I.2.15. Acuerdo 15/CG de 6-10-23 por el que se aprueba la modificación de la Normativa de gestión de identidades y control de acceso lógico de la Universidad Autónoma de Madrid.

NORMATIVA DE GESTIÓN DE IDENTIDADES Y CONTROL DE ACCESO LÓGICO DE LA UNIVERSIDAD AUTÓNOMA DE MADRID

(Aprobado en Consejo de Gobierno de 14 de julio de 2016 y modificada en Consejo de Gobierno de 6 de octubre de 2023)

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 las personas usuarias 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 quienes accedan a los servicios, 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 quienes utilicen el servicio por medio de técnicas de autenticación y autorización.

• Registrar y revisar los eventos y actividades llevados a cabo por quienes utilicen los servicios de los sistemas de información de la UAM.

• Informar a quienes utilicen el servicio 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 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

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 cualquier persona que acceda a los diferentes servicios, sistemas y demás recursos TIC 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 quienes utilicen los servicios 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:

• Quienes utilicen los servicios deben tener una relación formal y vigente con la UAM, perteneciendo al colectivo PDI, PTGAS, PI o estudiantado 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.

• Quienes utilicen los servicos deberán siempre autenticarse sin privilegios de sistema. Excepcionalmente, y sólo con fines de administración, podrán autenticarse como administradoras o administradores del mismo.

• Todos los sistemas de información de la UAM estarán dotados de mecanismos destinados a la identificación unívoca de quienes cuenten con autorización para acceder a ellos.

Quienes utilicen los servicios 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.

4.1 Tipos de cuentas

Se definen tres tipos de cuentas:

• Cuentas corporativas: Son todos aquellos identificadores asociados a personas físicas, utilizados para acceder a los sistemas de información de la UAM. Estas cuentas identifican unívocamente a la persona 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 la UAM agrupa las identidades corporativas de la UAM (PDI, PTGAS, PI, estudiantado y otros colectivos) y pretende asegurar la identificación única de la persona ante cualquier uso de la misma, así como el control de su ciclo de vida 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 corporativas es el siguiente:

• Alta: Creación de la cuenta 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 sea necesario o debido a cambios en 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, PTGAS y PI.

• Aplicación de gestión académica: Gestiona los datos del estudiantado.

• Aplicación de gestión de Alumni: Proporciona los datos del colectivo gestionado por la Oficina Alumni de la UAM.

Existen otros colectivos cuyos datos no están en las fuentes citadas (por ejemplo, personal no vinculado contractualmente con la UAM, colaboraciones, etc…). Para cada uno de ellos se define una persona 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 el servicio de autenticación y autorización para la mayor parte de los servicios que ofrece Tecnologías de la Información (en adelante, TI) por ejemplo: bibliotecas, correo electrónico, intranet (portal del empleado), carnet universitario, VPN, WiFi, telefonía IP, etc.

4.2.1 Funciones de la 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 corporativas para posibilitar la identificación segura.

• En función del colectivo correspondiente, seguimiento de la fecha fin de la relación para cada cuenta corporativa 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 cuentas corporativas de esta misma normativa.

• Asociación de los identificadores y cuentas corporativas 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 corporativa 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 corporativas genéricas. En el caso de cuentas de administración se asociará dicho rol al identificador de las personas que desarrollen estas funciones, siempre que sea posible técnicamente.

El servicio de gestión de identidades también permite registrar todos los cambios de credenciales realizados y el servicio desde el que se ha modificado.

4.2.3 Colectivos

Los colectivos considerados son los siguientes:

• Persona no corporativa: Se considerará persona no corporativa, en general, a cualquiera 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:

o Persona anónima: Se considerará persona anónima a cualquiera 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, quienes naveguen por las páginas web públicas de la UAM).

o Persona autenticada: Se considerará persona autenticada a quien 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.

o Persona solicitante de admisión: Quienes, sin formar parte de la comunidad universitaria, necesitan autenticarse para el inicio de trámites administrativos en algún servicio de la universidad por ejemplo, para las Pruebas de Acceso a la Universidad.

• Persona corporativa: Se considerará persona corporativa, 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:

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

o PTGAS: Se considerará PTGAS a quienes pertenezcan al personal técnico de gestión y de administración de 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.

o PDI: Se considerará PDI a quienes formen parte 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.

