PLAN DE ADECUACIÓN al ENS
Política de seguridad de la información.

UNIVERSIDAD
DE MÁLAGA

INDICE

1 INTRODUCCIÓN

1.1 Justificación de la Política de Seguridad

La Universidad de Málaga (en adelante la UMA) depende de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos como Organización. Estos sistemas deben ser administrados con diligencia, tomando 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.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Es por ello que el Esquema Nacional de Seguridad (Real Decreto 3/2010 de 8 de Enero, ENS en adelante), en su artículo 11 establece que "Todos los órganos superiores de las Administraciones Públicas deberán disponer formalmente de su Política de Seguridad, que será aprobada por el titular del órgano superior correspondiente".

Esto implica que las diferentes áreas de la UMA deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Todas las áreas deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, 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, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC. Las áreas deben estar preparadas para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

La UMA establece como **objetivos de la seguridad** de la información los siguientes:

- Cumplir la legislación de seguridad y privacidad.
- Garantizar la calidad y protección de la información.
- Garantizar la prestación continuada de los servicios.
- Lograr la plena concienciación de los usuarios respecto a la seguridad de la información.

2 ALCANCE

Esta política se aplica a todos los sistemas TIC de la UMA y a todos los miembros de la UMA, sin excepciones.

3 MISIÓN Y SERVICIOS PRESTADOS

La UMA como Universidad, para la gestión de sus intereses, y en el ámbito de sus competencias y como Administración pública, sirve con objetividad los intereses generales y actúa de acuerdo a los principios de eficacia, jerarquía, descentralización y coordinación, promueve toda clase de actividades y presta los servicios públicos que contribuyen a satisfacer las necesidades y aspiraciones de su personal y alumnos que cursan sus estudios.

La presente Política de Seguridad aplica a las diferentes actividades en las que participa la UMA a través de medios electrónicos, en concreto:

a. Las relaciones entre los alumnos, PAS, PDI y la UMA.
b. La consulta por parte de los estudiantes de la información pública administrativa y de los datos administrativos que estén en poder de la UMA.
c. La realización de los trámites y procedimientos administrativos incorporados para su tramitación en la Sede Electrónica de la UMA, de conformidad con lo previsto del Uso de la Administración Electrónica.
d. El tratamiento de la información obtenida por la UMA en el ejercicio de sus potestades.

4 MARCO NORMATIVO

El marco legal en materia de seguridad de la información viene establecido por la siguiente legislación:

- La Ley 11/2007, de 22 de junio, de **acceso electrónico de los ciudadanos a los servicios públicos**, en su artículo 42.2 sobre el Esquema Nacional de Seguridad establece, como uno de sus principios, que se debe disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos.
- Ley 39/2015 de 1 de Octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015 de 1 de Octubre, de Régimen Jurídico del Sector Público.
- 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, fija los principios básicos y requisitos mínimos, así como las medidas de protección a implantar en los sistemas de la Administración.
- Real Decreto 951/2015, de 23 de octubre, de modificación 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.
- 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, cuya finalidad es la creación de las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados por las Administraciones públicas, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso electrónico a los servicios públicos, a la vez que redunda en beneficio de la eficacia y la eficiencia.

- La Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantías de los Derechos Digitales de 13 de diciembre, tiene por objeto adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/67 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, garantizando el derecho fundamental de las personas físicas a la protección de datos, amparado por el artículo 18.4 de la Constitución y garantizar los derechos digitales de la ciudadanía, conforme al mandato establecido en el artículo 18.4 de la Constitución.
- El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el **Reglamento que desarrollaba la Ley Orgánica 15/1999**, la dota de coherencia en todo lo relacionado con la trasposición de la directiva 95/46/CE del Parlamento Europeo y desarrolla aquellos aspectos novedosos o que la experiencia ha aconsejado un cierto grado de precisión.
- El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD), en vigor desde el 24 de mayo de 2016 pero no será aplicable hasta el 25 de mayo de 2018.

5 PRINCIPIOS DE PROTECCIÓN.

Los principios básicos son directrices fundamentales de seguridad que han de tenerse siempre presentes en cualquier actividad relacionada con el uso de los activos de información. Se establecen los siguientes:

A. **Alcance estratégico:** La seguridad de la información debe contar con el compromiso y apoyo de todos los niveles directivos de forma que pueda estar coordinada e integrada con el resto de iniciativas estratégicas del Departamento para conformar un todo coherente y eficaz.
B. **Responsabilidad diferenciada**: En los sistemas de información se diferenciará el responsable de la información, que determina los requisitos de seguridad de la información tratada; el responsable del servicio, que determina los requisitos de seguridad de los servicios prestados; el responsable del sistema, que tiene la responsabilidad sobre la prestación de los servicios y el responsable de seguridad, que determina las decisiones para satisfacer los requisitos de seguridad.
C. **Seguridad integral:** La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información.
D. **Gestión de Riesgos:** El análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales.

