I.2.22. Acuerdo 22/ CG 16-07-15 por el que se aprueba la Política de Seguridad de la Información de la Universidad Autónoma de Madrid.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD AUTÓNOMA DE MADRID

Índice

1. Consideraciones previas

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

2. Aprobación y entrada en vigor

Texto aprobado por Acuerdo del Consejo de Gobierno de la Universidad Autónoma de Madrid de 16 de julio de 2015.

Esta Política de Seguridad de la Información entrará en vigor al día siguiente de su publicación en el BOUAM, y desde ese momento será de obligado cumplimiento para quienes se encuentren dentro del ámbito de aplicación de esta normativa.

Quedan derogadas las disposiciones de igual o inferior rango aprobadas por la UAM que se opongan a lo dispuesto en la presente Política de Seguridad de la Información.

3. Marco legal

Esta Política de Seguridad de la Información se dicta de conformidad con lo dispuesto en las leyes y reales decretos siguientes:

● Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, y legislación que la desarrolle (en adelante, Ley 11/2007).

● 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, Real Decreto 3/2010).

● Ley 59/2003, de 19 de diciembre, de firma electrónica y legislación que la desarrolle.

● Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y legislación que la desarrolle (en adelante, LOPD).

● Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica.

● Ley Orgánica 6/2001, de 21 de diciembre, de Universidades; y Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades.

4. Objetivo de la Política de Seguridad de la Información

La consagración del derecho de los ciudadanos a comunicarse con las Administraciones Públicas a través de medios electrónicos ha sido determinante para que el artículo 42.2 de la Ley 11/2007 dispusiera la creación del Esquema Nacional de Seguridad (en adelante ENS), cuyo desarrollo normativo ha sido abordado por el Real Decreto 3/2010. El fin que se persigue con esto es establecer los principios y requisitos de una política de seguridad en la utilización de medios electrónicos que permita la adecuada protección de la información. 4

Una de las exigencias del ENS es que todos los órganos superiores de las Administraciones Públicas dispongan formalmente de una política de seguridad de la información, cuya aprobación recaerá sobre el titular del órgano superior correspondiente. Esta política de seguridad se establecerá con base en los principios básicos y los requisitos mínimos definidos por la citada norma.

La Universidad Autónoma de Madrid (en adelante, UAM) es una entidad de Derecho Público a la que corresponde, en el ámbito de sus competencias, el servicio público de la educación superior mediante la investigación, la docencia y el estudio. Para desarrollar su actividad y así alcanzar los fines que está llamada a cumplir, la UAM cuenta con el apoyo de las Tecnologías de la Información y la Comunicación (en adelante, TIC). A estos efectos es fundamental que los sistemas TIC estén suficientemente protegidos contra cualquier amenaza con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información o en la continuidad de los servicios.

El objeto del presente documento es establecer la Política de Seguridad de la Información de la UAM, con la que se garantice una protección adecuada de la información y la prestación continuada de los servicios, de modo tal que la UAM esté preparada para prevenir, detectar, reaccionar y recuperarse de incidentes de seguridad. Para ello, deberá contar con las medidas de seguridad que le resulten exigibles por el ENS, así como realizar un seguimiento continuo de los niveles de prestación de servicios, analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes.

Los servicios de información de la UAM han de realizar sus funciones y custodiar la información de acuerdo con sus especificaciones funcionales, sin interrupciones o modificaciones no controladas, y sin que la información pueda llegar a conocimiento de personas no autorizadas. Conforme a ello, la capacidad de las redes y de los sistemas de información de la UAM ha de ser suficiente para resistir, con el nivel de confianza exigible, los accidentes o acciones ilícitas o malintencionadas que pongan en peligro el acceso, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, almacenados o transmitidos, así como de los servicios utilizados en medios electrónicos.

La UAM debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida de los sistemas de información, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición, y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación derivadas de cada etapa, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en los pliegos de licitación para proyectos de TIC.

