I.2.6. Acuerdo 6/ CG 14-07-16 por el que se aprueba la Normativa de gestión de identidades y control de acceso lógico de la Universidad Autónoma de Madrid.

1 Introducción

La Universidad Autónoma de Madrid (en adelante UAM), debe controlar adecuadamente los accesos que se realizan a sus sistemas informáticos, con el fin de garantizar la seguridad de los mismos. Para ello cuenta con un sistema de gestión de identidades (en adelante ID-UAM), para poder identificar y autenticar a los usuarios[1] y un control de acceso lógico para gestionar los accesos que se realizan a los servicios y aplicaciones basados en las Tecnologías de la Información y Comunicación (en adelante, TIC).

El servicio ID-UAM es el encargado de gestionar la identidad única de los usuarios, sus credenciales y la caducidad de las mismas, y la asignación o retirada de permisos en el acceso a los servicios.

El control de acceso lógico es el encargado de garantizar que el acceso a la información se realice de manera adecuada, supervisando en todo momento su funcionamiento. Para ello, debe controlar de manera individualizada todos los accesos electrónicos que se realizan sobre los Sistemas de Información de la UAM, verificando que se llevan a cabo de acuerdo a los principios establecidos.

2 Objetivo

La presente normativa pretende regular los principios generales que deben regir el control de los accesos a las aplicaciones, sistemas o servicios electrónicos de la UAM, con los siguientes objetivos:

- Regular la creación y uso de credenciales para el acceso a los sistemas de información de la UAM.
- Impedir el acceso no autorizado a los sistemas de información de la UAM.
- Implementar la seguridad en los accesos de los usuarios por medio de técnicas de autenticación y autorización.
- Registrar y revisar los eventos y actividades llevados a cabo por los usuarios en los sistemas de información de la UAM.
- Informar a los usuarios respecto de su responsabilidad frente a los accesos de que dispone.

La presente normativa deberá ser complementada, en su caso y en la medida oportuna, con la aplicación de las medidas de seguridad previstas en el Anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

[1] Se entiende como usuario a toda persona que haga uso de los recursos TIC de la UAM (Véase la definición de “usuario” en el apartado del “Ámbito de aplicación” de la Política de Seguridad de la Información de la UAM.)

3 Ámbito de aplicación

Esta normativa es de aplicación a todo el ámbito de actuación de la UAM, y sus contenidos derivan de las directrices de carácter más general definidas en la Política de Seguridad de la Información de la UAM. La presente normativa será de aplicación y de obligado cumplimiento para todos los usuarios que accedan a los diferentes servicios, sistemas y demás recursos TIC[2] de la UAM.

La presente normativa ha sido elaborada por el Comité de Seguridad de la Información de la UAM y aprobada por el Consejo de Gobierno de la UAM, estableciendo de esta forma las directrices generales para el uso adecuado de los recursos TIC de tratamiento de información que la UAM pone a disposición de los usuarios para el ejercicio de sus funciones, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

4 Normativa técnica

Los principios que rigen la gestión de identidades y el control de acceso a los Sistemas de Información de la UAM son los siguientes:

- Todo usuario debe tener una relación formal y vigente con la UAM, perteneciendo al colectivo PDI, PAS, PDIF o estudiante o bien a otro colectivo determinado por la UAM que haga uso de los servicios, sistemas o recursos TIC. Con la excepción de los servicios de acceso público, el acceso a los Sistemas de Información de la UAM requerirá siempre de autenticación previa.
- El control de acceso a los Sistemas de Información de la UAM se gestionará a través del servicio ID-UAM.
- Los usuarios deberán siempre autenticarse como usuarios no privilegiados del sistema. Excepcionalmente, y sólo con fines de administración, podrán autenticarse como administradores del mismo.
- Todos los sistemas de información de la UAM estarán dotados de mecanismos destinados a la identificación unívoca de los usuarios que estén autorizados a acceder a ellos,

Los usuarios deberán en todo momento hacer un uso responsable de la información y los sistemas de información accedidos, garantizando el nivel de seguridad adecuado, de acuerdo a las normativas aplicables en cada caso.

---

[2] Tal y como se define en el apartado del "Ámbito de aplicación" de la Política de Seguridad de la Información de la UAM, los recursos TIC son "…todos los sistemas centrales y departamentales, estaciones de trabajo, ordenadores de puesto, impresoras y otros periféricos y dispositivos de salida, sistemas de localización, redes internas y externas, sistemas multiusuario y servicios de comunicaciones (transmisión telemática de voz, imagen, datos o documentos) y sistemas de almacenamiento que sean de su propiedad.

En este marco no se considera "recurso TIC de la UAM" aquellos ordenadores o dispositivos personales financiados a título individual, no inventariados a nombre de la Universidad, aunque pudieran ocasionalmente ser usados para labores propias de investigación."