E. **Proporcionalidad:** El establecimiento de medidas de protección, detección y recuperación deberá ser proporcional a los potenciales riesgos y a la criticidad y valor de la información y de los servicios afectados.
F. **Mejora continua:** Las medidas de seguridad se reevaluarán y actualizarán periódicamente para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección. La seguridad de la información será atendida, revisada y auditada por personal cualificado, instruido y dedicado.
G. **Seguridad por defecto:** Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.

Las directrices fundamentales de seguridad se concretan en un conjunto de principios particulares y responsabilidades específicas, que se configuran como objetivos instrumentales que garantizan el cumplimiento de los principios básicos de la Política de Seguridad. Se establecen los siguientes:

a. Protección de datos de carácter personal: Se adoptarán las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
b. Gestión de activos de información: Los activos de información del Departamento se encontrarán inventariados y categorizados y estarán asociados a un responsable.
c. Seguridad ligada a las personas: Se implantarán los mecanismos necesarios para que cualquier persona que acceda, o pueda acceder a los activos de información, conozca sus responsabilidades y de este modo se reduzca el riesgo derivado de un uso indebido de dichos activos. d) Seguridad física: Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.
d. Seguridad en la gestión de comunicaciones y operaciones: Se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.
e. Control de acceso: Se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo. Además, quedará registrada la utilización del sistema con objeto de asegurar la trazabilidad del acceso y auditar su uso adecuado, conforme a la actividad de la organización.
f. Adquisición, desarrollo y mantenimiento de los sistemas de información: Se contemplarán los aspectos de seguridad de la información en todas las fases del ciclo de vida de los sistemas de información, garantizando su seguridad por defecto.

g. Gestión de los incidentes de seguridad: Se implantarán los mecanismos apropiados para la correcta identificación, registro y resolución de los incidentes de seguridad.
h. Gestión de la continuidad: Se implantarán los mecanismos apropiados para asegurar la disponibilidad de los sistemas de información y mantener la continuidad de sus procesos de negocio, de acuerdo a las necesidades de nivel de servicio de sus usuarios.
i. Cumplimiento: Se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para el cumplimiento de la normativa legal vigente en materia de seguridad de la información.

6 ORGANIZACIÓN DE LA SEGURIDAD

6.1 Definición de roles

Tal como indica el artículo 12 del ENS, La seguridad deberá comprometer a todos los miembros de la UMA.

La Política de Seguridad, según detalla el Anexo II del ENS, en su sección 3.1, debe identificar unos claros responsables para velar por su cumplimiento y ser conocida por todos los miembros de la UMA administrativa.

La responsabilidad del éxito de una Organización recae, en última instancia, en su Dirección. La Dirección es responsable de organizar las funciones y responsabilidades, la política de seguridad del Organismo, y de facilitar los recursos adecuados para alcanzar los objetivos propuestos.

La estructura organizativa de seguridad, y jerarquía en el proceso de decisiones la componen:

Rol	Funciones
Dirección	Órganos colegiados o unipersonales que deciden la misión y los objetivos de la UMA.
Comité de Seguridad de la Información y la Privacidad y Privacidad	Órganos colegiados o unipersonales que toman decisiones que concretan cómo alcanzar los objetivos de seguridad y protección de la privacidad marcados por los órganos de gobierno.
Responsable de la Información	A nivel de gobierno. Tiene la responsabilidad última sobre qué seguridad requiere una cierta información manejada por la UMA.
Responsable de Servicio	A nivel de gobierno o, en ocasiones baja a nivel ejecutivo. Tiene la responsabilidad última de determinar los niveles de servicio aceptables por la UMA.

Responsable de Seguridad	A nivel ejecutivo. Funciona como supervisor de la operación del sistema y vehículo de reporte al Comité de Seguridad de la Información y la Privacidad.
Responsable del Sistema	A nivel operacional. Toma decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día
Administradores de seguridad.	Son las personas encargadas de ejecutar las acciones diarias de operación del sistema según las indicaciones recibidas de sus superiores jerárquicos.
Delegado de Protección de Datos	Figura obligatoria para administraciones públicas, es el encargado de asesorar y supervisar todos los aspectos relacionados con el tratamiento de datos de carácter personal, incluidos los aspectos de seguridad (integridad, confidencialidad y disponibilidad) y violación de datos personales. Su nombramiento se produce por otra vía ya que sus cometidos no se ciñen únicamente a aspectos de seguridad.

6.2 Jerarquía en el proceso de decisiones y mecanismos de coordinación

Los diferentes roles de seguridad de la información (autoridad principal y posibles delegadas) se limitan a una jerarquía simple: el **Comité de Seguridad de la Información y la Privacidad y la Privacidad** da instrucciones al **Responsable de la Seguridad** de la Información que se encarga de cumplimentar, supervisando que administradores y operadores implementan las medidas de seguridad según lo establecido en la política de seguridad aprobada para la UMA. Por su parte el Delegado de Protección de Datos debe ser oído en todos los aspectos relacionados con la seguridad de los datos personales y violaciones de seguridad de datos personales, entendiendo las mismas desde la perspectiva de la confidencialidad, integridad y disponibilidad.

