Fecha de publicación: 13/03/2015

BUPO N.º: 3/2015

INSTRUCCIÓN DEL VICERRECTORADO DE TIC, CALIDAD E INNOVACION Y DE LA SECRETARÍA GENERAL POR LA QUE SE REGULA EL SISTEMA DE CREACIÓN Y GESTIÓN DE CONTRASEÑAS EN LOS PROCESOS ELECTRÓNICOS QUE REQUIEREN AUTENTICACIÓN

Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, consagra el derecho de los ciudadanos a relacionarse electrónicamente con las Administraciones Públicas, así como la obligación de éstas de dotarse de los medios y de los sistemas electrónicos para que aquél pueda efectivamente ejercerse, regulando los aspectos básicos de la utilización de las TIC en la actividad administrativa, así como de las relaciones de los interesados con las mismas con el objeto de garantizar no ya sólo sus derechos, sino la validez y la eficacia de la actividad administrativa en condiciones de seguridad jurídica.

En este contexto de desarrollo de los procesos electrónicos en el ámbito administrativo, el perfil de los usuarios de la comunidad universitaria y los usos que estos hacen de la red, han variado de manera significativa en los últimos años, incrementándose el riesgo de penetración en determinados servicios. El resultado de todo este proceso de incorporación de las TIC a la actividad de los servicios universitarios se traduce en el incremento del número de dispositivos con acceso a las redes de información y, por ende, del número y alcance de las gestiones que, desde los mismos, pueden llevarse a cabo.

Empero, si nos remitimos a los datos estadísticos sobre usos y hábitos de los usuarios en la red, se constatan carencias y lagunas en la gestión de la seguridad de la información en relación con el empleo de las contraseñas. En general, los miembros de la comunidad universitaria no utilizan claves o contraseñas seguras y, en particular, apenas las utilizan para el acceso y protección de los ficheros ubicados en sus equipos. Es más, sólo el 22,7% del PDI y el 10.7% del PAS han sustituido con regularidad sus credenciales. Ahora bien, el hecho de que no se trate de una medida de seguridad demasiado extendida entre los miembros de la comunidad universitaria, no nos exime del deber de actuar en consecuencia, procurando diseñar un sistema de gestión de las contraseñas y/o claves más robusto y más fiable.

En este contexto, y con el propósito de que todo el proceso de comunicación sea gestionado de forma segura, a la hora de acceder al correo electrónico y demás servicios a través de Internet, han de tomarse una serie de medidas y de buenas prácticas encaminadas a mejorar la seguridad. En este sentido, amén de la necesaria concienciación de los miembros de la comunidad universitaria para gestionar de manera más eficiente, léase segura, su información, es preciso definir mejor los parámetros de gestión y creación de las contraseñas que aquéllos han de utilizar en la mayoría de los procesos y operaciones que requieren de su autenticación.

Es por esto que, la Comisión de Seguridad de la Información y Protección de Datos de la Universidad Pablo de Olavide, en el ejercicio de una de sus atribuciones, cual es, la de responder de la integridad y actualización de la información y de los servicios a los que puede accederse electrónicamente, dispuso que se dictase una Instrucción, a cargo del Vicerrectorado de TIC, Calidad e Innovación y de la Secretaría General, en la que se arbitrase un procedimiento simplificado para fortalecer la seguridad de las contraseñas. Esta instrucción se enmarca, por tanto, en el margen de discrecionalidad de la acción de ambos órganos de gobierno para dar cumplida respuesta a la problemática creciente, que se ha suscitado en torno a la falta de seguridad en las contraseñas de los miembros de la comunidad universitaria. Ni que decir tiene que la dimensión prudencial, inherente a esta facultad de apreciación, no

se sitúa al margen del régimen normativo de aplicación, representado, en este caso, por el Documento de Seguridad de la Universidad Pablo de Olavide, de 11 de julio de 2013. Antes al contrario, es consecuencia de la imposibilidad del mismo para regular todo caso concreto (*sensus plenior versus sensus singular*) desde la generalidad de sus previsiones de seguridad, en la medida en que su contenido permite adoptar, dependiendo de los problemas, acciones distintas.

