POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

La Política de Seguridad de la Información se elabora en cumplimiento de la exigencia 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, que en su artículo 11 establece la obligación para las Administraciones Públicas de disponer de una Política de Seguridad e indica los requisitos mínimos que debe cumplir.

Esta Política de Seguridad sigue también las indicaciones de la guía CCN-STIC-805 del Centro Criptológico Nacional, centro adscrito al Centro Nacional de Inteligencia

La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

La Universidad de Almería, hace uso de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos institucionales. En consecuencia, 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.

Por ello, el objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución y 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.

Esto implica que la organización y su personal debe aplicar las medidas mínimas de seguridad exigidas por el Real Decreto 3/2010 (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.

La organización debe 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.

La organización debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

1.1. PREVENCIÓN

La organización debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello se 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, la organización debe:

- 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.

1.2. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, se debe monitorizar la operación de manera continuada 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 produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

1.3. RESPUESTA

La organización debe:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en áreas de la entidad o en otros organismos relacionados con la UAL.
- 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) reconocidos a nivel nacional: Iris-CERT, CCN-CERT,…

1.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, la organización debe desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

2. MISION

Según se refleja en sus estatutos, actualmente en vigor, la Universidad de Almería es una institución de derecho público, dotada de personalidad jurídica y patrimonio propio, a la que corresponde el servicio público de la educación superior mediante la docencia, el estudio y la investigación, con plena autonomía y de acuerdo con la Constitución y las leyes.

De forma estrechamente relacionada con el cumplimiento de esta misión, la organización desea manifestar la necesidad de una infraestructura TIC que prime y fomente las operativas abiertas, enfocadas a la funcionalidad, conectividad y servicio al usuario, como funciones prioritarias para la consecución de los objetivos estratégicos e institucionales.

3. ALCANCE

Debido a la misión de la entidad, reflejada en el punto 3 del presente documento, la organización desestima la aplicación de la presente política de seguridad sobre todo el conjunto del sistema de información.

En base a ello, la organización aplicará la presente política sobre el grueso de los sistemas TIC que gestiona de manera centralizada a través del Servicio de Tecnologías de la

Información y las Comunicaciones, y específicamente sobre todos aquellos sistemas que están relacionados con el ejercicio de derechos por medios electrónicos, con el cumplimiento de deberes por medios electrónicos o con el acceso a la información o al procedimiento administrativo.

De forma concreta la presente política de seguridad es aplicable sobre los siguientes servicios y los sistemas TIC que los conforman:

- **Sistema ERP[1] Institucional:**
  - Gestión Académica
  - Gestión Económica
  - Gestión de RRHH
  - Gestión de la Investigación
  - Gestión de la Calidad
  - Gestión de Espacios
  - Campus Virtual

- **Sistema de Administración Electrónica:**
  - Administración Electrónica
  - Atención al Usuario

- **Sistema de Docencia Virtual**

3.1. Ampliación del Alcance

Adicionalmente y aún entendiéndose que los siguientes servicios no se encuentran directamente en el alcance marcado por el Esquema Nacional de Seguridad, debido a su importancia en la comunidad universitaria, se acuerda extender el alcance al siguiente servicio de la UAL**:**

- **Sistema Web Institucional**

4. MARCO NORMATIVO

Son de aplicación las leyes y normativas españolas en relación a protección de datos personales, propiedad intelectual y uso de herramientas telemáticas. Por todo ello, la UAL podrá ser requerida por los órganos administrativos pertinentes a proporcionar los registros electrónicos o cualquier otra información relativa al uso de los sistemas de información.

[1] ERP = Sistema de Planificación de Recursos Empresariales. Del inglés *Enterprise Resource Planning*

Esta política se sitúa dentro del marco jurídico definido por las leyes y Reales Decretos siguientes:

- Reglamento Europeo de Protección de Datos 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.
- Ley Orgánica de Universidades (6/2001) y Ley Orgánica de modificación de la L.O.U. (4/2007).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Esquema Nacional de Seguridad (RD 3/2010).
- Ley Orgánica de Protección de Datos (15/1999) y Reglamento de desarrollo de la Ley Orgánica (RD 1720/2007).
- Ley de Servicios de la Sociedad de la Información (de 12 de octubre de 2002)

5. ORGANIZACIÓN DE LA SEGURIDAD

5.1. DELEGADO DE PROTECCIÓN DE DATOS (DPD)

Será una persona con conocimiento especializado en Derecho y en la práctica en materia de protección de datos. Estos conocimientos serán exigibles en relación con los tratamientos que se realicen, así como las medidas que deban adoptarse para garantizar un tratamiento adecuado de los datos personales objeto de esos tratamientos.