4.1 Tipos de cuentas

Se definen tres tipos de cuentas:

- **Cuentas de usuario:** Son todos aquellos identificadores asociados a personas físicas (usuarios), utilizados para acceder a los sistemas de información de la UAM. Estas cuentas identifican unívocamente al usuario en cada sistema de información.
- **Cuentas de aplicación:** Son todas aquellas cuentas de acceso a aplicaciones, servicios y/o equipos, que no corresponden a personas físicas, y que se utilizan para realizar las actividades automatizadas que necesitan dichos componentes tecnológicos, identificándolos.
- **Cuentas de administración:** Son todas aquellas cuentas de acceso que permiten llevar a cabo las tareas de administración de una aplicación, servicio y/o recurso TIC.

4.2 Gestión de identidades

La gestión de identidades de carácter corporativo de la UAM agrupa las identidades de todos los usuarios que tienen relación con la UAM (PDI, PAS, PDIF, estudiantes y otros colectivos) y pretende asegurar la identificación única de la persona ante cualquier uso de la misma, así como el control del ciclo de vida de las cuentas de usuario en la UAM.

Las cuentas se gestionan en diferentes ámbitos, que pueden ser generales para toda la UAM (directorio corporativo) o locales y específicos de activos concretos (aplicaciones, equipos o infraestructuras tecnológicas). Estas cuentas locales son independientes de las del directorio corporativo.

El ciclo de vida de las cuentas de usuario es el siguiente:

- **Alta**: Creación de la cuenta de usuario en el directorio corporativo y autorización de acceso a los servicios que tiene asociados en virtud de su relación con la UAM.
- **Modificación**: El cambio de los servicios asociados cada vez que cambia su relación con la UAM.
- **Baja**: Cuando finaliza la relación de la persona con la UAM (y expira el tiempo de extensión del servicio correspondiente), se retirará la autorización de acceso al servicio.

La gestión de identidades recibe los datos que son la base del inicio de cualquier tratamiento en la gestión de identidades de tres fuentes:

- **Aplicación de gestión de recursos humanos de la Universidad**: Gestiona los datos de todas aquellas personas que mantienen una relación contractual o de servicio con la UAM: PDI, PAS y PDIF.
- **Aplicación de gestión académica**: Gestiona los datos de los estudiantes.
- **Aplicación de gestión de Alumni**: Proporciona los datos de los usuarios gestionados por la Oficina Alumni de la UAM.

Existen otros colectivos cuyos datos no están en las fuentes citadas (por ejemplo, personal o investigadores no vinculados contractualmente con la UAM, colaboradores, etc…). Para cada uno de ellos se define un responsable en la UAM que autoriza y proporciona la información necesaria para la gestión (alta, modificación o baja) que se introduce de forma manual.

La gestión de identidades ofrece sus servicios a través del protocolo LDAP. Mediante dichos servicios se ofrece autenticación y autorización para la mayor parte de los servicios que ofrece Tecnologías de la Información (en adelante, TI) a los usuarios, como por ejemplo: bibliotecas, correo electrónico, intranet (portal del empleado), carnet universitario, VPN, WiFi, telefonía IP, etc.

4.2.1 Gestión de identidades

Tal y como se indica en el apartado anterior, el control de acceso se gestiona fundamentalmente desde el servicio de gestión de identidades centralizando las siguientes funciones:

- Nominalización de todas las cuentas de usuarios para posibilitar la identificación segura de los mismos.
- En función del colectivo correspondiente, seguimiento la fecha de fin de la relación a cada cuenta de usuario para su inactivación.
- Seguimiento de tiempos de extensión de servicio posteriores a la fecha de fin de relación según se indica en el apartado 4.2.4 de gestión de usuarios de esta misma normativa.
- Asociación de los identificadores y cuentas de usuario con ciertos roles o grupos que determinen los diferentes criterios para el control de acceso a los distintos servicios.

4.2.2 Identificación, autenticación y trazabilidad

El servicio de gestión de identidades garantiza, de manera general, que cada identificador y cuenta de usuario se corresponde inequívocamente con la persona que representa, de modo que ninguna otra persona pueda hacer uso de ellos. A tal fin, el servicio de gestión de identidades establece mecanismos de autenticación que permiten garantizar dicha relación.

No está permitido el uso de cuentas genéricas de usuario. En el caso de cuentas de administración se asociará dicho rol al identificador de los usuarios que desarrollen estas funciones y siempre que sea posible técnicamente.

El servicio de gestión de identidades también permite registrar todos los cambios de credenciales realizados así como su resultado, mostrando el recurso (servicio) desde el que se ha modificado.

