UNIVERSIDAD
DE MÁLAGA

REGLAMENTO DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN DE LA UNIVERSIDAD DE MÁLAGA

(Aprobado en el Consejo de Gobierno de la Universidad de Málaga el 19 de Julio de 2013)

EXPOSICIÓN DE MOTIVOS

La Política de Seguridad de la Universidad de Málaga, aprobada por Acuerdo del Consejo de Gobierno de fecha 20 de diciembre de 2012 supone un marco general sobre el tratamiento de la seguridad de la información en el ámbito de nuestra universidad que debe ser desarrollado con normativas más específicas. La creciente importancia de los sistemas de información en todas las actividades de la vida universitaria, incide en la relevancia de la seguridad de la información. Por ello, deben adoptarse las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados, garantizando al mismo tiempo la disponibilidad continuada de estos servicios.

ARTÍCULO 1. OBJETO Y ÁMBITO DE APLICACIÓN

1.1 El objetivo de esta normativa es proteger los recursos de información de la Universidad de Málaga y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

1.2 La presente normativa es de aplicación a todos los usuarios de la red de datos de la Universidad de Málaga (RedUMA).

ARTÍCULO 2. UTILIZACIÓN DE LOS EQUIPOS INFORMÁTICOS DE LA UMA

2.1. La Universidad de Málaga pondrá a disposición de su personal los medios y equipos informáticos que necesiten para el cumplimiento de sus obligaciones laborales. En consecuencia, dichos equipos informáticos no están destinados al uso personal o extraprofesional.

2.2. Los usuarios deberán utilizar los equipos informáticos, destinados a la docencia y a la gestión universitaria de los que sean proveídos, para usos compatibles con las funciones de la unidad a la que se encuentren adscritos.

2.3. Los usuarios deberán cuidar los equipos informáticos que les sean facilitados, no procediendo al alterarlos ni a modificarlos.

2.4. Queda prohibida expresamente la instalación de aplicaciones informáticas sin la correspondiente licencia o no adecuándose a la legislación vigente. Asimismo se excluirá la instalación o visualización de salvapantallas, fotos, videos, comunicaciones u otros medios con contenidos ofensivos, violentos, amenazadores, obscenos o, en general, aquellos que agredan la dignidad de la persona.

ARTÍCULO 3. CONEXIÓN A RedUMA

3.1. RedUMA es el conjunto de todos los recursos tanto físicos como lógicos que permiten el transporte de información de los distintos ordenadores existentes en la Universidad que estén conectados a la misma.

Se considera que un ordenador o dispositivo es miembro de RedUMA y está sujeto a esta normativa si:

a) Se encuentra conectado a la red informática desde cualquiera de los puntos de acceso que se facilitan a este efecto en los campus universitarios, ya sean éstos cableados o inalámbricos.

b) Está conectado a la Universidad de Málaga usando alguno de los métodos de acceso remoto que ésta proporciona.

3.2. Todos los equipos que se conecten a RedUMA deberán estar correctamente identificados en las condiciones que, para cada caso, se determinen en la normativa de acceso correspondiente. deben tener la configuración de red indicada por el SCI, además de ser incluidos en el registro correspondiente, junto con la identidad de los responsables del equipo.

3.3. Los responsables de los equipos conectados a RedUMA deben asegurarse de tener instalados los parches de seguridad, antivirus y actualizaciones de sistemas operativos y software que desde la Universidad de Málaga se les recomiende.

3.4. Se considera aceptable usar la red para acceder a u ofrecer información siempre que esté de alguna forma relacionada con el entorno universitario, que no viole derechos de propiedad intelectual, y que este uso se realice de forma eficiente a fin de evitar perjuicios a terceros.

3.5. No se considera aceptable y no puede ser usada la red bajo ningún concepto para:

a) Cualquier acto que viole la legalidad vigente o las normativas de las redes en las que RedUMA está integrada (RICA, RedIRIS).
b) Fines privados comerciales.
c) La búsqueda de claves de acceso de otros usuarios o cualquier intento de encontrar y explotar fallos en la seguridad de los sistemas informáticos de la Universidad de Málaga o de fuera de ella, o hacer uso de aquellos sistemas para atacar cualquier sistema informático.
d) Intentar acceder a la información de otro usuario que no haya sido puesta explícitamente de acceso público.
e) La creación, utilización y difusión de cualquier tipo de material que ponga en peligro la seguridad de la red, que esté destinado a sabotear el uso de la red o que cause molestias o daños a otros usuarios.
f) La conexión a la red de cualquier elemento físico o lógico que modifique la topología de la red ni la utilización de direcciones de red sin que hayan sido previamente autorizadas.
g) La manipulación de los componentes de RedUMA, tanto activos como pasivos o los mecanismos que les proporcionan suministro eléctrico.
h) La facilitación de acceso a la infraestructura de red y a los servicios ofertados a personas u organizaciones ajenas a la Universidad fuera de los cauces que se establezcan. sin autorización expresa.