El **Responsable del Sistema**:

- Informa al Responsable de la Información de las incidencias funcionales relativas a la información que le compete.
- Informa al Responsable del Servicio de las incidencias funcionales relativas al servicio que le compete.
- Da cuenta al Responsable de la Seguridad:
    - Actuaciones en materia de seguridad, en particular en lo relativo a decisiones de arquitectura del sistema.
    - Resumen consolidado de los incidentes de seguridad.
    - Medidas de la eficacia de las medidas de protección que se deben implantar.

El **Responsable de la Seguridad**:

- Informa al Responsable de la Información de las decisiones e incidentes en materia de seguridad que afecten a la información que le compete, en particular de la estimación de

riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.

- Informa al Responsable del Servicio de las decisiones e incidentes en materia de seguridad que afecten al servicio que le compete, en particular de la estimación de riesgo residual y de las desviaciones significativas de riesgo respecto de los márgenes aprobados.
- Da cuenta al Comité de Seguridad de la Información y la Privacidad y la Privacidad, como secretario:
  - Resumen consolidado de actuaciones en materia de seguridad.
  - Resumen consolidado de incidentes relativos a la seguridad de la información.
  - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.
- Da cuenta al Consejo de Dirección, según lo acordado en el Comité de Seguridad de la Información y la Privacidad y la Privacidad.
  - Resumen consolidado de actuaciones en materia de seguridad.
  - Resumen consolidado de incidentes relativos a la seguridad de la información.
  - Estado de la seguridad del sistema, en particular del riesgo residual al que el sistema está expuesto.
- Da cuenta al Delegado de Protección de Datos sobre los aspectos que afecten a la seguridad de los datos personales.
  - Violaciones de seguridad de los datos personales que afecten a la confidencialidad, disponibilidad e integridad de los datos personales.
  - Riesgos detectados y medidas correctoras oportunas relacionados con la seguridad de los tratamientos de datos personales.
  - Pedirá asesoramiento ante nuevas arquitecturas de seguridad, políticas y procedimientos que afecten al tratamiento de datos personales.

6.3 Procedimiento de designación de personas

La Dirección de la UMA nombrará formalmente mediante su publicación en el Boletín Oficial de la Universidad:

- Al Responsable de la Información.
- Al Responsable del Servicio.
- Al Responsable de la Seguridad.
- Al Responsable del Sistema.
- Al Administrador de Seguridad del Sistema, a propuesta del Responsable del Sistema o del Responsable de Seguridad de la Información.

6.4 Detalle de los roles

6.4.1 Dirección

La función de Dirección la desempeñará El Rector, que podrá delegar en el Vicerrector de Política Institucional, asesorado por el Consejo de Dirección, quien entiende la misión de la UMA, determina los objetivos que se propone alcanzar y responde que se alcancen.

Función	Detalle
Nombrar	• Designar los diferentes roles encargados de la gestión de la seguridad.
Objetivos	• Fijar y aprobar anualmente unos objetivos de nivel de riesgo aceptable. Los objetivos deben ser vigentes y estar alineados con el propósito y la estrategia de la UMA, ser medibles o estimables y coherentes con las presentes Directrices. El Comité de Seguridad seguirá y reportará anualmente la evolución de dichos objetivos.
Aprobar	• Aprobar el Plan de Adecuación al ENS. • Aprobar la Política de Seguridad así como las revisiones de la misma. • Aprobar, tras cada proceso de Apreciación del Riesgo que se realice, del Plan de Tratamiento del Riesgo que se elabore, que puede incluir la aplicación de controles, la transferencia a terceros, evitar riesgos –lo que deriva generalmente en la realización de cambios en procesos -, o bien la asunción de determinados riesgos.
Recursos	• Proporcionar los recursos necesarios para el aseguramiento del cumplimiento de estos objetivos y para la operación del Sistema Integrado de Gestión.

6.4.2 **Comité de Seguridad de la Información y la Privacidad.**

El Comité de Seguridad de la Información y la Privacidad coordina la seguridad de la información a nivel de Organización

Composición. Se ha creado el Comité de Seguridad de la Información y la Privacidad que estará compuesto por los siguientes miembros:

Presidente	El Rector	Delega en el Vicerrector de Política Institucional
Vicepresidente 1º	El Director TICs	
Vicepresidente 2º		
Secretario	Oficial Mayor	
Vocales	Responsable de Información 1º	Gerencia
	Responsable de Información 2º (contingencia)	Vicegerencia que se designe
	Responsable de Servicio	Vicerrectorado PDI
		Vicerrectorado Estudiantes
	Responsable de Seguridad	Funcionario SCI
	Responsable de Sistemas	Funcionario SCI
	Responsable de seguridad física	Funcionario SCI

	Adjunto Responsable Seguridad física	
	Responsable de Gestión de Personal	
	Administrador de Seguridad	
	Funcionario RPT	
Asesor / Consejero	Delegado de Protección de Datos	

A requerimiento del Comité se convocará cualesquiera otros Vicerrectores, Decanos o Directores de Centro, Jefes de Área y responsables, cuya intervención sea precisa por ser afectados por el Esquema Nacional de Seguridad y por el RGPD.

Funciones del Secretario. Corresponde al Secretario/a del Comité de Seguridad de la Información y la Privacidad:

- Convocar las reuniones del Comité de Seguridad de la Información y la Privacidad
- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.
- Elaborar el acta de las reuniones.
- La responsabilidad de la ejecución directa o delegada de las decisiones del Comité.