4.2.3 Colectivos

Los colectivos considerados son los siguientes:

- **Usuario no corporativo:** Se considerará usuario no corporativo, en general, a cualquier persona que no tenga relación de servicio ni vinculación contractual directa ni indirecta con la UAM. Este colectivo, de carácter general, no se integra en la gestión de identidades y se subdivide en los siguientes:
    - **Ciudadano anónimo**: Se considerará ciudadano anónimo a cualquier persona que acceda de manera anónima, y por lo tanto sin ningún tipo de identificación, a cualquiera de los servicios públicos dispuestos por la UAM (por ejemplo, cualquier usuario que navegue por las páginas web públicas de la UAM).
    - **Ciudadano autenticado:** Se considerará ciudadano autenticado a cualquier persona que acceda a los servicios de la UAM identificándose con cualquiera de los sistemas de autenticación reconocidos por la Administración Pública, según el marco normativo vigente en materia de administración electrónica.

- **Usuario solicitante de admisión:** Aquellos que, sin ser usuario de la Universidad, necesitan autenticarse para el inicio de trámites administrativos en algún servicio de la universidad (por ejemplo, para las Pruebas de Acceso a la Universidad).

- **Usuario corporativo**: Se considerará usuario corporativo, en general, a cualquier persona que tenga una o varias vinculaciones, directas o indirectas, con la UAM. Este colectivo, de carácter general, se subdivide en los siguientes:

  - **Estudiante**: Se considerará estudiante a cualquier persona matriculada en alguno de los estudios de grado, másteres oficiales, programas de doctorado o enseñanzas propias ofrecidos por la UAM, y que, en virtud de dicha vinculación, debe poder acceder a los servicios electrónicos desplegados por la UAM para este colectivo.

  - **PAS**: Se considerará PAS a cualquier miembro del personal de administración y servicios de la UAM, funcionario o laboral, y que, en virtud de dicha vinculación, debe poder acceder a los servicios electrónicos desplegados por la UAM para este colectivo.

  - **PDI**: Se considerará PDI a cualquier miembro del personal docente e investigador de la UAM, funcionario o laboral, y que, en virtud de dicha vinculación, debe poder acceder a los servicios electrónicos desplegados por la UAM para este colectivo.

  - **PDIF**: Se considerará PDIF a cualquier persona, con relación contractual con la UAM, que participa en alguno de los proyectos o programas de investigación de la UAM, como investigador o técnico, y no es ni PDI ni PAS de la UAM, y que, en virtud de dicha vinculación, debe poder acceder a los servicios electrónicos desplegados por la UAM para este colectivo.

  - **Personal externo**: Se considerará personal externo a cualquier persona que no tiene relación de servicio ni contractual con la universidad, sino a través de un contrato de servicio con un tercero. En virtud de dicha relación deben poder acceder a los servicios electrónicos desplegados por la UAM para este colectivo. Esta condición se obtiene mediante el aval del PDI o PAS responsable de su vinculación.

  - **Personal no vinculado:** Se considerará personal no vinculado a cualquier persona que colabora con la Universidad y que no teniendo relación de servicio ni contractual con la misma, necesita acceder a los servicios electrónicos desplegados por la UAM.

- **Alumni:** Se considerará Alumni a toda persona que esté inscrita en la Oficina Alumni (fundamentalmente antiguos estudiantes, PAS o PDI, o simpatizantes de la UAM). En función de la modalidad de Alumni en la que se registre podrá acceder a los servicios electrónicos que la UAM ofrezca a estos colectivos en cada momento.

4.2.4 Gestión de cuentas de usuarios

Las cuentas de usuario se tramitarán a través del sistema de Gestión de Identidades de la universidad, el cual se provee de diferentes fuentes de información: Recursos Humanos, Gestión Académica, Alumni y otros.

Una vez estas fuentes certifiquen el origen de un usuario, este será dado de alta automáticamente en el sistema de Gestión de Identidades de la UAM con lo que pasará a disponer de los accesos a los

servicios y sistemas autorizados para el colectivo que le corresponda. Cualquier modificación en la relación del usuario con la universidad, se verá reflejada en este sistema.

En el momento de finalizar la relación del usuario con la universidad dejará de tener los accesos a los servicios y sistemas que tuviera por pertenecer a su colectivo. En algunos servicios se permitirá extender el tiempo durante el que se puede utilizar el mismo de acuerdo con la siguiente tabla:

Tipo	Servicio	Periodo de extensión del servicio
1	Listas de correo institucionales Páginas blancas	Sin periodo de extensión
2	Correo UAM [3]	• 1 año • redirección del correo a petición
3	Correo Estudiantes [4]	1 año
4	Resto de Servicios	15 días

Dicha extensión no será aplicable en caso sanción disciplinaria, por el período de duración de ésta. La suspensión de la relación como media provisional adoptada durante la instrucción de un procedimiento disciplinario podrá conllevar la suspensión de los servicios y sistemas.