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

o Personal externo: Se considera personal externo a cualquier persona vinculada a un contrato administrativo suscrito con la UAM. En virtud de dicha relación deben poder acceder a los servicios electrónicos desplegados por la UAM para este colectivo. Esta condición se obtiene mediante la solicitud del PDI o PTGAS responsable del contrato administrativo asociado.

o Personal no vinculado: Se considerará personal no vinculado a cualquier persona que colabora con la UAM y que no teniendo relación de servicio ni contractual con la misma, necesita acceder a los servicios electrónicos desplegados por la UAM. Esta condición se obtiene mediante el aval del PDI o PTGAS responsable de su colaboración.

• Alumni: Se considerará Alumni a toda persona que esté inscrita en la Oficina Alumni (fundamentalmente exestudiantes, PTGAS 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 corporativas

Las cuentas corporativas 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 otras fuentes.

Una vez estas fuentes certifiquen el origen de la persona usuaria, esta será dada 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 su relación con la universidad, se verá reflejada en este sistema.

En el momento de finalizar la relación con la universidad, dejará de tener acceso a los servicios y sistemas que tuviera por pertenecer a su colectivo. Para algunos servicios podrá disponer de un periodo de extensión de acuerdo con la siguiente tabla:

Tipo Servicio Periodo de extensión del servicio

1 Sin periodo de extensión Listas de correo institucionales

Páginas blancas

2 Correo UAM Tres meses. Durante este periodo, la persona usuaria podrá activar las repuestas automáticas para informar al remitente de su nueva dirección de correo de contacto.

3 Correo Estudiantado Un año

4 Resto de Servicios 15 días

Estos periodos de extensión no se aplicarán en caso sanción disciplinaria. La suspensión de la relación como medida provisional adoptada durante la instrucción de un procedimiento disciplinario, podrá conllevar la suspensión inmediata de los servicios y sistemas.

4.3 Normas de seguridad en el uso de credenciales

4.3.1 Normas generales de obligado cumplimiento en el uso de contraseñas

Con independencia del tipo de cuenta, el uso de contraseñas debe cumplir las siguientes normas generales.

• Las contraseñas tendrán una longitud mínima específica para cada tipo de cuenta, y deberán contener caracteres de los siguientes tres tipos:

o Numérico

o Mayúsculas

o Minúsculas

• Las contraseñas no podrán contener caracteres en blanco.

• Las contraseñas no podrán estar formadas únicamente por palabras de diccionario u otras fácilmente predecibles o asociables a la persona titular de la cuenta (nombres, direcciones, matrículas, etc.)

• No está permitido el uso del nombre de la cuenta, ni el nombre ni los apellidos de la persona titular, como contraseña o parte de la misma.

• Cada persona responsable de mantener la confidencialidad de sus contraseñas.

• Las contraseñas son de uso exclusivo por la persona a la que pertenece la cuenta y no se comunicarán a nadie (ni siquiera a superiores o personal de TI) bajo ninguna circunstancia. Si alguna persona le solicitara la comunicación de sus credenciales, póngalo en conocimiento del CAU.

• Las contraseñas no se podrán escribir o enviar por medio alguno si no van cifradas. Las contraseñas no se guardarán sin cifrar, ni en los sistemas de información, ni por parte de la propia persona. En ningún caso se guardarán en soporte papel o informático de manera legible.

• Es recomendable cambiar periódicamente las contraseñas.

• No se podrán reutilizar las últimas seis (6) contraseñas.

• Si la persona usuaria sospecha que su identidad ha sido suplantada para acceder a cualquier servicio, debe cambiar de forma inmediata su contraseña. A continuación, lo pondrá en conocimiento de Tecnologías de la Información contactando con el Centro de Atención a Usuarios (CAU), que se encargará de tramitar la incidencia.

4.3.2 Uso de Múltiple Factor de Autenticación (MFA)

Debido al aumento de la actividad en el robo y venta de contraseñas, su uso por sí solo, no garantiza la seguridad en el acceso a los servicios. Por ello la UAM ha implantado el Múltiple Factor de Autenticación (en adelante MFA), que consiste en la introducción de una capa adicional de seguridad que complementa el uso de la contraseña y que refuerza el proceso de autenticación, garantizando la identidad de la persona usuaria y el acceso a la información por parte de la misma.

Para todos los servicios de la UAM que requieran autenticación, el refuerzo con MFA estará activado y será obligatorio para todas las cuentas corporativas y de Alumni.

4.3.3 Normas específicas para cada tipo de cuenta

Cuentas corporativas

Las cuentas corporativas 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 se bloqueará temporalmente tras un número determinado de intentos de accesos fallidos consecutivos según esté previsto por cada servicio.

• El bloqueo de cualquier cuenta se prolongará durante un tiempo mínimo de cinco minutos.