5. Ámbito de aplicación

En virtud de esta Política de Seguridad de la Información y su normativa de desarrollo se definirán unas medidas de seguridad que se aplicarán, según se determine en dichas normas, a todos los servicios, sistemas y demás recursos TIC de la UAM que den soporte a sus procesos y que afecten a los diferentes activos de información sustentados en ellos.

Los recursos TIC de la UAM tienen como finalidad el apoyo a la docencia, a la investigación y a las tareas administrativas necesarias para el funcionamiento de la Universidad. 5

Son recursos TIC de la UAM 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 quedan fuera de este ámbito dichos elementos, así como las acciones sobre ellos o riesgos de seguridad de tales elementos. No obstante, en el caso de que se acceda a la red corporativa mediante dichos ordenadores o dispositivos personales, quedarán sujetos a las obligaciones establecidas en la presente Política de Seguridad de la Información y a las normas e instrucciones de desarrollo.

Esta política se aplica también a todas aquellas personas, instituciones, entidades o unidades y servicios, sean internos o externos, que hagan uso de los recursos TIC de la UAM, sea mediante conexión directa o indirecta con los mismos, conexión remota o a través de equipos ajenos a la misma, incluyendo expresamente los servicios prestados a través de Internet. En adelante tales sujetos tendrán la consideración de "usuarios".

6. Principios Básicos de Seguridad

La presente Política de Seguridad de la Información de la UAM así como la normativa que la desarrolle se fundamenta en los principios básicos de protección previstos en el artículo 4 del Real Decreto 3/2010, cuyo fin es asegurar que una organización administrativa podrá cumplir sus objetivos utilizando sistemas de información. Estos principios básicos, que deberán ser tenidos en cuenta siempre que se adopten decisiones en materia de seguridad de la información, son los siguientes:

a) Seguridad integral.

La seguridad ha de ser entendida como un proceso integral que involucra a todos y cada uno de los elementos humanos, técnicos, materiales y organizativos relacionados con el sistema.

En consecuencia, habrán de adoptarse las medidas oportunas para que todas las personas que intervienen en el proceso conozcan esta Política de Seguridad y desarrollen sus funciones de conformidad con la misma. Todos los implicados en el proceso de seguridad actuarán de manera coordinada en la aplicación y control de las medidas de seguridad. Esta coordinación se extenderá a todas las iniciativas y actuaciones de la UAM.

b) Gestión de riesgos.

El análisis y la gestión de riesgos es una parte esencial del proceso de seguridad. Los niveles de riesgo han de mantenerse dentro de unos niveles mínimos aceptables, mediante el despliegue de las medidas de seguridad apropiadas y permanentemente actualizadas, de modo tal que se establezca un equilibrio y proporcionalidad entre la naturaleza de los datos y los tratamientos realizados, los riesgos a los que estén expuestos y las medidas de seguridad aplicadas.

c) Prevención, reacción y recuperación.

La seguridad del sistema debe contemplar los aspectos de prevención, detección y recuperación, para conseguir que las amenazas sobre el mismo no se materialicen o no afecten gravemente a los datos que manejan los sistemas de información o los servicios que prestan.

Las medidas de prevención contemplarán, entre otras, la disuasión y la reducción de la exposición.

Las medidas de detección se acompañarán de medidas de reacción, para garantizar que los incidentes de seguridad se atajen a tiempo.

Las medidas de recuperación deben permitir la restauración de la información y los servicios de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

El sistema garantizará la conservación de los datos e informaciones en soporte electrónico, y mantendrá disponibles los servicios durante todo el ciclo vital de la información digital.

d) Líneas de defensa.

El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad, dispuestas de tal forma que si una de ellas falla por causa de un incidente que no ha podido evitarse, se gane tiempo para una reacción adecuada, se reduzca la posibilidad de que el sistema se vea comprometido en su conjunto, y se minimice el impacto final sobre el mismo.

Las líneas de defensa han de estar constituidas por medidas de naturaleza organizativa, física y lógica.

e) Reevaluación periódica.