El Delegado de Protección de Datos debe desempeñar sus tareas y funciones con total independencia.

Las funciones del Delegado se encuentran especificadas en el artículo 39 del *RGPD*, siendo las siguientes:

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones del RPGD y demás normativa aplicable en protección de datos.
- Supervisar el cumplimiento del RGPD y demás normativa aplicable en protección de datos, y de las políticas del responsable o encargado del tratamiento en dicha materia, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en operaciones de tratamiento, y las auditorías correspondientes.
- Ofrecer el asesoramiento que se solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación conforme al artículo 35 del RGPD.

- Cooperar con la Autoridad de control.
- Actuar como punto de contacto de la Autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa del artículo 36 del RGPD, y realizar consultas, en su caso, sobre cualquier otro asunto.

5.2. COMITÉS: FUNCIONES Y RESPONSABILIDADES

Las funciones del **Comité de Gestión del ENS** las asume la actual **Comisión de Seguridad Informática y Protección de Datos**, en adelante Comisión de Seguridad.

La Comisión de Seguridad tendrá informado al Equipo de Gobierno.

Las funciones de la Comisión de Seguridad en relación al ENS son:

- Divulgación de la política y normativa de seguridad de la Organización.
- Aprobación de la normativa de seguridad de la Organización.
- Revisión anual de la política de seguridad.
- Desarrollo del procedimiento de designación de roles.
- Designación de roles y responsabilidades.
- Supervisión y aprobación de las tareas de seguimiento del Esquema Nacional de Seguridad:
    - Tareas de adecuación
    - Análisis de Riesgos
    - Auditoría Bienal

5.3. ROLES: FUNCIONES Y RESPONSABILIDADES

.

Responsable de la información

La **Secretaría General** tendrá el rol de responsable de la información de la Organización. Teniendo por funciones las siguientes:

- Establecimiento de los requisitos de la información en materia de seguridad.
- Trabajo en colaboración con el responsable de seguridad y el de sistema en el mantenimiento de los sistemas catalogados según el Anexo I del Esquema Nacional de Seguridad.

Responsable de los servicios TIC

El Gerente tendrá el rol de responsable de los servicios TIC de la Organización. Teniendo por funciones las siguientes:

- Establecimiento de los requisitos de los servicios TIC en materia de seguridad.
- Trabajo en colaboración con el responsable de seguridad y el de sistema en el mantenimiento de los sistemas catalogados según el Anexo I del Esquema Nacional de Seguridad.

Responsable de Seguridad

El Director del Servicio de Tecnologías de la Información y las Comunicaciones tendrá el rol de responsable de seguridad de la Organización. Teniendo por funciones las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas TIC en su ámbito de responsabilidad.
- Promover la formación y concienciación del Servicio de Tecnologías de la Información y las Comunicaciones dentro de su ámbito de responsabilidad.
- Verificar que las medidas de seguridad establecidas son adecuadas para la protección de la información manejada y los servicios prestados.
- Analizar, completar y aprobar toda la documentación relacionada con la seguridad del sistema.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría implementados en el sistema.
- Apoyar y supervisar la investigación de los incidentes de seguridad desde su notificación hasta su resolución.
- Elaborar el informe periódico de seguridad para el propietario del sistema, incluyendo los incidentes más relevantes del periodo.
- Aprobación de los procedimientos de seguridad elaborados por el Responsable del Sistema.
- Elaboración de la normativa de seguridad de la entidad.

Esta figura de "Responsable de Seguridad" descrita por el ENS, no coincide con la del responsable de seguridad de los ficheros de la UAL.

