistema de autenticación por múltiple factor (MFA) para poder acceder a los servicios de Office 365 por parte de la comunidad universitaria.

Los motivos principales de las quejas planteadas son, por un lado, la falta de información clara y útil por parte de la UAH sobre cómo debe activarse y sobre la obligatoriedad de facilitar datos personales, como el teléfono móvil particular y, por otro lado, las dudas acerca de que si las autoridades responsables de la UAH habían llevado a cabo, de acuerdo con la normativa vigente, un análisis de riesgos y de evaluación de impacto en relación con la seguridad de la información y en materia de privacidad y protección de datos, con carácter previo a la decisión de implantar este sistema de autenticación de múltiple factor.

Dentro de su marco de actuación, el Defensor Universitario desempeña la función de velar por el respeto a los derechos y libertades de todos los miembros de la comunidad universitaria ante actuaciones de los órganos y servicios de la misma, con el objeto de evitar situaciones de discriminación, indefensión o arbitrariedad (art. 1 del Reglamento del Defensor Universitario de la UAH). Y es en el cumplimiento de esas funciones en el que se enmarca la Recomendación que aquí se presenta.

Consideraciones.

1. El 19 de diciembre de 2022, a través de UAH Comunica, el Vicerrectorado de Innovación Docente y Transformación Digital informaba de la decisión del Equipo de Dirección de implantar el Múltiple Factor de Autenticación (MFA) para el acceso a los sistemas de información de la Universidad de Alcalá con **carácter obligatorio** para toda la comunidad universitaria, en concreto, para el Personal Docente e Investigador tiene carácter obligatorio desde el 1 de febrero de 2023. El uso de esta medida de seguridad está previsto para los servicios de Microsoft Office365 (correo electrónico, OneDrive, Teams, etc.,). Asimismo, en ese comunicado se informaba de que **se cortaría el acceso a los servicios de la Universidad** a todas aquellas personas que no hubieran activado esta medida en el plazo fijado.

2. De acuerdo con la información proporcionada por las personas responsables en materia de administración electrónica y seguridad de la UAH y de la Delegada de Protección de Datos de la UAH, la activación del sistema de MFA es una exigencia normativa derivada del Esquema Nacional de Seguridad del CCN-CNI, que ya ha sido implantada en el 100%

3. De la información a la que ha podido acceder esta Defensoría y la proporcionada por el Delegado del Rector para la Administración Electrónica y Seguridad y por la Delegada de Protección de Datos, la Comisión de Administración Electrónica y Seguridad de la UAH, en la reunión de 16 de diciembre de 2020, aprobó la puesta en marcha de un programa piloto del Doble Factor de Autenticación, pero no consta ningún acuerdo posterior de esta Comisión, ni de ningún otro órgano de la UAH en la que se apruebe el MFA ni la manera concreta en que debe llevarse a cabo.

4. La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE de 6 de diciembre de 2018), establece en su artículo 6, que **el tratamiento de los datos personales está basado en el consentimiento del afectado**. En este sentido, y de conformidad con lo dispuesto en el artículo 4.11 del Reglamento (UE) 2016/679, del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones "se entiende por consentimiento del afectado toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". Asimismo, este artículo señala que "cuando se pretenda fundar el tratamiento de los datos en el consentimiento del afectado para una pluralidad de finalidades será preciso que conste de manera específica e inequívoca que dicho consentimiento se otorga para todas ellas".

A este respecto, y teniendo en cuenta que la opción principal para activar la doble autenticación es a través del teléfono móvil personal de los miembros de la comunidad universitaria, debe exigirse la existencia del consentimiento de acuerdo en lo previsto en la LO 3/2018, es decir, un **consentimiento libre, específico, informado e inequívoco**. Y para ello, resulta preciso contar con información clara sobre el uso que se va a dar de esos datos personales, el tratamiento de los mismos y los mecanismos de seguridad y de privacidad fijados al efecto por la UAH. Hasta la fecha, la información que se ha proporcionado desde la UAH resulta confusa. Así, en principio el MFA se aplica únicamente a los servicios prestados por Microsoft Office 365 y no a otros servicios o aplicaciones de la Universidad, como, por ejemplo, Aula virtual, pero no se aclara los motivos por los que únicamente se aplica a unos servicios y no a otros. Igualmente, tampoco queda claro en qué ámbitos se va a exigir el MFA, ya que en algunos comunicados se hace referencia a la necesidad de utilizar el MFA solamente cuando se utilice la VPN o en remoto, en "entornos no controlados", mientras que en otros comunicados se señala que se aplicará el MFA de manera general. Además, tal y como se ha implantado la medida, no se ha solicitado ni se ha tenido en cuenta el consentimiento de los miembros de la comunidad universitaria (en los términos exigidos por la LO 3/2018 y el Reglamento

europeo de protección de datos). Al contrario, se ha establecido como una medida de carácter obligatorio que se debe cumplir bajo la amenaza de que si no se activa se contará el acceso a los servicios de la Universidad.