Funciones de los Vocales. Corresponde a los vocales del Comité de Seguridad de la Información y la Privacidad:

- Participar en las reuniones.
- Contribuir con ideas y sugerencias para el buen desarrollo de las reuniones.

Todos miembros del Comité actuarán con voz y voto y sus acuerdos requerirán, como mínimo, el voto de la mayoría simple de sus miembros.

Funciones del Delegado de Protección de Datos. Corresponde al Delegado de Protección de Datos asesorar en aquellos aspectos que afecten a la seguridad de los datos personales y violaciones de seguridad de los datos personales:

- Participar en las reuniones.
- Emitir su parecer en aquellos aspectos relacionados con la seguridad de los datos personales, promover, en su caso, revisiones de análisis de riesgos, elaboración de evaluaciones de impacto en protección de datos, elaboración o modificación de procedimientos o políticas de seguridad de datos personales, entre otros.

Funciones del Comité. Corresponde al Comité de Seguridad de la Información y la Privacidad:

Función	Detalle
Informar	• Atender las inquietudes de la Alta Dirección y de los diferentes departamentos/áreas. • Informar regularmente del estado de la seguridad de la información

	a la Alta Dirección.
Promover	• Promover la mejora continua del Sistema de Gestión de la Seguridad de la Información. • Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.
Coordinar	• Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades. • Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables y/o entre diferentes áreas de la UMA, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.
Elaborar	• Elaborar (y revisar regularmente) la Política de Seguridad de la información para que sea aprobada por la Dirección. • Elaborar la estrategia de evolución de la UMA en lo que respecta a la seguridad de la información.
Aprobar	• Aprobar la normativa de seguridad de la información. • Elaborar y aprobar los requisitos de formación y cualificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información • Aprobar planes de mejora de la seguridad de la información de la UMA. En particular, velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.
Controlar	• Monitorizar los principales riesgos residuales asumidos por la UMA y recomendar posibles actuaciones respecto de ellos. • Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información. • Velar para que la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular, deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.
Decidir	• Si una violación de seguridad de datos personales debe ser notificada a la Agencia Española de Protección de Datos y/o a los propios interesados.
Asesorar	• Emitir su opinión y participar en los aspectos de seguridad de las Evaluaciones de impacto en protección de datos.

6.4.3 **Responsable de la Información**

El Responsable de la Información debe ser una persona que ocupa un alto cargo en la dirección de la UMA.

Compatibilidades. Este rol únicamente podrá coincidir con la del Responsable de Servicio y el Responsable de Información en organizaciones de reducidas dimensiones que tengan una estructura autónoma de funcionamiento.

Incompatibilidades. Este rol no podrá coincidir con el de Responsable de Sistema y el de Administrador de Seguridad del Sistema, aunque se trate de organizaciones de reducidas dimensiones que tengan una estructura autónoma de funcionamiento**.**

Se ha designado responsable de la Información a GERENCIA y a VICEGERENCIA para las situaciones de contingencia.

Las funciones del Responsable de la Información son las siguientes:

Función	**Detalle**
Establecer requisitos de seguridad sobre la información	Establece los requisitos de la información en materia de seguridad. En el marco del ENS, equivale a la potestad de determinar los niveles de seguridad de la información.
Determinar niveles de seguridad en cada dimensión	Determinar los niveles de seguridad en cada dimensión (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad. Aunque la aprobación formal de los niveles corresponda al Responsable de la Información, podrá recabar una propuesta del Responsable de la Seguridad y conviene que escuche la opinión del Responsable del Sistema.
Adoptar medidas sobre los datos personales	Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. Solicitar opinión al Delegado de Protección de Datos y a Responsable de Seguridad sobre las violaciones de seguridad de datos personales y en su caso, recomendar la notificación a la Agencia Española de Protección de Datos y /o a los propios interesados.
Responder del uso	Tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
Responder ante errores	El Responsable de la Información es el responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.

6.4.4 **Responsable del Servicio**

El Responsable del Servicio puede ser una persona concreta o puede ser un órgano corporativo, que revestirá la forma de órgano colegiado de acuerdo con la normativa administrativa.

Compatibilidades.

- Es posible que coincidan en la misma persona u órgano las responsabilidades de la información y del servicio. La diferenciación tiene sentido:
  - Cuando el servicio maneja información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio.
  - Cuando la prestación del servicio no depende de la unidad que es Responsable de la Información.

Incompatibilidades.

- Este rol no podrá coincidir con el de Responsable de Seguridad, salvo en organizaciones de reducida dimensión que funcionen de forma autónoma.
- Este rol no podrá coincidir con el de Responsable de Sistema ni con el de Administrador de la Seguridad del Sistema, ni siquiera cuando se trate de organizaciones de reducida dimensión que funcionen de forma autónoma.

Se ha designado como Responsable de Servicio a las siguientes personas

RESPONSABLES	SERVICIO
VICERECTORADO PDI	XXX
VICERRECTORADO ESTUDIANTES	Sede electrónica.