Las medidas de seguridad adoptadas por la UAM se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

El proceso de seguridad de la información implantado por la UAM será actualizado y mejorado de forma continua, mediante la aplicación de una metodología PDCA.

f) Función diferenciada

En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de seguridad. Asimismo, la responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios.

El responsable de la información determinará los requisitos de la información tratada; el responsable del servicio determinará los requisitos de los servicios prestados; y el responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

7. Organización de la seguridad

Según lo dispuesto en los artículos 10 y 12 del Real Decreto 3/2010, la política de seguridad de la información que se establezca tendrá que detallar las atribuciones de cada responsable y los mecanismos de coordinación y resolución de conflictos. En cumplimiento de tal exigencia se indica a continuación quiénes son a estos efectos los sujetos y órganos responsables de la UAM, así como las atribuciones que les son conferidas para garantizar la seguridad de la información:

- Responsable de la Información.
- Responsable de los Servicios.
- Responsable de la Seguridad de la Información.
- Responsable del CERT (Computer Emergency Reaction Team).
- Responsables de los Sistemas de la Información.
- Comité de Seguridad de la Información.
- Comité Técnico de Seguridad de la Información.

7.1 Responsable de la Información

Establecerá los requisitos de seguridad aplicables a la información bajo su responsabilidad. Este cargo lo ostentará el Secretario General o persona en la que delegue, asumiendo las siguientes responsabilidades específicas:

Definir para la información bajo su responsabilidad, las dimensiones de la seguridad relevantes (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) y su nivel correspondiente.

Clasificar e inventariar los activos de la información en virtud de su naturaleza de acuerdo con lo establecido en la presente Política de Seguridad de la Información. El nivel de protección y las medidas a aplicar se basarán en el resultado de dicha clasificación.

Recomendar la inclusión de cláusulas de seguridad en los contratos con terceras partes.

Colaborar en el análisis de impacto de los incidentes que se puedan producir y plantear las estrategias y salvaguardas ante los mismos.

Actualizar y mantener los ficheros que contienen datos personales de la UAM, conforme se dispone en la LOPD.

Cualquier otra función que le pueda ser encomendada por los órganos correspondientes.

7.2 Responsable de los Servicios

Establecerá los requisitos de seguridad aplicables a los servicios bajo su responsabilidad. Este cargo lo ostentará el Vicerrector de quien dependa Tecnologías de la Información o persona en la que delegue, asumiendo las siguientes responsabilidades específicas:

Definir para los servicios electrónicos bajo su responsabilidad, las dimensiones de la seguridad relevantes (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad) y su nivel correspondiente.

Establecer los requisitos de los servicios en materia de seguridad que deban ser garantizados en el tratamiento de la información.

Colaborar en el análisis de impacto de los incidentes que se puedan producir y plantear las estrategias y salvaguardas ante los mismos.

Cualquier otra función que le pueda ser encomendada por los órganos correspondientes.

7.3 Responsable de la Seguridad de la Información

Tomará las decisiones necesarias para satisfacer los requisitos de seguridad establecidos por los Responsables de la Información y de los Servicios. Este cargo lo ostentará el Director de Tecnologías de la Información, asumiendo las siguientes responsabilidades específicas:

Determinar las medidas de seguridad necesarias para la protección de la información manejada y los servicios prestados, y verificar que las establecidas son adecuadas en todo momento.

Determinar la categoría del sistema y las medidas de seguridad que deben aplicarse.

Reportar el estado de la seguridad al Comité de Seguridad de la Información.

Impulsar o instar la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones en materia de seguridad.

Llevar a cabo el seguimiento de la Política de Seguridad de la Información de manera operativa, así como de la seguridad física y lógica de los recursos.

Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.

Elaborar un informe periódico de seguridad, que incluya los incidentes más relevantes del periodo.

Informar al Comité de Seguridad de la Información de las incidencias de seguridad de carácter grave.

