

Política de Seguridad de la Información

ENS RD 311/2022

Por: Calidad

28 enero de 2026

SIGMA

helping universities succeed

Información del documento

Documento	Política de Seguridad de la Información
Tipo de documento	Política
Fichero	POL001_Política de Seguridad.docx

Tabla de contenido

1. Introducción	1
1.1. Objeto y Contenido	1
1.2. Ámbito de Aplicación	1
1.3. Distribución	1
2. Definiciones	2
3. Misión de la Organización	2
4. Marco legal y regulatorio	3
5. Estructura organizativa	3
5.1. Nivel de gobierno	3
5.2. Nivel ejecutivo / supervisión	3
5.3. Nivel operacional	3
6. Roles y Responsabilidades	4
6.1. Comité de Continuidad y Seguridad	4
6.2. Dirección General	5
6.3. Responsable de la Información	5
6.4. Responsable del Servicio	5
6.5. Responsable de Seguridad	5
6.6. Responsable del Sistema	6
6.7. Delegado de Protección de Datos	6
6.8. Designación y Coordinación	7
6.9. Gestión de personal y profesionalidad	7
6.10. Datos de Carácter Personal	7
7. Política de Seguridad de la Información	7

7.1. Incidentes de Seguridad y Continuidad de la Actividad	8
7.2. Gestión de riesgos	8
7.3. Terceras Partes	9
7.4. Concienciación y formación	9
7.5. Aplicabilidad de la Política de Seguridad	9
7.6. Mejora Continua	10
8. Revisión y mantenimiento	11
9. Aprobación del documento	11

1. Introducción

En este documento se describe la política que se sigue en SIGMA Gestión Universitaria A.I.E (M.P.), a partir de ahora SIGMA, sobre la seguridad de la información.

Esta política está basada en los principios básicos y en los requisitos mínimos del Real Decreto 311/2022.

1.1. Objeto y Contenido

SIGMA quiere reforzar el compromiso con sus Clientes, expresado en términos de mejora continua del Nivel de Servicio ofrecido, del cumplimiento de la legislación vigente, de la mejora continua de los procesos internos y de la protección de la información de los clientes de la compañía.

La presente Política de Seguridad de la Información fija y alinea los objetivos de seguridad de la compañía con sus necesidades de negocio, en las dimensiones de confidencialidad, integridad, disponibilidad, autenticación y trazabilidad de la Información, tal y como marca el ENS.



El objetivo de esta política es definir el propósito, dirección, principios y reglas básicas para la correcta gestión de la seguridad de la información, siguiendo el estándar UNE-ISO/IEC 20000-1:2018 y del Esquema Nacional de Seguridad (ENS), teniendo en cuenta los requisitos de los servicios, legales y regulatorios, y las obligaciones contractuales de la empresa.



1.2. Ámbito de Aplicación

El alcance de este procedimiento es el enmarcado por la establecido en el Esquema Nacional de Seguridad (ENS) y que aplicará a todos los procesos, usuarios y procedimientos de la organización de SIGMA.

1.3. Distribución

La distribución de este documento se realizará a toda la organización de SIGMA y se publicará en la página web.

2. Definiciones

Concepto	Descripción / Definición
Seguridad de la información	Garantizar la confidencialidad, integridad, disponibilidad de la información, la autenticidad de cada persona con acceso autorizado, la trazabilidad de las tareas realizadas.
Incidencia de seguridad de la información	Evento no deseado, o inesperado, que tiene una alta probabilidad de comprometer las operaciones de negocio y amenazar la seguridad de la información.
Política	<ul style="list-style-type: none"> • Intención y voluntad expresada formalmente por la Dirección con los objetivos o misión de la organización. • El marco legal y regulatorio en el que se desarrollan las actividades. Los roles o funciones de seguridad, definiendo para cada uno, los deberes y responsabilidades del cargo. • La estructura del comité o los comités para la gestión y coordinación de la seguridad, detallando su ámbito de responsabilidad, los miembros y la relación con otros elementos de la organización. • Las directrices para la estructuración de la documentación de seguridad del sistema, su gestión y acceso.
Sistema de información	Conjunto de ficheros automatizados, soportes, equipos y programas utilizados para el almacenamiento y tratamiento de datos.
Confidencialidad	Propiedad de la información por la que se garantiza que esta sólo será accesible por aquellas personas autenticadas y autorizadas a acceder a dicha información.
Integridad	Hace referencia a la corrección y complementación de los datos.
Disponibilidad	Condición donde un recurso dado puede ser accedido por sus consumidores.
Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.
Autenticidad	Es la propiedad que permite identificar el generador de la información después que haya sido autenticado.