En consecuencia, los sistemas de información (y software de base) habilitados por el CIC deben disponer de mecanismos de identificación y autenticación, que prevengan los accesos no autorizados, basados en la existencia de un identificador unívoco de usuario y contraseña, o mediante la utilización de certificado digital o de cualesquiera otros mecanismos de protección suficientemente probados, dependiendo de los recursos tecnológicos disponibles y de las características de la información a proteger. Para gestionar correctamente la seguridad de las contraseñas los usuarios generales (sin privilegios especiales asociados a tareas de administración) deberán satisfacer, al menos, los siguientes criterios para la creación y establecimiento de contraseñas seguras:

1. En el caso de sistemas de identificación basados en usuario y contraseña, la asignación de contraseña inicial será aleatoria y, dependiendo del sistema de información, pre-expirada. El usuario deberá cambiar la contraseña en el primer acceso a los sistemas que realice. El período de validez de los identificadores o contraseñas será de un año, de tal modo que, fuera de este rango de fechas, el sistema conminará al usuario al cambio de su identificador o contraseña. Para el caso de los usuarios que no hubieren renovado su contraseña en plazo, se procederá al bloqueo de usuario por el/la administrador/a. Adicionalmente, deberá evaluarse la posibilidad de exigir reglas adicionales de complejidad en base al grado de madurez de los controles de seguridad implantados.

2. Las contraseñas de los sistemas de información serán asignadas y comunicadas a los usuarios de forma que se garantice la confidencialidad e integridad de las mismas, de forma tal que sólo sean conocidas por el usuario al que pertenecen.

3. No se permitirá, con carácter general, el acceso a los sistemas a través de usuarios genéricos. Esto incluye a aquellos que, por defecto, son creados en el proceso de instalación de los sistemas y aplicaciones. En cualquier caso, deberá asignarse un responsable de aquellos usuarios genéricos que se estimen necesarios. Las contraseñas que, por defecto, se inserten en paquetes y programas, especialmente las relacionadas con administradores o usuarios con accesos amplios, serán sustituidas de manera inmediata por otras con requisitos de seguridad más complejos.

4. El código o contraseña de usuario o identificador es personal e intransferible. No se permite el acceso a los sistemas de información con un identificador que no sea el propio, así como su comunicación o cesión a cualquier otra persona perteneciente o no a la comunidad universitaria.

5. Se deben utilizar al menos 8 caracteres para crear la clave. La contraseña debe contener dígitos, letras, signos de puntuación y/o caracteres especiales. Las letras deberán alternar mayúsculas. En el caso de incluir otros caracteres que no sean alfa-numéricos en la contraseña, se recomienda la inclusión de los símbolos admitidos por el Documento de Seguridad.

Fecha de publicación: 13/03/2015

BUPO N.º: 3/2015

6. Existirá un histórico de contraseñas que prevenga la re-utilización de la contraseña anterior. En cualquier caso, los sistemas permitirán el cambio autónomo de contraseña por parte de los usuarios, aun cuando no sea como consecuencia del cambio periódico descrito *ut supra*. El archivo en el que queden almacenadas las contraseñas de todos los usuarios y aplicaciones será accesible exclusivamente por el administrador/a del CIC. En el caso de sistemas no gestionados por el CIC, solo podrá acceder el administrador o administradora designado por el responsable o la responsable de seguridad del fichero. A su vez el campo contraseña de este archivo deberá estar encriptado.

7. No se permite la existencia en los sistemas de información que traten datos de carácter personal clasificados en el Documento de Seguridad, como de nivel medio y alto, de identificadores o contraseñas que no reúnan los criterios descritos *ut supra y* que no puedan ser relacionados de forma unívoca con un usuario en concreto de dichos sistemas. Asimismo, para este tipo de usuarios el período de validez de sus identificadores o contraseñas será de 6 meses.

8. Deberán arbitrarse mecanismos de bloqueo de los usuarios. En particular, se considerará, al menos, los siguientes: (i) el bloqueo por intentos reiterados de acceso fallidos (3 intentos); (ii) el bloqueo asociado a intentos de acceso fuera del intervalo de fechas de validez de un identificador de usuario; y (iii) el bloqueo manual por parte de Administrador/a.

9. Existirá un procedimiento actualizado de altas, modificaciones y bajas de usuarios en los sistemas de información que garantice el cumplimiento de las normas anteriores relativas a la gestión de usuario.

La Presente Instrucción entrara en vigor al día siguiente de su publicación en el BUPOe.

LA VICERRECTORA DE TIC, CALIDAD E INNOVACION

Dña. Alicia Troncoso Lora

EL SECRETARIO GENERAL

D. José María Seco Martínez

Fecha de publicación: 13/03/2015

BUPO N.º: 3/2015