Proponer el desarrollo y posterior modificación de aquella normativa, instrucciones y directrices técnicas que considere necesaria en materia de seguridad al Comité de Seguridad de la Información.

Aprobar los procedimientos de seguridad elaborados por los Responsables de los Sistemas cuando en virtud del contenido definido no requieran la revisión y aprobación del Comité de Seguridad de la Información.

Tareas o funciones derivadas de la responsabilidad de Secretario del Comité de Seguridad de la Información.

Cualquier otra función que le pueda ser encomendada por los órganos correspondientes.

7.4 Responsable del CERT

Este cargo lo ostentará el Responsable del Área de Seguridad TIC de la Unidad Técnica de Comunicaciones de Tecnologías de la Información de la UAM, asumiendo las siguientes responsabilidades:

Tratamiento en materia de LOPD de los ficheros en Tecnologías de la Información.

Informar al Responsable de la Seguridad de la Información de los incidentes de seguridad.

Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.

Coordinar de forma centralizada la seguridad de la información.

Realización de labores de prevención y monitorización continua de la seguridad.

Formación y difusión en materia de seguridad de la información.

Tareas o funciones derivadas de la responsabilidad de Secretario del Comité Técnico de Seguridad de la Información.

Cualquier otra tarea o función que le pueda ser encomendada por el Responsable de la Seguridad de la Información.

7.5 Responsables de los Sistemas

Su función será aplicar las medidas de seguridad de índole tecnológica determinadas por el Responsable de la Seguridad de la Información. Este cargo lo ostentarán quienes tengan la condición de Jefes de las Unidades Técnicas de Tecnologías de la Información, asumiendo dentro de su ámbito de competencia las siguientes responsabilidades específicas:

Garantizar que las tareas propias de la administración de la seguridad de sus sistemas se llevan a cabo de manera correcta.

Garantizar que los sistemas de información de los que es responsable permanecen bajo control.

Llevar a cabo los procesos de seguridad en el ámbito de su área.

Implementar la seguridad física y lógica dentro de su área.

Colaborar en las auditorias de seguridad y en la gestión de riesgos.

Cualquier otra función que pueda ser encomendada por los órganos correspondientes.

7.6 Comité de Seguridad de la Información

El Comité de Seguridad de la Información es el órgano colegiado que dirige, establece y aprueba las actuaciones en materia de seguridad.

Este comité es el órgano en el que se resolverán los conflictos que puedan surgir en la aplicación de esta Política de Seguridad de la Información o de las normativas y procedimientos que la desarrollen, y estará compuesto por quienes ocupen los siguientes cargos: 10

El Responsable de la Información.

El Responsable de los Servicios.

El Responsable de la Seguridad de la Información.

El Comité de Seguridad de la Información podrá invitar a sus sesiones a cuantos expertos estime necesarios para el adecuado desempeño de sus funciones. Dichos expertos asistirán en calidad de asesores.

El Comité de Seguridad de la Información recabará información y auxilio de todas las áreas de la Universidad cuando así lo considere necesario; en particular, del Comité Técnico de Seguridad de la Información. Todos los servicios y unidades de la UAM estarán obligados a informar y prestar apoyo al Comité de Seguridad de la Información cuando éste así lo requiera. Este comité tiene las siguientes funciones y responsabilidades concretas:

Divulgar esta política de seguridad y la documentación elaborada dentro del marco normativo de dicha política.

Informar del estado de la seguridad a los órganos de gobierno de la Universidad.

Resolver los conflictos surgidos en materia de seguridad.

Promover la mejora continua de la seguridad.

Revisar y hacer el seguimiento regularmente de esta Política de Seguridad de la Información proponiendo a los órganos de gobierno de la Universidad las modificaciones que considere oportunas.

Elaborar, revisar y hacer un seguimiento periódico de las normativas generales de seguridad que derivan de esta política.

Impulsar nuevas líneas estratégicas en materia de seguridad.