La descripción en detalle de los pasos técnicos a seguir para realizar el alta, modificación y baja de usuarios está definida con detalle en el Procedimiento de gestión de usuarios de TI.

4.3 Normas de seguridad en el uso de credenciales

4.3.1 Normas generales de obligado cumplimiento en el uso de credenciales

Con independencia del tipo de cuenta que se esté usando, el uso de credenciales debe cumplir las siguientes normas generales.

- Las credenciales tendrán una longitud mínima específica para cada tipo de cuenta, y deberán contener caracteres de los siguientes tres tipos:
    - Numérico
    - Mayúsculas
    - Minúsculas
- Las credenciales no podrán contener caracteres en blanco.
- Las credenciales no podrán estar formadas únicamente por palabras de diccionario u otras fácilmente predecibles o asociables al usuario (nombres, direcciones, matrículas, etc.)
- No está permitido el uso del nombre de la cuenta, ni el nombre ni los apellidos del usuario, como credencial o parte de la misma.

[3] Las especialidades referidas al correo electrónico se regularán en la Normativa de uso de correo electrónico.
[4] Las especialidades referidas al correo electrónico se regularán en la Normativa de uso de correo electrónico.

- El usuario es responsable de mantener la confidencialidad de sus credenciales.
- Las credenciales son de uso exclusivo por el usuario al que pertenece.
- Las credenciales no se podrán escribir o enviar por medio alguno si no van cifradas.

Las credenciales de los usuarios no se guardarán sin cifrar, ni en los sistemas de información ni por parte del propio usuario. En ningún caso se guardarán en soporte papel o informático de manera inteligible.

- Las credenciales se deben cambiar periódicamente, con una periodicidad máxima establecida para cada tipo de cuenta.
- No se podrán reutilizar las últimas seis (6) credenciales.
- Ante la sospecha de que su identidad haya sido suplantada para acceder a un determinado Sistema de Información, lo pondrá inmediatamente en conocimiento del Centro de Atención al Usuario (CAU), que se encargará de tramitar la incidencia. Adicionalmente modificará las credenciales de forma inmediata.

4.3.2 Normas específicas para cada tipo de cuenta

4.3.2.1 Cuentas de usuarios corporativos

Las cuentas de usuarios corporativos están sujetas a las normas generales de obligado cumplimiento en el uso de credenciales, que están definidas en el punto 4.3.1 del presente documento, así como a las siguientes medidas de seguridad específicas:

- Todas las credenciales tendrán una longitud mínima de ocho (8) caracteres.
- Cualquier cuenta de usuario se bloqueará temporalmente tras la introducción de un número de credenciales erróneas de forma consecutiva según esté previsto por cada sistema.
- El bloqueo de cualquier cuenta de usuario se prolongará durante un tiempo mínimo de una (1) hora.
- Las credenciales se deberán modificar con una periodicidad de quince (15) meses.
- No se comunicarán a nadie (ni siquiera a superiores, compañeros o personal de TI) bajo ninguna circunstancia. Si alguna persona le solicitara la comunicación de sus credenciales, póngalo en conocimiento del CAU.
- Siempre que la aplicación lo soporte, se utilizará el directorio corporativo de la UAM para la validación, a través de comunicación segura, de las credenciales de autenticación.

Recomendaciones:

- Nunca se solicitarán las credenciales de los usuarios por ningún medio (correo electrónico, teléfono, etc.).
- Ante la menor duda sobre un mensaje de este estilo, debe descartarse. Si se necesitan aclaraciones, debe ponerse en contacto con el CAU y solicitarlas, siempre antes de responder a dicho mensaje.
- No usar en la UAM las mismas credenciales utilizadas fuera de ella para acceder a otro tipo de servicios: cuentas de correo o servicios internet, tele-compra, banca, etc.
- Introducir sus credenciales en ambiente de confidencialidad. Del mismo modo, facilite (retirándose, mirando para otro lado, etc.) la confidencialidad de quien debe introducir credenciales en su presencia.

- No guardar las credenciales en navegadores, clientes de correo electrónico y en general en cualquier equipamiento móvil, tanto corporativo como personal, siempre que sea posible.

4.3.2.2 Cuentas de aplicación

Las cuentas de aplicación están sujetas a las normas generales de obligado cumplimiento en el uso de credenciales, que están definidas en el punto 4.3.1 del presente documento, así como a las siguientes medidas de seguridad específicas:

- Todas las credenciales tendrán una longitud mínima de doce (12) caracteres.
- Las credenciales se deberán modificar con una periodicidad de un (1) año.
- Se asegurará que las credenciales son guardadas en el sistema mediante cifrado no reversible o reversible suficientemente seguro.
- Cuando no sea técnicamente posible el cumplimiento de estas normas, se planificará la implementación: de soluciones informáticas que permitan el cumplimiento de la presente normativa, de contramedidas que reduzcan el riesgo al mínimo asumible.

