I.2.5. Acuerdo 5/ CG 14-07-16 por el que se aprueba la Normativa general de uso de recursos TIC y sistemas de información de la Universidad Autónoma de Madrid.

1 Introducción

Conforme a lo dispuesto en el 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 (en adelante ENS), este documento contiene la normativa general de utilización de los recursos TIC y sistemas de información de la Universidad Autónoma de Madrid (en adelante UAM), gestionados y bajo la responsabilidad de Tecnologías de la Información (en adelante TI), señalando asimismo los compromisos que deben adquirir los usuarios respecto a la seguridad de la información (en adelante seguridad) y buen uso de estos recursos TIC.

Esta normativa se complementa con aquella que regula de manera específica las obligaciones de los usuarios en el uso de los recursos TIC en ámbitos tales como la gestión de accesos, el uso del correo electrónico, la gestión de identidades, el uso de la red de comunicaciones, etc.

2 Objetivo

Los recursos TIC[1] y sistemas de información constituyen elementos básicos para la UAM. Por tanto, sus usuarios deben utilizar estos recursos y sistemas de manera que se preserven en todo momento las dimensiones de seguridad (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) tanto de la información como de los servicios.

La utilización de recursos tecnológicos para el tratamiento de la información tiene una doble finalidad para la UAM:

- Facilitar y agilizar el desarrollo de la actividad docente e investigadora, así como las tareas administrativas necesarias para su funcionamiento, mediante el uso de redes de comunicación, herramientas informáticas y aplicaciones.
- Proporcionar información completa, homogénea, actualizada y fiable.

La utilización de equipamiento informático y de comunicaciones es actualmente una necesidad en cualquier organización del sector público. Estos medios y recursos se ponen a disposición de los usuarios como instrumentos de trabajo para el desempeño de su actividad profesional, razón por la cual compete a la UAM determinar las normas, condiciones y responsabilidades bajo las cuales se deben utilizar tales recursos tecnológicos.

[1] 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".

Por tanto, la presente Normativa General tiene como objetivo establecer y desplegar normas encaminadas a alcanzar la mayor eficacia y seguridad en su uso.

3 Ámbito de aplicación

La presente 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. Se aplicará a todo "recurso TIC de la UAM" y a cualquier dispositivo conectado (de forma local o remota) a la red de la UAM.

Esta normativa afectará a todos los usuarios. Conforme a definición recogida en la Política de Seguridad de la Información de la UAM, se entiende como usuario a toda persona que haga uso de los 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 los usuarios para el ejercicio de sus funciones, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.

4 Normas técnicas de uso de recursos TIC y sistemas de información

La presente normativa regula el marco general de los usos de los recursos TIC y los sistemas de información de la UAM.

4.1 Uso aceptable y obligaciones de los usuarios

1. Para acceder a los sistemas de información de la UAM es necesario tener asignada previamente una cuenta de usuario. La autorización del acceso se establecerá en función del perfil de cada usuario. Cada perfil tendrá configuradas las funcionalidades y privilegios disponibles en las aplicaciones según las competencias atribuidas a cada usuario. Se adoptará la política de asignación de los privilegios mínimos necesarios para la realización de las funciones encomendadas.
2. En todo momento se debe hacer un uso ético y legal de los recursos TIC que la UAM pone a disposición de los usuarios.
3. Los recursos TIC deben utilizarse únicamente para el desarrollo de las funciones encomendadas de conformidad con la relación del usuario con la UAM.
4. Los equipos informáticos facilitados y configurados por la UAM para su utilización por parte de los usuarios (incluyendo portátiles, pc de sobremesa, tabletas, cualquier otro dispositivos móviles con capacidad de acceso a los sistemas de información) constituyen un elemento esencial en la cadena de seguridad de los sistemas de información.
5. Únicamente el personal autorizado por TI podrá distribuir, instalar o desinstalar software y hardware, o modificar la configuración de cualquiera de los elementos de la infraestructura de los sistemas de información de la UAM, especialmente en aquellos aspectos que puedan repercutir en la seguridad de los mismos.

6. Los usuarios no tendrán privilegio de administrador sobre los recursos TIC, salvo autorización expresa del responsable de Seguridad de la UAM o de aquel en quien delegue tal competencia. El privilegio de administrador se solicitará por el usuario mediante escrito motivado en el que describa su necesidad. La autorización sólo podrá denegarse si los usos para los que se solicita tal privilegio supusieran un riesgo potencial para la seguridad de la información de la UAM. Concedida la autorización, el usuario se compromete a usar su privilegio de administrador de conformidad con lo dispuesto en esta normativa, asumiendo la responsabilidad correspondiente en caso de incumplimiento de lo aquí previsto.