Aprobar anualmente un informe en el que consten las medidas de seguridad que, conforme al principio de gestión de riesgos, deberían ser implementadas durante el ejercicio siguiente por su carácter necesario, así como aquellas medidas que sería deseable incluir para impulsar la estrategia de seguridad diseñada por el Comité.

Elevar anualmente a Gerencia el anterior informe, así como una memoria justificativa en la que se especifiquen los recursos que se precisan para implementar las medidas de seguridad de carácter necesario mencionadas en el informe.

Comunicar a los órganos competentes el incumplimiento de la Política de Seguridad de la Información y de las normativas derivadas, e instar, en su caso, la adopción de las medidas disciplinarias correspondientes.

Elaborar y aprobar un Reglamento de funcionamiento del Comité de Seguridad de la Información.

Ejercerá como Presidente del Comité de Seguridad de la Información el Responsable de la Información de la UAM, y como Secretario, el Responsable de Seguridad de la Información de la UAM.

7.7 Comité Técnico de Seguridad de la Información

El Comité Técnico de Seguridad de la Información es el órgano colegiado que gestiona y coordina las actuaciones en materia de seguridad, y auxilia al Comité de Seguridad de la Información en el desarrollo de sus funciones.
Este comité estará compuesto por quienes ocupen los siguientes cargos:

- El Responsable de la Seguridad de la Información.
- El Responsable del CERT.
- Los Responsables de los Sistemas.

El Comité Técnico de Seguridad de la Información podrá recabar información y auxilio de todas las áreas de la Universidad cuando así lo considere necesario. Todos los servicios y unidades de la UAM estarán obligados a informarle y prestarle apoyo. Este comité tiene las siguientes funciones y responsabilidades concretas:

- Coordinar las tareas periódicas derivadas de la revisión y mantenimiento del análisis de riesgos.
- Interpretar los conflictos surgidos en materia de seguridad, elevando el correspondiente informe al Comité de Seguridad de la Información para que éste resuelva.
- Proponer al Comité de Seguridad de la Información los cambios normativos que resulten necesarios conforme a las nuevas exigencias tecnológicas.
- Auxiliar al Comité de Seguridad de la Información en la elaboración, revisión y seguimiento periódico de las normativas generales de seguridad que derivan de esta política.
- Proponer al Comité de Seguridad de la Información nuevas líneas estratégicas en materia seguridad.

- Elevar informes con planes de mejora basados en los resultados de las auditorias periódicas o cuando se encuentren deficiencias que supongan una amenaza para la seguridad de la información.
- Comunicar al Comité de Seguridad de la Información el incumplimiento de la Política de Seguridad de la Información y de las normativas derivadas.
- Implantar y supervisar el proceso de seguridad.
- Gestionar los incidentes de seguridad que se hayan podido producir y las medidas aplicadas en cada caso.
- Supervisar los resultados de las auditorias para el cumplimiento de la LOPD.
- Supervisar y aprobar las tareas de seguimiento del ENS.
- Informar al Comité de Seguridad de la Información de las actividades desarrolladas en el marco de las funciones de supervisión, gestión y coordinación que le han sido encomendadas.
- Elaborar y aprobar un Reglamento de funcionamiento del Comité Técnico de Seguridad de la Información.

Ejercerá como Presidente del Comité el Responsable de Seguridad de la Información de la UAM, y como Secretario, el Responsable del CERT.

8. Datos de carácter personal

La UAM realiza tratamientos en los que hace uso de datos de carácter personal. Los Documentos de Seguridad LOPD de la UAM recogen los ficheros afectados y los responsables correspondientes.

Todos los sistemas de información de la UAM se ajustarán a los niveles de seguridad requeridos por la normativa aplicable según la naturaleza y finalidad de los datos de carácter personal recogidos en los mencionados documentos de seguridad.

9. Acceso a la información

Según el artículo 16 del Real Decreto 3/2010, el acceso al sistema de información deberá ser controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, de manera que quede restringido el acceso a las funciones permitidas.

Conforme a lo anterior, quienes traten información de la UAM que no sea de acceso público, deberán estar debidamente identificados y tener los privilegios de acceso a la información estrictamente necesarios para desempeñar su cometido.