4.3.2.3 Cuentas de administración

Las cuentas de administración están sujetas a las normas generales de obligado cumplimiento en el uso de credenciales, que están definidas en el punto 4.3.1 del presente documento, así como a las siguientes medidas de seguridad específicas:

- Todas las credenciales tendrán una longitud mínima de doce (12) caracteres.
- Las credenciales se deberán modificar con una periodicidad de un (1) año.
- Cuando no sea técnicamente posible el cumplimiento de estas normas, se planificará la implementación de soluciones informáticas que permitan el cumplimiento de la presente normativa en el menor plazo posible.
- Se garantizará que los usuarios de estas cuentas sólo tendrán acceso a la información que les incumba en función de su perfil.
- Se garantizará la modificación o revocación de las autorizaciones de acceso al Sistema de Información de aquellas cuentas que cambien o cesen en su actividad.

4.3.2.4 Certificados digitales de la UAM

La puesta a disposición por parte de la UAM de certificados electrónicos a *usuarios corporativos* para el ejercicio de sus funciones exigirá por parte del usuario, la aceptación de una serie de medidas de seguridad comunes, y otras específicas en función del dispositivo en donde se almacene el certificado electrónico.

Las medidas de seguridad comunes, tanto para el proceso inicial de emisión como para el posterior de renovación son:

- El usuario deberá acudir personalmente a la ODA (Oficina de Acreditación) mostrando su DNI (Documento Nacional de Identidad) ó NIE (Número de Identidad de Extranjero).
- El usuario deberá aportar, en caso de que se lo requieran, la documentación oficial que permita acreditar el cargo que ostenta.

Las medidas de seguridad específicas en función del dispositivo en donde se almacene el certificado electrónico son:

- Si el dispositivo de almacenamiento es el Carné Universitario son:
  - El usuario deberá cambiar obligatoriamente el PIN del Carné Universitario en la misma ODA (Oficina de Acreditación), inmediatamente después de que se le haga entrega de la tarjeta conteniendo el certificado electrónico.
  - El usuario no revelará el PIN del Carné Universitario a ninguna persona en ninguna circunstancia.
- Si el dispositivo de almacenamiento es el contenedor de certificados del sistema operativo de un ordenador personal, o cualquier otro contenedor expresamente diseñado para la importación, uso y custodia de certificados electrónicos de forma segura:
  - Se recomienda habilitar una protección segura de la clave privada, mediante la configuración de una contraseña de acceso al almacén de certificados, cada vez que una aplicación la use. El usuario no revelará esta contraseña a ninguna persona bajo ninguna circunstancia.
  - El proceso de instalación de este certificado electrónico, garantizará que la clave primaria del certificado electrónico no sea exportable posteriormente.
- Si el dispositivo de almacenamiento es un almacén centralizado, cuya gestión dependa del Servicio de TI, éste último implementará las medidas de seguridad necesarias para garantizar la custodia efectiva de los certificados electrónicos.

4.3.2.5 Otros sistemas de autenticación

Cuando los mecanismos de identificación y autenticación se fundamenten en métodos distintos a la utilización tradicional de credenciales, como por ejemplo los sistemas de credenciales de un solo uso, métodos biométricos, etc., serán de aplicación las medidas generales a que se refiere esta normativa, y se incorporarán las instrucciones específicas sobre la utilización de los nuevos medios de autenticación.

4.3.3 Cambio de credenciales

Si un usuario entiende que sus credenciales han quedado comprometidas o las ha cedido a terceros autorizados por motivos de trabajo o mantenimiento, debe proceder a sustituirlas por otras de manera inmediata.

Por otro lado, el usuario deberá realizar una petición de cambio de credenciales al CAU cuando se produzca alguna de las situaciones siguientes:

- Olvido de las credenciales de acceso.

- Bloqueo del acceso a través de credenciales tras el número de intentos fallidos determinados por el sistema.

El usuario tendrá acceso a un sistema que permita modificar las credenciales en cualquier momento. En el caso de que necesite recuperarla, lo podrá hacer siempre y cuando se haya facilitado previamente al sistema un teléfono móvil y/o correo alternativo.

4.4 Privilegios

4.4.1 Tipos de privilegios y principios básicos de gestión

La gestión de privilegios contempla la determinación y asignación de las capacidades que tiene cada cuenta sobre información, aplicaciones, servicios, sistemas y demás recursos TIC (en adelante activos de la UAM). Para ello, el responsable de cada activo dentro de la UAM debe determinar qué cuenta puede acceder al activo bajo su responsabilidad, y con qué privilegios.