3.6. Cuando se detecte un uso incorrecto, se podrá decidir la suspensión del servicio a cualquier usuario o entidad conectada a ella en una de las dos formas siguientes:

a) Suspensión temporal o de emergencia del servicio, cuando la violación de las normas indicadas en este documento esté causando o pueda estar causando una degradación de los servicios de la red y/o implique a la Universidad de Málaga en algún tipo de responsabilidad, así como cuando suponga una modificación de la topología de RedUMA o una conexión no autorizada. Está decisión se tomará por el Administrador de la red y se restablecerá la conexión en el momento en que se compruebe que el motivo de la suspensión se ha eliminado.

b) Si se producen infracciones de una especial gravedad, o una reiteración de las mismas, la Universidad de Málaga podrá suspender indefinidamente la conexión a red de un usuario, restableciéndose el servicio cuando se considere que se dan las condiciones necesarias para ello.

ARTÍCULO 4. IDENTIFICACIÓN DE USUARIOS

4.1. Una cuenta de servicio es un identificador unívoco que permite a una persona, en virtud de su vinculación a la Universidad de Málaga, el acceso a un conjunto de servicios.

Las cuentas de servicio son personales e intransferibles. La Universidad de Málaga se reserva el derecho de aceptar o no la creación de cuentas. Asimismo, la Universidad de Málaga podrá, sin previo aviso, suspender o cancelar cuentas por uso indebido, sin perjuicio de imponer las sanciones que pudieran corresponder.

4.2. Los identificadores de cada cuenta de servicio son gestionados mediante el Servicio de Directorio Centralizado de la Universidad de Málaga (DUMA) y se constituyen como el único método de control de acceso a los servicios telemáticos institucionales.

Claves de acceso

4.3. Las claves de los usuarios se guardarán en un único punto de almacenamiento, iDuma, cifrada con un algoritmo de vía única que no permita la reconstrucción de la misma.

4.4. El acceso a todos los servicios identificados por iDUMA se hará mediante protocolos cifrados.

4.5. Se proveerá a los usuarios de mecanismos para cambiar la clave y generar una nueva en caso de olvido.

4.6. Como norma general, la Universidad de Málaga no forzará el cambio de clave por antigüedad de la misma, pero sí se recomienda a los usuarios su cambio cuando se sospeche que pueda ser conocida.

4.7. Dado que la clave es llave de acceso a datos protegidos, y se podría usar para hacer responsable a su propietario de acciones que no ha realizado, el usuario no debe compartir la clave con otras personas ni cederla a otras entidades.

4.8. Se establecerán las medidas necesarias para evitar un mal uso de las claves, o minimizar sus consecuencias al tiempo que proveerá mecanismos de identificación no basados en clave como los certificados digitales o el DNI electrónico.

4.9. Los procedimientos de asignación de claves informarán a los usuarios del nivel de calidad de la misma. Para que la clave sea de calidad se recomienda:
- Un mínimo de 14 caracteres que incluyan tanto alfabéticos como numéricos.
- No utilizar palabras contenidas en los diccionarios ya que se utilizan para la realización de ataques de usurpación de claves.
- Que sea fácil de recordar por el usuario pero no fácil de relacionar con él.

Debe tenerse en cuenta que el uso de caracteres nacionales como la ñ o las vocales acentuadas podría dificultar su acceso en teclados donde estos no aparezcan (por ejemplo si se viaja al extranjero).

ARTÍCULO 5. CONDICIONES EN QUE SE PRESTAN LOS SERVICIOS

5.1. La Universidad de Málaga presta servicios telemáticos a los miembros de la Comunidad Universitaria para facilitar la realización de sus tareas.

5.2. La creación de nuevos servicios telemáticos deberá contar con la aprobación previa de la Comisión de Seguridad de la Universidad de Málaga.

5.3. La Universidad de Málaga, a través de sus órganos de gobierno de carácter general, y de acuerdo con los normas específicas establecidas al efecto, podrá establecer prácticas generales y limitaciones con respecto al uso de los recursos y servicios.

5.4. La Universidad de Málaga, en cumplimiento de lo dispuesto por la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) guarda registro del uso de las cuentas de los usuarios y de los recursos y servicios de RedUMA, para poder determinar en caso de un mal uso las posibles responsabilidades de sus usuarios.