Responsables del Sistema IT

Se designa a los Jefes de Servicio del Servicio de Tecnologías de la Información y las Comunicaciones en el rol de Responsables del Sistema de la Organización. Teniendo por funciones, dentro de sus áreas de actuación, las siguientes:

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y política de gestión del Sistema 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.
- Aprobar los cambios que afecten a la seguridad del modo de operación del Sistema.
- Decidir las medidas de seguridad que aplicarán los suministradores de componentes del Sistema durante las etapas de desarrollo, instalación y prueba del mismo.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que éstas se integren adecuadamente dentro del marco general de seguridad.
- Determinar la configuración autorizada de hardware y software a utilizar en el Sistema.
- Aprobar toda modificación sustancial de la configuración de cualquier elemento del Sistema.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.
- Determinar la categoría del sistema según el procedimiento descrito en el Anexo I del ENS y determinar las medidas de seguridad que deben aplicarse según se describe en el Anexo II del ENS.
- Elaborar y aprobar la documentación de seguridad del Sistema.
- Delimitar las responsabilidades de cada entidad involucrada en el mantenimiento, explotación, implantación y supervisión del Sistema.
- *Velar por el cumplimiento de las obligaciones del Administrador de Seguridad del Sistema (ASS).*
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al Responsable de Seguridad o a quién éste determine.
- Establecer planes de contingencia y emergencia, llevando a cabo frecuentes ejercicios para que el personal se familiarice con ellos.
- Además, el responsable del sistema puede 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 el responsable de seguridad, antes de ser ejecutada.
- Elaboración de los procedimientos de seguridad necesarios para la operativa en el sistema.

Administrador de la Seguridad del Sistema

El Administrador de Servicios de Red y Seguridad TIC tendrá el rol de Administrador de la Seguridad del Sistema. Teniendo por funciones las siguientes:

- Verificar la aprobación de los procedimientos operativos de seguridad
- Asegurar el cumplimiento de los controles de seguridad
- Asegurar que son aplicados los procedimientos aprobados para manejar el 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
- Supervisar la monitorización del estado de la seguridad del sistema
- Informar a los Responsables de 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.

5.4. POLÍTICA DE SEGURIDAD

Será misión de la Comisión de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por Consejo de Gobierno y difundida para que la conozcan todas las partes afectadas.

6. DATOS DE CARÁCTER PERSONAL

La UAL realiza tratamientos en los que hace uso de datos de carácter personal, adoptando las medidas de seguridad adecuadas siguiendo las directrices del Reglamento Europeo de Protección de Datos, las indicaciones del Delegado de Protección de Datos y manteniendo la suficiente diligencia para cumplir con el principio de responsabilidad proactiva y el principio de accountability que establece la actual normativa de seguridad.

7. GESTIÓN DE RIESGOS

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

- Regularmente, al menos una vez cada dos años
- Cuando cambie la información manejada
- Cuando cambien los servicios prestados
- Cuando ocurra un incidente grave de seguridad
- Cuando se reporten vulnerabilidades graves
- Cuando así lo indique el Delegado de Protección de Datos.

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

El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

8. DESARROLLO DE LA POLÍTICA DE SEGURIDAD

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la intranet, a través del portal de administración electrónica (http://ae.ual.es), y de la página web de la Comisión de Seguridad (http://seguridad.ual.es)

Así mismo podrá encontrarse impresa en el Servicio de Tecnologías de la Información y las Comunicaciones.

9. OBLIGACIONES DEL PERSONAL

Todos los miembros de la UAL tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad desarrollada a partir de ella, siendo responsabilidad de la Comisión de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todos los trabajadores de la UAL atenderán a una acción de concienciación en materia de seguridad TIC al menos una vez cada dos años. Se establecerá un **programa de acciones en concienciación** continua para atender a todos los miembros de la UAL, en particular a los de nueva incorporación, teniendo en cuenta siempre las disponibilidades presupuestarias de la UAL.

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.

10. TERCERAS PARTES

Cuando la UAL preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información. Para ello, se establecerán canales para informe y coordinación de los respectivos Comités de Coordinación del ENS y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la UAL utilice 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 la mencionada normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de informe 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.
El informe debe ser aprobado por los responsables de la información y los servicios afectados antes de seguir adelante.

11. ENTRADA EN VIGOR

Esta política de Seguridad de la Información es efectiva desde el día siguiente al de su fecha de aprobación por el Consejo de Gobierno de la UAL y hasta que sea reemplazada por una nueva Política.

Queda derogada la anterior Política de Seguridad de la Información, que fue aprobada por el Consejo de Gobierno de la Universidad de Almería, en fecha 17 de diciembre de 2012.