En relación a los tipos de cuentas, existen dos tipos de privilegios básicos en torno a cualquier activo:

- **Privilegios de administración del activo,** que permite configurar su funcionamiento, determinar las cuentas que pueden acceder a él y las actividades que pueden realizar dichas cuentas.
- **Privilegios de uso del activo,** que permiten acceder al activo y ejecutar las actividades permitidas.

Considerando que los privilegios de administración del activo están asociados a las cuentas de administración, sólo tendrá sentido hablar de gestión de privilegios de administración para aquellas cuentas de usuario a las que se les deben conceder dichos privilegios.

Los sistemas deben estar diseñados o configurados de tal forma que sólo se acceda a las funciones permitidas.

Considerando la gran cantidad de activos existentes en la UAM y la enorme cantidad de cuentas cuyos privilegios se deben gestionar, se han definido una serie de principios básicos que rigen la gestión de privilegios:

- De manera general, los privilegios de acceso que tiene cada cuenta de usuario respecto de cada activo viene determinado por:
    - Los colectivos a los que pertenece la persona (por ejemplo: PAS, PDI, alumni, etc.).
    - Las labores específicas que dicha persona desarrolla dentro de su colectivo (centro, departamento, cargo, etc.).
    - Las tareas funcionales que la persona tenga encomendadas.
- Estos roles son los que se utilizan como referencia inicial para la asignación de privilegios de cada cuenta de usuario respecto de cada activo.
- Siempre que sea posible, la asignación y retirada de privilegios de cada cuenta de usuario a cada activo se llevará a cabo de manera automatizada en función de su rol.
- Se realizará una gestión manual de las excepciones a los privilegios genéricos que cada cuenta de usuario tenga en función de su rol.

4.4.2 Gestión de privilegios y sus responsabilidades

La asignación, modificación o revocación de privilegios en los Sistemas de Información de la UAM será solicitada por los responsables del departamento o área a la que pertenezca el destinatario de dichos privilegios.

TI será responsable de registrar, mantener actualizados y custodiar los permisos otorgados a los usuarios.

La información que contenga datos de carácter personal será accesible únicamente por personal debidamente autorizado por los correspondientes responsables de fichero, de acuerdo a los perfiles de acceso asignados en el documento de seguridad.

Será necesario crear y mantener un Inventario de Privilegios de Acceso, que contendrá información relativa a cada usuario y sus privilegios de acceso concedidos para cada uno de los Sistemas de Información.

La información se creará al dar de alta a un usuario por primera vez en alguno de los sistemas afectados y deberá mantenerse actualizada, registrándose todas aquellas modificaciones que se produzcan en los privilegios de acceso, incluyendo las bajas de usuario.

De acuerdo con lo establecido en los apartados anteriores, la gestión de identidades que se lleva a cabo en la UAM se establece de la siguiente forma:

- No se lleva a cabo ningún tipo de gestión de los ciudadanos anónimos debido a sus características intrínsecas.
- La gestión de usuarios no corporativos se lleva a cabo de manera independiente para cada uno de ellos y el único privilegio que se les concede es el acceso al servicio específico relacionado con el seguimiento de sus trámites.
- La gestión de los usuarios corporativos y de los antiguos usuarios se lleva a cabo de la siguiente manera:
    - La gestión de los privilegios de acceso a los activos se lleva a cabo de manera centralizada y automatizada.
    - La gestión de las excepciones se lleva a cabo de manera específica por aplicación y cuenta de usuario, de forma completamente manual. Dicha gestión la realiza el administrador de cada aplicación.
- La gestión de cuentas de administración se lleva a cabo de forma manual e individualizada en cada sistema de información.
- La gestión de cuentas de aplicación se lleva a cabo de forma manual e individualizada en cada sistema de información.

4.5 Gestión de Accesos Lógicos

La gestión de accesos lógicos permite aplicar controles de acceso en todos los niveles de la arquitectura y topología de los Sistemas de Información de la UAM.

En cada uno de estos ámbitos están regulados los criterios de identificación y autenticación, autorización de accesos, verificación de dichos accesos y registro y monitorización de las actividades.