10. Gestión de incidentes de seguridad

Tecnologías de la Información debe disponer de un servicio de respuesta ante incidentes de seguridad (CERT) que esté dotado de los medios para implantar y gestionar todas y cada una de las medidas de seguridad requeridas a cada sistema de información y para dar respuesta a los incidentes de seguridad

que se produzcan. Este servicio podrá efectuar las auditorías de seguridad que considere oportunas sobre cualquier equipo conectado a la red de la Universidad, pudiendo proceder a su desconexión o aislamiento en aquellos casos que supongan un riesgo potencial o real para el resto de los sistemas de información de la UAM.

Los incidentes de seguridad pueden ser detectados por el responsable o administrador del sistema, por inspección o alarma en el servicio CERT o comunicados desde el exterior de la UAM. En el sistema de gestión de incidentes del Centro de Atención a Usuarios (CAU) se debe centralizar la recogida, análisis y gestión de los incidentes identificados.

Asimismo, cualquier usuario debe trasladar incidentes, sugerencias y/o debilidades que puedan tener relación con la seguridad de la información y las directrices contempladas en la presente política, comunicándolas al CAU.

Se desarrollará un procedimiento específico que determine los criterios generales a la hora de gestionar los incidentes de seguridad. 13

11. Obligaciones de los usuarios

Según el artículo 12 del Real Decreto 3/2010, la seguridad deberá comprometer a todos los miembros de la organización. Todos los usuarios de la UAM tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la normativa e instrucciones de seguridad desarrolladas a partir de ella, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Todos los usuarios de la Universidad deben ser conscientes de la necesidad de garantizar la seguridad de los sistemas de información, así como que son una pieza esencial para el mantenimiento y mejora de la seguridad.

Se promoverá un programa continuo de concienciación que alcance a todos los usuarios de la UAM, en particular a los de nueva incorporación. Todo el personal relacionado con la información y los sistemas deberá ser formado e informado de sus deberes y obligaciones en materia de seguridad.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

12. Responsabilidades de los usuarios en caso de incumplimiento de la normativa de seguridad de la información

El Comité de Seguridad de la Información podrá apreciar si por parte de los usuarios de la UAM existe algún tipo de incumplimiento en las obligaciones previstas en la Política de Seguridad de la Información o en su normativa e instrucciones de desarrollo.

En caso de incumplimiento, se establecerán medidas preventivas y correctivas encaminadas a salvaguardar y proteger las redes y sistemas de información, sin perjuicio de la correspondiente exigencia de responsabilidad disciplinaria.

Constatado un incumplimiento de la Política de Seguridad de la Información de la UAM, el Comité de Seguridad de la Información instará, por los cauces establecidos en los Estatutos de la UAM, 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 del personal al servicio de las Administraciones Publicas o de la propia UAM.

13. Relación con terceras partes

Cuando la UAM preste servicios a otros organismos o maneje información de los mismos, el responsable de esa relación les hará partícipe de esta política de seguridad y de las normas e instrucciones derivadas. Se establecerán canales de comunicación y coordinación entre los respectivos Comités de Seguridad de la Información, y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Asimismo, cuando la UAM utilice servicios de terceros o ceda información a terceros, se les hará igualmente partícipes de esta política de seguridad y de la normativa e instrucciones de seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones y medidas de seguridad establecidas en dicha normativa e instrucciones, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de prevención, detección, reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta política de seguridad.

En concreto, los terceros deberán acreditar el cumplimiento de políticas de seguridad basadas en estándares auditables y someterse a controles y revisiones de terceros que certifiquen el cumplimiento de estas políticas. Asimismo, se garantizará mediante auditoría o certificado de destrucción y borrado que el tercero cancela y elimina los datos pertenecientes a la UAM a la finalización del contrato.