Las funciones del Responsable del Servicio son las siguientes:

Función	Detalle
Responsabilidad	Tiene la responsabilidad última del uso que se haga de determinados servicios y, por tanto, de su protección.
Establecer los requisitos de seguridad del servicio	Tiene la potestad de establecer los requisitos del servicio en materia de seguridad o, en terminología del ENS, la potestad de determinar los niveles de seguridad de los servicios. Aunque la aprobación formal de los niveles corresponda al Responsable del Servicio, se puede recabar una propuesta al

	Responsable de la Seguridad y conviene que se escuche la opinión del Responsable del Sistema.
Riesgos	Aprobar el riesgo residual (el resultante una vez aplicados los controles de seguridad).
Gestionar los tratamientos de datos personales	En cuanto al Reglamento 2016/679 General de Protección de Datos, por delegación del Responsable del Tratamiento se encomienda al Responsable del Servicio el desarrollo de las tareas relacionadas con la gestión de los tratamientos de datos personales que se realizan en su área en concreto. Esta figura en terminología de protección de datos de carácter personal se denomina Gestor de Tratamientos Concretos.

Consideraciones. El Responsable del Servicio deberá tener en cuenta las siguientes consideraciones:

- La determinación de los niveles de seguridad en cada dimensión de seguridad debe realizarse dentro del marco establecido en el Anexo I del Esquema Nacional de Seguridad. Se recomienda que los criterios de valoración estén respaldados por la Política de Seguridad en la medida en que sean sistemáticos, sin perjuicio de que puedan darse criterios particulares en casos singulares.

- La prestación de un servicio siempre debe atender a los requisitos de seguridad de la información que maneja, de forma que pueden heredarse los requisitos de seguridad de la misma, añadiendo requisitos de disponibilidad, así como otros como accesibilidad, interoperabilidad, etc.

6.4.5 **Responsable de Seguridad**

El Responsable de Seguridad de la Información es una figura clave, ya que a él le corresponde dinamizar y gestionar el día a día de todo el proceso de seguridad de la información.

Se ha designado como Responsable de Seguridad de la Información al al FUNCIONARIO SCI

Las **funciones** del Responsable de Seguridad son las siguientes:

Función	**Detalle**
Política, Normativa y Procedimientos	• Participará en la elaboración, en el marco del Comité de Seguridad de la Información y la Privacidad, de la Política y Normativa de Seguridad de la Información, para su aprobación por Dirección. • Elaborará y aprobará los Procedimientos Operativos de Seguridad de la Información.
Seguridad en el tratamiento de datos	• Coordinará la realización de un análisis de riesgos, así como la efectiva implementación de los controles previstos para eliminar

personales	o reducir el riesgo. • Reportará al Delegado de Protección de Datos, al Responsable de Información y al Comité de Seguridad sobre las violaciones de seguridad de los datos personales. • Coordinará la elaboración de la Documentación de Seguridad del Sistema.
Formación y concienciación	• Promoverá la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad. • Elaborará los Planes de Formación y Concienciación del personal en Seguridad de la Información, que deberán ser aprobados por el Comité de Seguridad de la Información y la Privacidad
Gestión de la Seguridad	• Mantendrá la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la UMA. • Recopilará los requisitos de seguridad de los Responsables de Información y Servicio y determinará la categoría del Sistema. • Realizará el Análisis de Riesgos. • Facilitará a los Responsable de Información y a los Responsables de Servicio información sobre el nivel de riesgo residual esperado tras implementar las opciones de tratamiento seleccionadas en el análisis de riesgos y las medidas de seguridad requeridas por el ENS. • Elaborará una Declaración de Aplicabilidad a partir de las medidas de seguridad requeridas conforme al Anexo II del ENS y del resultado del Análisis de Riesgos. • Elaborará, junto a los Responsables de Sistemas, Planes de Mejora de la Seguridad, para su aprobación por el Comité de Seguridad de la Información y la Privacidad. • Validará los Planes de Continuidad de Sistemas que elabore el Responsable de Sistemas, que deberán ser aprobados por el Comité de Seguridad de la Información y la Privacidad y probados periódicamente por el Responsable de Sistemas. • Aprobará las directrices propuestas por los Responsables de Sistemas para considerar la Seguridad de la Información durante todo el ciclo de vida de los activos y procesos: especificación, arquitectura, desarrollo, operación y cambios.
Comité de Seguridad.	• Facilitará periódicamente al Comité de Seguridad un resumen de actuaciones en materia de seguridad, de incidentes relativos a seguridad de la información y del estado de la seguridad del sistema (en particular del nivel de riesgo residual al que está expuesto el sistema).

Delegación de funciones

En caso de que, por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable

de la Seguridad, se podrá designar cuantos Responsables de Seguridad Delegados considere necesarios.

La designación corresponde al Responsable de la Seguridad. Por medio de la designación de delegados, se delegan funciones. La responsabilidad final sigue recayendo sobre el Responsable de la Seguridad.

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable de la Seguridad. Es habitual que se encarguen de la seguridad de sistemas de información concretos o de sistemas de información horizontales.

Cada delegado tendrá una dependencia funcional directa del Responsable de la Seguridad, que es a quien reportan.