4.5.1 Principios

Los principios que rigen el control de acceso a los Sistemas de Información de la UAM son las siguientes:

- Con la excepción de los servicios de acceso público, el acceso a los Sistemas de Información de la UAM requerirá siempre de autenticación previa.
- Siempre que ello sea posible, el control de acceso a los Sistemas de Información de la UAM se realizará a través del servicio de gestión de identidades. Para el resto, las medidas de control de acceso lógico se implementarán de forma específica en cada uno de los sistemas y se gestionarán de manera independiente siguiendo las directrices especificadas en este documento.
- Los usuarios deberán siempre autenticarse como usuarios no privilegiados del sistema. Excepcionalmente, y sólo con fines de administración, podrán autenticarse como administradores del mismo.
- Los usuarios deberán en todo momento hacer un uso responsable de la información y de los sistemas de información accedidos, garantizando el nivel de seguridad adecuado, de acuerdo a las normativas aplicables en cada caso.
- Se realizará una gestión centralizada de todos los eventos de seguridad relativos a los accesos lógicos de los usuarios que permita la monitorización de dichos eventos y garantice los periodos de retención legalmente establecidos.
- Todas las contraseñas asignadas a las cuentas de usuarios deberán respetar la política de contraseñas detallada en el apartado 4.3 de Normas de seguridad en el uso de credenciales de la presente normativa.

4.5.2 Revisión periódica del control de acceso

A fin de mantener un control eficaz del acceso con privilegios de administración a los activos de la UAM, se llevará a cabo un proceso formal, a intervalos regulares de no más de 1 año, a fin de revisar los derechos de acceso de los usuarios administradores.

Para el caso de los usuarios que dispongan únicamente de privilegios de acceso y no de administración, se establecerá de la misma forma una revisión periódica de los mismos para identificar anomalías o posibles desviaciones que se hayan derivado de los procedimientos de alta, baja o modificación establecidos para cada tipología de usuario. Se habitarán procesos que comprueben automáticamente que el control de acceso dispuesto es el correcto.

4.5.3 Control de acceso a los sistemas operativos de los sistemas de información

Para el acceso al sistema operativo de los diferentes Sistemas de Información de la UAM, ya sean servidores, equipos personales o equipos personales de uso compartido, y sea cual sea la forma de acceso (local o remota), los usuarios contarán con una cuenta creada y asignada por el administrador correspondiente, que les permitirá realizar en dicho sistema únicamente las acciones que le hayan sido encomendadas.

4.5.3.1 Inicio seguro de sesión

El acceso a los sistemas operativos estará protegido mediante un inicio seguro de sesión, que contemplará las siguientes condiciones:

- En función del tipo de sistema (servidores, aplicaciones, etc….) y de la criticidad del mismo, se mostrará, siempre que sea posible, un mensaje adaptado que advierta de que el uso del sistema sólo está permitido a usuarios autorizados.
- Hasta que no se haya completado con éxito el proceso de autenticación, no se deberá mostrar ningún tipo de información relativa al sistema (tal como identificadores del sistema o versiones de software instalado), que puedan ayudar a identificarlo, así como cualquier otro tipo de información que pueda facilitar el acceso no autorizado.
- La validación de los datos de acceso (cuenta de usuario, contraseña, etc.) se realizará únicamente cuando se hayan introducido todos los datos. Si alguno de los datos de acceso es incorrecto, el sistema no debería indicar de cual se trata. (Por ejemplo, nunca debería indicar si lo que se ha introducido de forma incorrecta es el nombre de usuario, o la contraseña, etc.).

4.5.3.2 Bloqueo de sesiones en los equipos personales

Cuando un usuario se ausente de su equipo de trabajo, aunque sea temporalmente, deberá bloquear la sesión. En cualquier caso, el sistema operativo activará automáticamente el salvapantallas al cabo de treinta (30) minutos, siendo necesaria la introducción de la contraseña para desactivarlo.

4.5.3.3 Cierre de sesiones de aplicaciones

Siempre que sea posible, las sesiones tendrán configurada una desconexión por tiempo de inactividad (time-out), de modo que una vez transcurrido dicho tiempo, la sesión se cerrará automáticamente. El valor de ese tiempo dependerá de cada aplicación, pero no debería ser superior a 2 horas.

Además, y siempre que sea posible, la duración máxima de las sesiones también estará limitada, de forma que tras un determinado periodo de tiempo será imprescindible que el usuario vuelva a autenticarse para poder mantener abierta la sesión. El valor de ese tiempo dependerá de cada aplicación, pero no debería ser superior a 12 horas.

Para cada aplicación el tiempo de inactividad debe ser inferior a la duración máxima de la sesión.

4.5.4 Control de Acceso a la red

Podrán establecerse controles de acceso a la red, tanto si el acceso es interno como si es remoto, implantando medidas de seguridad y procedimientos de autorización de acceso, según lo dispuesto en la Normativa de uso de la red de comunicaciones.

4.5.5 Control de acceso a bases de datos y aplicaciones

Se debe controlar de manera especial el acceso a las aplicaciones y bases de datos por la información sensible que contienen.

Los usuarios de administración con los que se acceda a las aplicaciones y/o bases de datos deben ser diferentes de los del acceso al sistema operativo.