• Como buena práctica, se recomienda cambiar la contraseña una vez al año.

• Siempre que la aplicación lo soporte, se utilizará el servicio de gestión de identidades de la UAM para la validación de las credenciales de autenticación a través de comunicación cifrada.

Recomendaciones:

• Nunca se solicitarán las credenciales por ningún medio (correo electrónico, teléfono, etc.).

• No usar en la UAM las mismas contraseñas utilizadas fuera de la institución para acceder a otro tipo de servicios: cuentas de correo o servicios internet, comercio electrónico, banca, etc.

• Introducir sus contraseñas en ambiente de confidencialidad. Del mismo modo, facilite (retirándose, mirando para otro lado, etc.) la confidencialidad de quien debe introducir contraseñas en su presencia.

• Es una buena práctica 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.

Cuentas de aplicación y de administración

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 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 su cumplimiento o en su defecto de las contramedidas que reduzcan el riesgo al mínimo asumible.

Certificados digitales de empleado público de la UAM

La puesta a disposición de certificados electrónicos de empleada o empleado público al personal por parte de la UAM para el ejercicio de sus funciones exigirá, la aceptación de una serie de medidas de seguridad comunes, y otras específicas en función del dispositivo donde se almacene el certificado electrónico.

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

• La persona deberá acudir personalmente a la ODA (Oficina de Acreditación) mostrando su DNI (Documento Nacional de Identidad) o NIE (Número de Identidad de Extranjero).

• Aportará, 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 donde se almacene el certificado electrónico son:

• Si el dispositivo de almacenamiento es el Carné Universitario son:

o 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.

o No se 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:

• Es obligatorio habilitar una protección segura de la clave privada, mediante la configuración de una contraseña de acceso al almacén de certificados, que será solicitada cada vez que una aplicación la use. No se revelará esta contraseña a ninguna persona bajo ninguna circunstancia.

• Durante el proceso de instalación de este certificado electrónico se debe configurar de forma que la clave primaria del certificado electrónico no sea exportable posteriormente.

• Si el dispositivo de almacenamiento es un almacén centralizado se deberán implementar las medidas de seguridad necesarias para garantizar la custodia efectiva de los certificados electrónicos.

Otros sistemas de autenticación

Cuando los mecanismos de identificación y autenticación se fundamenten en métodos distintos a la utilización tradicional de identificador/contraseña, 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.

4.3.4 Cambio de contraseña

Si una persona usuaria sospecha que su contraseña ha sido comprometida o las ha cedido a terceras personas autorizadas por motivos de trabajo o mantenimiento, debe proceder a sustituirla por otra de manera inmediata.

Por otro lado, la persona usuaria debe realizar una petición de cambio de contraseña al CAU cuando se produzca alguna de las situaciones siguientes:

• Olvido de la contraseña de acceso.

• Bloqueo del acceso tras el número de intentos de acceso fallidos determinados por el sistema.

Existe un servicio que permite a la persona usuaria modificar la contraseña en cualquier momento. En el caso de olvido de la contraseña, podrá generar automáticamente una nueva siempre y cuando haya facilitado previamente al sistema un teléfono móvil y/o correo alternativo. En caso contrario deberá acudir presencialmente al CAU acreditando su identidad.

4.4 Gestión de derechos de acceso

4.4.1 Tipos de derechos de acceso y principios básicos de gestión

La gestión de los derechos de acceso 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, la persona 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.

Los derechos de acceso a un activo se limitarán atendiendo a los siguientes principios:

• Todo acceso a un activo estará prohibido, salvo autorización expresa.

• Mínimo privilegio: los privilegios se reducirán al mínimo imprescindible para cumplir sus obligaciones o funciones.

• Los privilegios se asignarán de forma que sólo se accederá al conocimiento de aquella información requerida para cumplir sus obligaciones o funciones. La información es patrimonio de la UAM y toda aquella que resulte necesaria estará disponible.

• Exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los activos, conforme a los criterios establecidos por su responsable. Los permisos de acceso se revisarán de forma periódica.

• Existe una normativa específica donde se recoge la obligación de autorización expresa para el acceso remoto a los activos.

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 corporativa respecto de cada activo vienen determinados por:

o Los colectivos a los que pertenece la persona (por ejemplo: PTGAS, PDI, Alumni, etc.).

o Las labores específicas que dicha persona desarrolla dentro de su colectivo (centro, departamento, cargo, etc.).

o 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 corporativa respecto de cada activo.

• Siempre que sea posible, la asignación y retirada de privilegios de cada cuenta corporativa 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 corporativa tenga en función de su rol.