6.4.6 **Responsable del Sistema**

El Responsable del Sistema es la persona que toma las decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día.

Compatibilidades. Este rol podrá coincidir con el de Administrador de Seguridad del Sistema en organizaciones de una dimensión reducida o intermedia que tengan una estructura autónoma de funcionamiento.

Incompatibilidades. Este rol no podrá coincidir con el de Responsable de Información, con el de Responsable de Servicio ni con el de Responsable de Seguridad Corporativa o de la Información.

Se ha designado como Responsable del Sistema a FUNCIONARIO SCI

Las funciones del Responsable del Servicio son las siguientes:

Función	Detalle
Gestionar el Sistema	• Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento. • Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad. • acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los Responsables de la Información afectada, del Servicio afectado y con el Responsable de la Seguridad antes de ser ejecutada.
Establecer directrices y medidas	• Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo. • Definir la política de conexión o desconexión de equipos y usuarios nuevos en el Sistema. • Decidir las medidas de seguridad que aplicarán los

	suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo. • Determinar la configuración autorizada de hardware y software a utilizar en el Sistema. • Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
Elaborar	• Elaborar procedimientos operativos de seguridad. • Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
Aprobar	• Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema. • Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
Monitorizar	• Monitorizar el estado de la seguridad del Sistema de Información y reportarlo periódicamente o ante incidentes de seguridad relevantes al Responsable de Seguridad de la Información. • Comunicar tan pronto como se tenga constancia de la misma al Responsable de Seguridad las violaciones de seguridad que afecten a datos personales.

Delegación de funciones.

En caso de que, por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite de personal adicional para llevar a cabo las funciones de Responsable del Sistema, se podrá designar cuantos Responsables de Sistema Delegados considere necesarios.

La designación corresponde al Responsable del Sistema. Por medio de la designación de delegados, se delegan funciones. La responsabilidad final sigue recayendo sobre el Responsable del Sistema.

Los delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del Sistema de información. Es habitual que se encarguen de subsistemas de información de cierta envergadura o de sistemas de información que presten servicios horizontales.

6.4.7 **Administrador de la Seguridad del Sistema**

El Administrador de seguridad es la persona encargada de ejecutar las acciones diarias de operación del sistema según las indicaciones recibidas de sus superiores jerárquicos.

Se ha designado como Administrador de la Seguridad del Sistema a FUNCIONARIO SCI

Las funciones del Administrador de la Seguridad del Sistema son las siguientes:

Función	**Detalle**

Implementar, gestionar y mantener la seguridad	• La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información. • Asegurar que los controles de seguridad establecidos son cumplidos estrictamente. • Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad. • Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
Gestión, configuración y actualización	• La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información. • Aprobar los cambios en la configuración vigente del Sistema de Información. • Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
Gestión de las autorizaciones	• La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
Aplicar los procedimientos	• La aplicación de los Procedimientos Operativos de Seguridad. • Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
Monitorizar la seguridad	• Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema. • Comunicar tan pronto como se tenga constancia de la misma al Responsable de Seguridad las violaciones de seguridad que afecten a datos personales.

6.4.8 **Delegado de Protección de Datos (DPD).**

El Delegado de Protección de Datos será único para todos los órganos de la UMA informándose de su nombramiento y cese a la Agencia Española de Protección de Datos.

Las funciones el Delegado de Protección de datos serán las indicadas en el ya mencionado Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y demás disposiciones reguladoras de la materia. Te atenderán las recomendaciones establecidas por la Agencia Española de Protección de Datos respecto a las funciones y atribuciones de este cargo en las Administraciones Públicas según la guía “El Delegado de Protección de Datos en las Administraciones Publicas”.

6.4.9 **Responsable de Seguridad Física**

Se ha designado como responsable de Seguridad Física a FUNCIONARIO SCI al que le corresponderá implantar las medidas de seguridad que le competan dentro de las determinadas

por el responsable de la Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

6.4.10 **Adjunto al Responsable de Seguridad física**

Función	Detalle
Implementar, gestionar y mantener la seguridad	• La implementación, gestión y mantenimiento de las medidas de seguridad aplicables a la seguridad física de las instalaciones. • Asegurar que los controles de seguridad establecidos son cumplidos estrictamente. • Informar al Responsable de Seguridad física de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad. • Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

6.4.11 **Responsable de Gestión de Personal**

Se ha designado como responsable de Gestión de Personal al FUNCIONARIO SCI al que le corresponde implantar las medidas de seguridad que le competan dentro de las determinadas por el Responsable de Seguridad de la Información, e informará a éste de su grado de implantación, eficacia e incidentes.

7 DATOS DE CARÁCTER PERSONAL

Para la prestación de los servicios previstos deben ser tratados datos de carácter personal. La UMA dispone de un análisis de riesgos de seguridad con controles y medidas que reducen o eliminan los riesgos detectados y para determinados tratamientos de alto riesgo, se ha elaborado una Evaluación de impacto en protección de datos, que, entre otros aspectos, identifica los riesgos en materia de seguridad y recoge medidas y controles para que el riesgo residual sea aceptable.