5. En este mismo sentido, de acuerdo con reiteradas resoluciones de la Agencia Española de Protección de Datos, **el personal no está obligado a facilitar a su empresa su número de teléfono ni su correo electrónico personal, salvo que se cuente con su consentimiento expreso**. Del mismo modo, la AEPD ha señalado que **el uso de los dispositivos móviles personales como doble factor de autenticación no está legitimado, al entender que no existe ninguna base legítima para ello**, de conformidad con lo dispuesto en el art. 6.1 del RGPD. Y ha exigido la **utilización de otros medios para llevar a cabo la doble autenticación,** sin necesidad de que se aporten datos personales de los trabajadores.

6. La Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales establece en su Disposición adicional primera que el "Esquema Nacional de Seguridad incluirá las **medidas** que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679. Para ello, **"los responsables deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad**". Y también dispone que "en los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad".

7. Por su parte, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (BOE de 4 de mayo de 2022), establece la obligatoriedad de los organismos públicos cuenten con una **política de seguridad** (artículo 12), además de la exigencia de que se lleve a cabo un **análisis y gestión de los riesgos** (artículo 14). Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema y las **medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas** y, en todo caso, existirá una **proporcionalidad** entre ellas y los riesgos. Para ello, es el responsable del tratamiento, asesorado por el Delegado de Protección de Datos, quien debe realizar un análisis de los riesgos y una evaluación de impacto en la protección de datos (artículo 3).

8. La UAH cuenta con una **política de seguridad de la información**, aprobada por el Consejo de Gobierno de 15 de julio de 2020. En este documento, que **no está adaptado a las exigencias establecidas en el RD 311/2022,** por el que se regula el Esquema Nacional de Seguridad, se dispone que "la UAH debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde

su concepción hasta la retirada del servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación". Y para garantizarlo, la UAH "debe autorizar los sistemas antes de entrar en operación; evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración; solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente y realizar las correspondientes evaluaciones de impacto y análisis de riesgos".

Asimismo, en este mismo documento se establece que "todos los sistemas sujetos a la política de seguridad de la información **deberán realizar un análisis de riesgos,** evaluando las amenazas y los riesgos a los que están expuestos y deberán tenerse en cuenta lo previsto para dichos análisis y evaluaciones de impacto regulados tanto en el RGPD como en la LPPDGDD, tomando como referencia las guías, directrices y aplicaciones elaboradas por las autoridades de control competentes al respecto". Y en especial, **este análisis debe realizarse**, regularmente, una vez cada dos años, cuando cambie sustancialmente la información manejada, cuando cambien sustancialmente los servicios prestados, cuando ocurra un incidente grave de seguridad o se reporten vulnerabilidades graves que **impliquen un cambio sustancial en las salvaguardas del sistema** y, especialmente**, cuando se traten de datos especialmente protegidos o categorías especiales de datos**, como es el caso que nos ocupa.

De acuerdo con la información de la que dispone la Defensoría Universitaria, no se ha llevado a cabo el análisis de riesgos en materia de seguridad de la información y en materia de protección de datos y privacidad antes de poner en marcha esta medida, como resulta obligatorio de acuerdo con la propia normativa de la UAH. Es más, el último informe de análisis de riesgos efectuado data de 2018 y, al respecto, desde la Unidad de Protección de Datos únicamente se ha publicado una circular informativa, pero no se han realizado los informes de análisis que exige la normativa aplicable.

Por todo ello, teniendo en cuenta las consideraciones anteriores, y de acuerdo con lo establecido en los artículos 4 y 5 del Reglamento del Defensor Universitario,

RECOMIENDO:

1. *Que se adopten las medidas oportunas para cumplir con el procedimiento exigido por la legislación aplicable para implantar el sistema MFA con todas las garantías previstas en la ley.*

2. *Que se suspenda la implantación del MFA hasta que se hayan llevado a cabo los informes que exige la legislación vigente en materia de análisis de riesgos y evaluación de impacto en la protección de datos personales.*

3. *Que no se corte el acceso a los servicios de la universidad a todas aquellas personas que no hayan activado el Múltiple Factor de Autenticación.*

4. *Que se valore la posibilidad de eliminar el uso del teléfono móvil personal para activar el PFA y se promueva el uso de otros métodos alternativos, de acuerdo a lo exigido por la Agencia Española de Protección de Datos.*

5. *Que se ofrezca a la comunidad universitaria información clara y comprensible sobre en qué consiste el MFA, a qué servicios de la UAH se aplica y si ha de exige únicamente en la VPN y acceso remoto.*

6. *Que se adapte la Política de seguridad de la UAH al RD 311/2022 y que se cumpla con la Recomendación de la Delegada de Protección de Datos de la UAH de establecer una Política de uso de dispositivos móviles del personal de la UAH.*

Alcalá de Henares, a 16 de mayo de 2023

EL DEFENSOR UNIVERSITARIO,

Juan Soliveri de Carranza

SECRETARÍA GENERAL. – **Dña. María Marcos González**
CC.- Delegada de Protección de Datos. – **Dña. Remedios Menéndez Calvo**
CC.- Delegado del Rector para Administración electrónica y seguridad. – **D. José Javier Martínez Herráiz**