4.4.2 Gestión de privilegios y sus responsabilidades

La asignación, modificación o revocación de privilegios en los servicios de la UAM será solicitada por las personas responsables del departamento o área a la que pertenezca la persona usuaria destinataria de dichos privilegios.

La información que contenga datos de carácter personal será accesible únicamente por personal debidamente autorizado en el ejercicio de sus responsabilidades.

Quedarán registrados los privilegios de acceso de cada persona usuaria concedidos para cada uno de los servicios, así como las modificaciones y bajas que sufran a lo largo del tiempo.

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 las personas anónimas debido a sus características intrínsecas.

• La gestión del resto de personas no corporativas se lleva a cabo de manera independiente y el único privilegio que se les concede es el acceso al servicio específico relacionado con el seguimiento de sus trámites.

• La gestión de personas corporativas y Alumni se lleva a cabo de la siguiente manera:

o La gestión de los privilegios de acceso a los activos se lleva a cabo de manera centralizada y automatizada.

o La gestión de las excepciones se lleva a cabo de manera específica por aplicación y cuenta, de forma manual. Dicha gestión la realiza quien administra cada servicio.

• La gestión de cuentas de administración se lleva a cabo de forma manual e individualizada en cada servicio.

• La gestión de cuentas de aplicación se lleva a cabo de forma manual e individualizada en cada servicio.

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 servicios 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 servicios de la UAM son los siguientes:

• Con la excepción de los servicios de acceso público, el acceso a los servicios de la UAM requerirá siempre de autenticación previa.

• Siempre que ello sea posible, el control de acceso a los servicios 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.

• El control de acceso se realizará siempre siguiendo el principio de mínimo privilegio. Excepcionalmente, y sólo con fines de administración, se asignarán privilegios superiores.

• En todo momento se deberá hacer un uso responsable de la información y de los servicios 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 que permita la monitorización de dichos eventos y garantice los periodos de retención legalmente establecidos.

• Todas las contraseñas asignadas a las cuentas corporativas 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.

El proceso de autenticación en cuentas corporativas y Alumni para el acceso a todos los servicios debe incluir el uso de MFA como refuerzo al uso único de contraseñas.

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, las administradoras y administradores de seguridad de cada servicio llevarán a cabo un proceso formal, a intervalos regulares de no más de un año, a fin de revisar los derechos de acceso de las personas administradoras.

Para el caso de quienes 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. Se habitarán procesos que comprueben automáticamente que el control de acceso dispuesto es el correcto.

4.5.3 Control de acceso a los equipos informáticos y aplicaciones

Para el acceso a aplicaciones y equipos 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), las personas usuarias con una cuenta creada y asignada por la persona encargada de la administración, que les permitirá realizar en dicho activo únicamente las acciones que le hayan sido encomendadas.

Inicio seguro de sesión

El acceso a estos activos estará protegido mediante un inicio seguro de sesión, que contemplará las siguientes condiciones:

• En función del tipo de activo (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 personas autorizadas.
• 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 (identificador/contraseña) 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. Nunca debería indicarse si lo que se ha introducido de forma incorrecta es el identificador o la contraseña.

Bloqueo de sesiones en los equipos personales

Cuando una persona usuaria 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 diez minutos, siendo necesaria la introducción de la contraseña para desactivarlo.

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 volver 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 de la UAM.

4.5.5 Control de acceso a bases de datos

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

Las cuentas de administración con los que se acceda a las 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) 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.

• Cambio de contraseñas

• Auditoria de cambios de MFA

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:

o Dirección IP origen de la conexión.

o Identificador de persona.

o Actividad realizada.

o Fecha / hora.

o Activo o componente sobre el que se realiza la actividad.

o 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.

4.5.7 Revisión de los registros

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

• El administrador o administradora de seguridad del servicio o aplicación correspondiente o la persona que designe a tal fin revisará los informes generados por el SIEM relativos a los registros de accesos privilegiados (cuentas de administración), con una periodicidad mínima de 6 meses, a no ser que exista alguna indicación diferente al respecto.

• El acceso a los registros estará restringido a la administradora o administrador de seguridad del servicio 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 durante la revisión de los registros el administrador o administradora de seguridad detecte un incidente de seguridad, deberá notificarlo vía gestor de incidencias a CERT-UAM y a la persona responsable del sistema para su tratamiento de acuerdo con el procedimiento de gestión de incidentes de seguridad establecido.

5. Responsabilidades e incumplimientos

Todos las personas usuarias tienen la obligación de colaborar con Tecnologías de la Información 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 luga

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.