8 GESTIÓN DE RIESGOS

8.1 Justificación

Todos los sistemas sujetos a esta Política deberán realizar un **análisis de riesgos**, evaluando las amenazas y los riesgos a los que están expuestos.

El análisis de riesgos será la base para determinar las medidas de seguridad que se deben adoptar además de los mínimos establecidos por el Esquema Nacional de Seguridad, según lo previsto en el Artículo 6 del ENS.

El proceso de gestión de riesgos, que comprende las fases de categorización de los sistemas, análisis de riesgos y selección de medidas de seguridad a aplicar, que deberán ser proporcionales a los riesgos y estar justificadas, deberá revisarse y aprobarse cada año por el titular del órgano o unidad administrativa o, en su caso, organismo autónomo, a través de un Plan de Adecuación al Esquema Nacional de Seguridad.

Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en los anexos I y II del Real Decreto 3/2010, de 8 de enero y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional, así como todo lo referente al análisis de riesgo y de impacto en la protección de datos especificado en el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

El análisis de los riesgos y su tratamiento deben ser una actividad repetida regularmente, según lo establecido en el Artículo 9 del ENS. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando se produzcan cambios significativos en la información manejada.
- Cuando se produzcan cambios significativos en los servicios prestados.
- Cuando se produzcan cambios significativos en los sistemas que tratan la información e intervienen en la prestación de los servicios.
- Cuando ocurra un incidente grave de seguridad.
- Cuando se reporten vulnerabilidades graves.

El análisis de riesgos también contemplará los requisitos establecidos por el Articulo 32 del RGPD para decidir y establecer las medidas técnicas y organizativas que corresponda implantar para atender los riesgos generados por el tratamiento de acuerdo a lo exigido por el citato Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

8.2 Criterios de evaluación de riesgos

Para la armonización de los análisis de riesgos, el Comité de Seguridad de la Información y la Privacidad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

Los criterios de evaluación de riesgos detallados **se especificarán en la metodología** de evaluación de riesgos que elaborará la UMA, basándose en estándares y buenas prácticas reconocidas.

Deberán tratarse, como mínimo, todos los riesgos que puedan impedir la prestación de los servicios o el cumplimiento de la misión de la UMA de forma grave.

Se priorizarán especialmente los riesgos que impliquen un cese en la prestación de servicios a los alumnos, PAS, PDI y el resto de ciudadanos vinculados con la UMA.

8.3 Proceso de aceptación del riesgo residual

Los riesgos residuales serán **determinados por** el Responsable de Seguridad de la Información.

Los niveles de Riesgo residuales esperados sobre cada Información tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán **ser aceptados previamente por** su Responsable de esa Información.

Los niveles de Riesgo residuales esperados sobre cada Servicio tras la implementación de las opciones de tratamiento previstas (incluida la implantación de las medidas de seguridad previstas en el Anexo II del ENS) deberán **ser aceptados previamente por** su Responsable de ese Servicio.

Los **niveles de riesgo residuales** serán presentados por el Responsable de Seguridad de la Información al Comité de Seguridad de la Información y la Privacidad, para que éste proceda, en su caso, a evaluar, aprobar o rectificar las opciones de tratamiento propuestas.

9 GESTIÓN DE INCIDENTES DE SEGURIDAD

9.1 Prevención de incidentes

Las áreas deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. El ENS a través de su artículo 19 establece la que los sistemas deben diseñarse y configurarse de forma que garanticen la seguridad por defecto. De igual forma, el artículo 17 del citado ENS define que los sistemas de instalarán en áreas separadas, dotadas de un procedimiento de control de acceso.

Para ello las áreas deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, las áreas deben:

- Establecer áreas seguras para los sistemas de información crítica o confidencial.
- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

9.2 Monitorización y detección de incidentes

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de

manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produzca una desviación significativa de los parámetros que se hayan preestablecido como normales.

Los sistemas de detección de intrusos cumplen fundamentalmente con una labor de supervisión y auditoría sobre los recursos de la UMA, verificando que la política de seguridad no es violada e intentando identificar cualquier tipo de actividad maliciosa de una forma temprana y eficaz.

Se deberán establecer, en función de las necesidades, las siguientes clasificaciones:

- Sistemas de detección de intrusos a nivel de red.
- Sistemas de detección de intrusos a nivel sistema.

Por su parte, el Reglamento General de Protección de Datos en sus artículos 33 y 34, respectivamente, obliga a notificar las violaciones de seguridad de datos personales a la Agencia Española de Protección de Datos cuando existe riesgo para los interesados y a los propios interesados cuando la violación suponga un alto riesgo para ellos. Por ello se deberán establecer controles internos para identificar y catalogar este tipo de incidencias relacionadas con datos personales y comunicarlas al Responsable de Seguridad.

9.3 Respuesta ante incidentes

Las áreas deben:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

10 OBLIGACIONES DEL PERSONAL

Los miembros de la UMA tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad de la Información y la Privacidad disponer los medios necesarios para que la información llegue a los afectados.

Se desarrollarán actividades formativas específicas orientadas a la concienciación y formación de los empleados públicos de la UMA, así como a la difusión entre los mismos de la Política de seguridad y de su desarrollo normativo.