7. Quien detectase cualquier anomalía que indicase una utilización de los recursos TIC contraria a la presente normativa, lo comunicará al Responsable de Seguridad a través del Centro de Atención a Usuarios (CAU), que tomará las medidas oportunas.

8. Cada recurso TIC de la UAM deberá estar asignado a un usuario o responsable concreto. Tales usuarios son responsables de su correcto uso.

9. Se permite la instalación de cualquier software siempre que se cuente con la correspondiente licencia y su uso sea consecuente con los fines de la universidad.

10. El usuario se compromete a garantizar la privacidad de la información sensible, confidencial y protegida, propiedad de la UAM, que está accesible desde los recursos TIC y a evitar la difusión de la misma.

11. Cuando un usuario deje de atender un equipo informático durante un cierto tiempo, es necesario bloquear la sesión de usuario o activar el salvapantallas, siendo necesaria la introducción de la contraseña para desactivarlo. Con ello se evitará que alguna persona pueda hacer un mal uso de sus credenciales, pudiendo llegar a suplantarlo.

12. Cualquier documento, soporte informático, dispositivo de almacenamiento que pueda contener datos de carácter personal o información confidencial deberá protegerse frente a posibles revelaciones o robos de terceros no autorizados. En caso de considerarse necesario, esa información deberá almacenarse de forma cifrada.

13. Se deben seguir las normas y procedimientos definidos y tomar las medidas de seguridad para el uso de recursos TIC en las instalaciones de la UAM.

14. Las medidas mínimas de seguridad que deben cumplir los usuarios respecto de los equipos informáticos en el ámbito de la UAM son:

    - Firewall activado en el caso del sistema operativo Windows.
    - Actualizaciones de seguridad de todo el software instaladas en todos los sistemas operativos.
    - Antivirus instalado y actualizado en todos los sistemas operativos en los que esté disponible. En el caso de los equipos suministrados por TI será el antivirus corporativo.
    - Inclusión en el dominio corporativo (directorio activo) en el caso del sistema operativo Windows para los equipos suministrados por TI.

4.2 Uso no aceptable

1. Se prohíbe la utilización en el equipamiento informático de cualquier tipo de software dañino.
2. Queda explícitamente prohibido que los usuarios revelen o entreguen sus credenciales de acceso a los recursos, tarjeta criptográfica o certificados electrónicos a otras personas, ni mantenerlas por escrito o a la vista o alcance de terceros.
3. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización de su titular.
4. No se podrá instalar o utilizar software que no disponga de la licencia correspondiente o cuya utilización no sea conforme con la legislación vigente en materia de Propiedad Intelectual.
5. Se prohíbe la reproducción, modificación, distribución o uso fuera del ámbito establecido por la UAM, de los programas y aplicaciones informáticas instaladas en los equipos que pertenecen a la universidad.
6. En ningún caso se podrán eliminar o deshabilitar las aplicaciones informáticas relacionadas con la seguridad, tales como: antivirus corporativo, anti-spam, cortafuegos, etc.
7. No está permitido almacenar información de carácter privado en los recursos de almacenamiento compartido.
8. No está permitida la utilización de programas que, por su naturaleza, hagan un uso abusivo de la red y resto de recursos TIC de la UAM.
9. No se podrá modificar la configuración de cualquiera de los equipos, especialmente en aquellos aspectos que puedan repercutir en la seguridad de los recursos TIC de la UAM.
10. Se prohíbe toda transmisión, distribución o almacenamiento de cualquier material obsceno, difamatorio, amenazador o que constituya un atentado contra la dignidad de las personas.
11. Se prohíbe la degradación de los servicios, recursos informáticos de la UAM o de otras instituciones.
12. No se podrá proceder a la destrucción o modificación no autorizada de la información de la UAM, de manera premeditada.
13. Se prohíbe toda actuación que pueda suponer la violación de la intimidad, del secreto de las comunicaciones y del derecho a la protección de los datos personales.
14. Se prohíbe el uso de los sistemas de información para fines ajenos a los de la UAM.
15. Se prohíbe, en general, cualquier uso de los sistemas de información de la UAM contrario a la legalidad vigente.

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.