Cuando algún aspecto de la Política de Seguridad de la Información de la UAM no pueda ser satisfecho por una tercera parte, se requerirá la emisión de un informe por quien ostente el cargo de Responsable de Seguridad de la Información, en el que se especifiquen los riesgos en que se incurre y la forma de tratarlos. A la vista de este informe, el Comité de Seguridad de la Información de la UAM deberá pronunciarse sobre la posición y medidas a adoptar en ese caso concreto.

14. Desarrollo normativo de la Política de Seguridad de la Información

En cumplimiento de lo dispuesto en la legislación aplicable, esta Política de Seguridad de la Información ha de ser objeto de desarrollo para que queden perfectamente definidas las medidas de seguridad específicas para los distintos ámbitos contemplados. En todo caso, las diferentes políticas, normativas y regulaciones específicas que resulten de tal desarrollo deberán respetar lo dispuesto en la presente política de seguridad y derivarse de la misma.

En consecuencia, la UAM establecerá un marco normativo propio en materia de seguridad, estructurado en diferentes niveles, a fin de garantizar que los objetivos y medidas establecidos en el presente documento tengan un desarrollo específico:

1) Primer nivel: la Política de Seguridad de la Información.

2) Segundo nivel: las normativas generales de seguridad que emanan de la Política de Seguridad de la Información. 15

3) Tercer nivel: los procedimientos de seguridad, que son el conjunto de documentos que describen explícitamente, paso a paso, cómo realizar una cierta actividad.

4) Cuarto nivel: documentación de buenas prácticas, recomendaciones, guías, cursos de formación, presentaciones, etc.

La Política de Seguridad de la Información será aprobada por el Consejo de Gobierno de la UAM, al igual que las normativas generales de seguridad que emanan de la Política de Seguridad de la Información, a propuesta del Comité de Seguridad de la Información. Los procedimientos de seguridad así como las guías del tercer y cuarto nivel serán aprobados por el Comité de Seguridad de la Información, a propuesta del Responsable de Seguridad de la Información.

15. Difusión de la normativa sobre Seguridad de la Información de la UAM

Tras su aprobación, la Política de Seguridad de la Información y su normativa de desarrollo deberá ser notificada y difundida convenientemente a todos los afectados.

Las normativas de primer y segundo nivel se publicarán necesariamente en el BOUAM.

Todas las disposiciones de seguridad correspondientes a los cuatro niveles se publicarán, según quienes sean sus destinatarios, en la Intranet de la UAM o, cuando resulten de aplicación a todos los usuarios, en una sección de la página web de la UAM de acceso público.

Anexo. Glosario de términos

Este glosario de términos ha sido elaborado de conformidad con lo dispuesto en Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y legislación que la desarrolle; y en el anexo IV 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.

CERT (Computer Emergency Reaction Team).

Centro de Respuesta ante Incidentes de Seguridad de la información. Es el equipo especializado en responder inmediatamente a incidencias relacionadas con la seguridad de las redes o los equipos. También publica alertas sobre amenazas y vulnerabilidades de los sistemas. En general tiene como misiones elevar la seguridad de los sistemas de los usuarios y atender a los incidentes que se produzcan.

Datos de carácter personal.

Cualquier información concerniente a personas físicas identificadas o identificables, según la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Gestión de incidentes de seguridad.

Plan de acción para atender a los incidentes de seguridad que se den. Además de resolverlas debe incorporar medidas de desempeño que permitan conocer la calidad del sistema de protección y detectar tendencias antes de que se conviertan en grandes problemas.

Incidente de seguridad.

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

Metodología PDCA.

La metodología PDCA también conocida como ciclo de Deming, es una estrategia de mejora continua de la calidad en cuatro pasos (Plan, Do, Check, Act).

Política de seguridad.

Conjunto de directrices plasmadas en documento escrito, que rigen la forma en que una organización gestiona y protege la información, y los servicios que considera críticos.

Servicio.

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los ciudadanos.

Sistema de información.

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

Vulnerabilidad.

Situación de debilidad en un sistema de información que posibilita que se produzca un incidente de seguridad.