5.5. Se respetará en los términos establecidos por las normas la privacidad del contenido de los mensajes de correo electrónico, sin menoscabo de la capacidad de la Universidad de Málaga para la aplicación sistemática de programas de detección y eliminación de virus y programas de filtro anti-spam a los mensajes que llegan a la estafeta de la Universidad.

5.6. En cumplimiento de lo dispuesto por la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD), se hará un seguimiento de los accesos que sus usuarios realicen o intenten realizar a los ficheros con datos personales cuya titularidad corresponda a la universidad.

5.7. Todo el personal de la Universidad de Málaga que por su trabajo tenga acceso a información de carácter personal debe cumplir con la obligación de secreto y confidencialidad, lo que no excluye la posibilidad de que, en estricto cumplimiento de los pertinentes requerimientos judiciales o, en su caso, autoridad legalmente autorizada, deban revelarse estos contenidos.

5.8. La Universidad de Málaga utilizará todos los mecanismos de que disponga para garantizar la seguridad de los servicios ofertados. En virtud de los principios de responsabilidad y autoprotección, los usuarios deberán adoptar todas aquellas medidas que se establezcan para garantizar la seguridad de los sistemas informáticos de la Universidad.

ARTÍCULO 6. SISTEMAS DE INFORMACIÓN UNIVERSITARIOS

6.1. La Universidad de Málaga reconoce expresamente la importancia de los Sistemas de Información, así como la necesidad de su protección, por constituir un activo estratégico y vital. Esta necesidad de protección está establecida en la legislación española, y se aplica en defensa de los intereses de todos y cada uno de los miembros de la comunidad universitaria, proveedores, y otros posibles afectados.

6.2. Se establecerán los medios necesarios y adecuados para la protección de datos, programas, equipos, instalaciones, documentación y otros soportes que contengan información, y en general de cualquier activo de la Universidad de Málaga.

6.3. Los accesos a los Sistemas de Información Institucional de la Universidad de Málaga se realizarán mediante el identificador único recogido en iDUMA, de manera que aquellas operaciones realizadas por un usuario, serán imputadas al identificador utilizado. No se permitirá, pues, el acceso a los sistemas a través de usuarios genéricos.

6.4. Cada usuario sólo podrá realizar las tareas y acceder a los datos necesarios que se requieran para cumplir su cometido, es decir se considerará el principio del llamado "mínimo privilegio". Asimismo usarán los datos accedidos únicamente para las operaciones para las que fueron generados e incorporados, sin destinarlos a otros fines o incurrir en actividades que puedan considerarse ilícitas o ilegales.

6.5. Se registrarán pistas de auditoría y seguimiento de actividad de los accesos. Estos rastros, en el caso de modificación de datos personales, incluyen la identificación del usuario, la fecha y hora del acceso y la operación realizada.

6.6. No está permitida la instalación, por parte de los usuarios, de cualquier aplicación o producto informático en los Sistemas de Información. sin autorización expresa.

6.7. Para los equipos que contengan o tengan acceso a datos personales, se establecerá su tipo de configuración y el nivel de acceso a redes internas o externas de forma que se garantice la seguridad de dicha conexión.

6.8. Las empresas proveedoras con acceso a los Sistemas de Información, deberán cumplir con el presente reglamento así como con las indicaciones que en materia de seguridad les haga la Universidad y, especialmente, con las contempladas para este tipo de accesos en la LOPD.

ARTÍCULO 7. CORREO ELECTRÓNICO

7.1. La Universidad de Málaga pone un buzón personal de correo electrónico a disposición de cada uno de sus miembros que sirve como medio de comunicación básico, eficiente, homogéneo, y gratuito para apoyar la realización de las actividades universitarias.

7.2. El servicio institucional de correo electrónico tiene como elemento principal la Estafeta Central por la que se encamina todo el correo entrante y saliente de la Universidad de Málaga. La Universidad de Málaga dispone también de servidores para contener los buzones personales que se asignan a cada miembro de la Universidad cuando ingresa en ella, y los buzones institucionales que puedan crearse.

7.3. Los usuarios son responsables legales de cualquier actividad que se pueda realizar desde las cuentas asociadas a sus buzones de correo personales, por lo que no deben permitir que nadie más que ellos puedan utilizarlas.

Envío de mensajes

7.4. A fin de evitar saturaciones que puedan afectar al buen funcionamiento del servicio, el tamaño máximo de los mensajes que se pueden enviar está limitado, fijándose dicho límite en función de los recursos disponibles en cada momento.