Los miembros de la UMA atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez cada dos años. Se establecerá un programa de concienciación continua para atender a los miembros de la UMA, en particular a los de nueva incorporación.

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.

El cumplimiento de la presente Política de Seguridad es obligatorio por parte de todo el personal interno o externo que intervenga en los procesos la UMA, constituyendo su incumplimiento infracción grave a efectos laborales.

11 RESOLUCIÓN DE CONFLICTOS.

En caso de conflicto entre los diferentes responsables que componen la estructura organizativa de la Política de Seguridad prevalecerá la decisión del Comité de Seguridad de la Información y la Privacidad.

12 TERCERAS PARTES

Cuando se presten servicios o se gestione información de otras organizaciones, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad de la Información y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando se utilicen servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla.

Se establecerán procedimientos específicos de 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.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Las terceras partes involucradas en tratamientos de datos de carácter personal deberán satisfacer los requisitos establecidos por la UMA y deberán formalizar su relación como encargados de tratamientos.

13 REVISIÓN Y APROBACIÓN DE LA POLÍTICA DE SEGURIDAD

La Política de Seguridad de la Información será **revisada** por el Comité de Seguridad de la Información y la Privacidad a intervalos planificados, que no podrán exceder **el año** de duración,

o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Los cambios sobre la Política de Seguridad de la Información deberán ser aprobados por el órgano superior competente que corresponda, de acuerdo con el artículo 11 del ENS.

Cualquier cambio sobre la misma deberá ser difundido a todas las partes afectadas.

14 Estructura y desarrollo de la Política de Seguridad de la Información.

La estructura jerárquica de la documentación de seguridad es la siguiente:

Documento	Detalle
Política	• Define las metas y expectativas de seguridad. • Describe qué tipo de gestión de la seguridad se pretende lograr y cuáles son los objetivos perseguidos. • Debe ser elaborada por el Comité de Seguridad y ser aprobada por la Dirección.
Normativa	• Establece lo que se debe hacer y uniformiza el uso de aspectos concretos del sistema. • Es de carácter obligatorio. • Debe ser escrita por personas expertas en la materia o por el Responsable de Seguridad y aprobada por el Comité de Seguridad.
Procedimiento	• Determina las acciones o tareas a realizar en el desempeño de un

	proceso relacionado con la seguridad y las personas o grupos responsables de su ejecución. • Un procedimiento debe ser claro, sencillo de interpretar y no ambiguo en su ejecución. No tiene por qué ser extenso, dado que la intención del documento es indicar las acciones a desarrollar. • Un procedimiento puede apoyarse en otros documentos para especificar, con el nivel de detalle que se desee, las diferentes tareas. Para ello, puede relacionarse con otros procedimientos o con instrucciones técnicas de seguridad. • Debe ser elaborado por el Responsable del Sistema y aprobado por el Responsable de Seguridad.
Instrucciones técnicas	• Determina las acciones o tareas necesarias para completar una actividad o proceso de un procedimiento concreto sobre una parte concreta del sistema de información (hardware, sistema operativo, aplicación, datos, usuario, etc.). • Al igual que un procedimiento, son la especificación pormenorizada de los pasos a ejecutar. • Una instrucción técnica debe ser clara y sencilla de interpretar. • Debe documentar los aspectos técnicos necesarios para que la persona que ejecute la instrucción técnica no tenga que tomar decisiones respecto a la ejecución de la misma. A mayor nivel de detalle, mayor precisión y garantía de su correcta ejecución. • Pueden ser elaborados por el Responsable del Sistema o Administrador del Sistema y deben ser aprobados por el Responsable de Seguridad.
Guías	• Tienen un carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos. Por ejemplo, suele haber una guía sobre cómo escribir procedimientos de seguridad. • Las guías ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas. • Deben ser aprobadas por el Responsable de Seguridad.

En la guía CCN-STIC-801 Responsabilidades y Funciones, se detalla el esquema de las principales responsabilidades (quien debe elaborarlo y quién aprobarlo) para cada uno de estos documentos.

15 REFERENCIAS

DOCUMENTOS Y REGISTROS RELACIONADOS			
Código	**Titulo**	**Responsable**	**Periodo de Conservación**

ANEXO. GLOSARIO DE TÉRMINOS

Análisis de riesgos

Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

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.

Gestión de incidentes

Plan de acción para atender a las incidencias 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.

Gestión de riesgos

Actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

Incidente de seguridad

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

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 consideran críticos.

Principios básicos de seguridad

Fundamentos que deben regir toda acción orientada a asegurar la información y los servicios.

Responsable de la información

Persona que tiene la potestad de establecer los requisitos de una información en materia de seguridad.

Responsable de la seguridad

El responsable de seguridad determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Responsable del servicio

Persona que tiene la potestad de establecer los requisitos de un servicio en materia de seguridad.

Responsable del sistema

Persona que se encarga de la explotación del sistema de información.

Servicio

Función o prestación desempeñada por alguna entidad oficial destinada a cuidar intereses o satisfacer necesidades de los alumnos, personal propio PAS o PDI y cualquier ciudadano que se relacione con la UMA.

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.