4.5.6 Monitorización y trazabilidad de los accesos

Se deben realizar labores periódicas de monitorización y trazabilidad de los sistemas con el fin de detectar accesos anómalos o no autorizados a cualquier tipo de sistema de información. Para ello se registrarán los eventos que suministren evidencias en caso de producirse incidentes relativos a la seguridad. Todos los eventos de seguridad relacionados con los accesos lógicos a los sistemas de información se enviarán a un sistema centralizado (SIEM[5]) para su almacenamiento y gestión.

A tal efecto, se tendrán monitorizados, al menos, los siguientes eventos:

- Intentos exitosos y fallidos de autenticación del sistema.
- Usos de las cuentas con privilegios especiales del sistema.
- Bloqueos de cuenta por exceso de autenticaciones fallidas.
- Últimos accesos a cuentas.
- Inhabilitación de cuentas.

La hora de todos los sistemas debe estar sincronizada con el servicio de tiempo de la UAM (hora.uam.es) para garantizar la exactitud de los registros de tiempo.

Los sistemas de información que procesen, transmitan o almacenen información deben generar un registro de los accesos lógicos producidos, siempre que técnicamente sea posible, y bajo las siguientes características:

- Registro de eventos en orden cronológico, posibilitando la reconstrucción, revisión y examen de la secuencia de actividades relacionadas con un determinado evento.
- Registro de sucesos en todos los sistemas con el objeto de aportar las pruebas necesarias para el seguimiento de los mismos, en el caso de accesos no autorizados.
- Registro de accesos al sistema, actividades de administración y otros eventos críticos.
- Los registros de conexiones y otros eventos relativos a la seguridad se almacenarán durante al menos dos años. Dichos registros contendrán, como mínimo, la siguiente información:
    - Cuenta de Usuario.
    - Actividad realizada por el usuario.
    - Fecha / hora.
    - Activo o componente sobre el que se realiza la actividad.
    - Resultado de la actividad (correcto o erróneo).

- Uso de herramientas o utilidades que faciliten la revisión de los registros de eventos. Todos los sistemas de información deberán contar con medios para monitorizarlos y generar alarmas o alertas.
- Los ficheros de registro de eventos estarán protegidos lógicamente para prevenir su acceso no autorizado.
- Los sistemas de información que contengan datos de carácter personal catalogados como nivel alto en la LOPD, deberían implementar, siempre que ello sea posible, un registro de accesos a los datos de nivel alto que contenga la siguiente información:
    - Usuario que accede.
    - Fecha / hora del acceso.
    - Tipo de acceso (lectura, modificación o borrado).

[5] SIEM: https://en.wikipedia.org/wiki/Security_information_and_event_management

- Resultado del acceso (autorizado o denegado).
- Datos accedidos.

Además, ese registro debe guardarse por un tiempo mínimo de dos años.

4.5.7 Revisión de los registros

Los registros de eventos deberán ser revisados de acuerdo a las siguientes condiciones:

- El responsable del sistema o aplicación correspondiente o la persona que designe a tal fin revisarán los informes generados por el SIEM relativos a los registros de accesos privilegiados, con una periodicidad mínima de 6 meses, a no ser que exista alguna indicación diferente al respecto.
- El acceso a los registros estará restringido al responsable del sistema o aplicación correspondiente y a las personas designadas por éste. Se evitará el acceso de personas no autorizadas que puedan ver, alterar o eliminar registros.
- Cuando los registros de eventos muestren evidencias de problemas en la seguridad de los sistemas monitorizados, el responsable del sistema deberá generar un incidente de seguridad para su tratamiento de acuerdo con el procedimiento de gestión de incidentes de seguridad establecido.
- Los informes de registros de accesos generados por el SIEM correspondientes a ficheros LOPD de nivel alto serán revisados mensualmente por los órganos y/o personas encomendadas a esta tarea, que además elaborarán un informe de las revisiones realizadas y los problemas detectados.

5 Responsabilidades e incumplimientos

Todos los usuarios tienen la obligación de colaborar con TI para corregir, cesar y, en su caso, rectificar el ejercicio de acciones que incumplan esta normativa.

Aquellas personas que de forma reiterada, deliberada o por negligencia ignoren o infrinjan la presente normativa, podrán verse sujetas a las actuaciones técnicas (para minimizar los efectos de la incidencia) que se estimen oportunas.

Constatado un incumplimiento de las obligaciones derivadas de esta normativa, el Comité de Seguridad de la Información podrá instar la depuración de las responsabilidades disciplinarias a las que hubiera lugar.

El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de estudiantes, del personal al servicio de las Administraciones Publicas o de la propia UAM.

6 Disposición final

En el presente documento se utiliza el masculino gramatical como genérico, según los usos lingüísticos, para referirse a personas de ambos sexos.