7.5. Es ilegal y estará penalizada la falsificación de cabeceras del correo electrónico.

7.6. No está permitida la utilización de las cuentas de correo personales de la Universidad de Málaga para el envío de publicidad ni para enviar correo a personas que han expresado su deseo de no recibirlo.

7.7. No puede enviarse mensajes a través de la estafeta de la Universidad de Málaga con direcciones de origen que no sean “uma.es”.

7.8. En ningún caso se podrá utilizar el servicio de correo electrónico de forma que interfiera con el rendimiento del servicio o con las labores propias de los gestores del servicio. Este apartado engloba la prohibición explícita de prácticas englobadas en los tipos definidos de Abuso de Correo Electrónico (ACE).

7.9. Los usuarios deben ser conscientes de que la dirección de correo electrónico @uma.es informa de su relación con la institución universitaria a diferencia de las direcciones ofrecidas por cualquier proveedor de Internet.

Recepción de mensajes

7.10. Con carácter general, la estafeta central de la Universidad de Málaga sólo admitirá mensajes dirigidos a los dominios propios de la Universidad de Málaga y sus subdominios registrados. Tampoco se reenviarán ni se redirigirán mensajes con destino a direcciones del dominio @uma.es o cualquiera de sus subdominios a servidores externos de la red de la Universidad de Málaga.

ARTÍCULO 8. PUBLICACIÓN DE CONTENIDOS EN LA WEB

En el uso del servicio de alojamiento de contenidos web, deberá tenerse en cuenta lo dispuesto por la Ley Orgánica de Protección de Datos de Carácter Personal en todos aquellos contenidos que presenten datos de carácter personal. En especial, se evitará hacer públicos mediante este servicio datos personales salvo que esté legalmente establecido. En cualquier caso, se recomienda que sólo se permita el acceso a información personal al interesado. Es también necesario caducar estos documentos cuando haya concluido el período razonable de exposición.

ARTÍCULO 9. DOMINIOS ESPECÍFICOS DISTINTOS DEL CORPORATIVO 'UMA.ES'.

9.1. La Universidad de Málaga tiene asociado el dominio uma.es como dominio corporativo.

9.2. La creación de dominios alternativos, subdominios bajo uma.es y asignación de nombres a servicios, requerirán autorización previa de la UMA mediante el procedimiento que se regule en la normativa correspondiente.

DISPOSICIÓN ADICIONAL ÚNICA

Todos los términos contenidos en este Reglamento, en el que se utiliza la forma del masculino genérico, se entenderán aplicables a personas de ambos sexos.

DISPOSICIÓN FINAL

Las presentes normas entrarán en vigor al día siguiente de su aprobación por el Consejo de Gobierno de la Universidad de Málaga, debiendo publicarse en el Boletín Oficial de la Junta de Andalucía.

ANEXO: GLOSARIO

AUTENTICIDAD
Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.

CONFIDENCIALIDAD
Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

DATOS DE CARÁCTER PERSONAL
Cualquier información concerniente a personas físicas identificadas o identificables. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

DISPONIBILIDAD
Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.

DOMINIO
Identificación asociada a un grupo de dispositivos o equipos conectados a internet. Por ejemplo uma.es

DOMINIO ALTERNATIVO
Dominio distinto a uma.es gestionado por la Universidad de Málaga.

INCIDENTE DE SEGURIDAD
Suceso inesperado o no deseado con consecuencias en detrimento de la seguridad del sistema de información.

INFORMACIÓN INSTITUCIONAL
Información surgida de los procesos de gestión universitaria.

INTEGRIDAD
Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.

MEDIDAS DE SEGURIDAD
Conjunto de disposiciones encaminadas a protegerse de los riesgos posibles sobre el sistema de información, con el fin de asegurar sus objetivos de seguridad. Puede tratarse de medidas de prevención, de disuasión, de protección, de detección y reacción, o de recuperación.

SEGURIDAD DE LA INFORMACIÓN
Protección de la información y de los sistemas de información frente al acceso, uso, divulgación, alteración, modificación o destrucción no autorizadas, con el fin de proporcionar confidencialidad, integridad y disponibilidad.

SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN
Es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

SERVICIOS TELEMÁTICOS INSTITUCIONALES
Servicios telemáticos ofertados a la comunidad universitaria que contribuyen al cumplimiento de los objetivos de la institución.

SISTEMAS DE INFORMACIÓN INSTITUCIONAL UNIVERSITARIOS
Conjunto organizado de recursos para que la información institucional se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir.

SUBDOMINIO
Dominio que forma parte de otro dominio más general. Por ejemplo centro.uma.es.

TRAZABILIDAD
Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.