3. Misión de la Organización

SIGMA como agrupación sin ánimo de lucro se centra en ayudar a las instituciones de educación superior en la optimización de la gestión de sus tecnologías de la información (TI), aportando soluciones avanzadas para la gestión académica, docencia e investigación.

Las soluciones que aporta SIGMA se basan en:

- SIGMA Academic: Solución cloud que ofrece servicios para la gestión académica universitaria.

- SIGMA Research: Solución cloud que ofrece servicios para la gestión del ciclo de vida de la investigación.

SIGMA, como proveedor de servicio y soluciones tecnológicas completas e innovadoras, reconoce la importancia de la información como activo fundamental para poder desarrollar sus servicios.

Es por ello, que la organización asume la seguridad de la información como una responsabilidad asociada a la protección de esta, teniendo en cuenta todas las dimensiones que le afectan.

4. Marco legal y regulatorio

Como base normativa para realizar la presente política, se ha analizado la legislación vigente que afecta al desarrollo de las actividades propias de SIGMA. Estas normativas están recogidas en un documento que incorpora todas las leyes actualizadas que se aplican en SIGMA y que, de forma periódica, la organización revisa con la finalidad de cumplir y estar siempre alineada con la legislación vigente.

5. Estructura organizativa

A continuación, se enumeran los distintos niveles existentes en SIGMA referentes a la seguridad de la información.

5.1. Nivel de gobierno

El nivel de gobierno será el encargado de definir la estrategia de la compañía a nivel de seguridad de la información y seguridad integral. Este nivel estará formado por:

- Dirección General
- Responsable de la Información
- Responsable del servicio

5.2. Nivel ejecutivo / supervisión

El nivel de supervisión será el encargado del control y supervisión de la correcta ejecución de las estrategias definidas. Este nivel estará formado por:

- Responsable de Seguridad
- Técnico de Mejora Continua
- Delegado de Protección de Datos

5.3. Nivel operacional

El nivel operacional será el encargado de desarrollar y ejecutar las estrategias definidas en el nivel de gobierno. Este nivel estará formado por:

- Responsable del Sistema
- Técnicos de Tecnología

6. Roles y Responsabilidades

A continuación, se enumeran los distintos roles existentes en SIGMA referentes a la seguridad de la información y sus responsabilidades:

- Dirección General.
- Responsable de la Información.
- Responsable del servicio.
- Responsable de Seguridad.
- Responsable del Sistema.
- Delegado de Protección de Datos.

Un sistema de gestión de la seguridad de la información debe comprometer a todos los miembros de una organización, con el detalle de los roles y sus responsabilidades dentro de cada comité de seguridad.

6.1. Comité de Continuidad y Seguridad

Los miembros integrantes del Comité de Seguridad de la Información son los mismos que los del Comité de Continuidad del Servicio, por lo que se han unificado los dos comités en el Comité de Continuidad y Seguridad (CCyS).

El CCyS es responsable de:

- La gestión de los aspectos físicos y lógicos de seguridad de la información.
- La coordinación de servicios para evitar disfunciones y maximizar el uso.
- La coordinación de adquisiciones y desarrollos, con el fin de decidir las inversiones y controlar el gasto.
- La coordinación y la gestión de actividades y revisiones de seguridad de la información.
- La elaboración y aprobación de las políticas, normas, procedimientos, planes e instrucciones de seguridad de la información que garanticen el cumplimiento de los principios contenidos en la presente política.
- La revisión periódica de las políticas, normas, procedimientos, planes e instrucciones de seguridad de la información para garantizar la eficiencia y la eficacia de los controles de seguridad, y para recomendar e implementar mejoras cuando sea necesario.
- La identificación de las tendencias y los cambios significativos en los niveles de riesgo de seguridad de la información para, en su caso, proponer mejoras de control.
- La revisión de los principales incidentes de seguridad para, en su caso, recomendar mejoras estratégicas que permitan hacer frente a las causas raíz.
- Responsabilidades derivadas del tratamiento de datos de carácter personal.
- Realizar una reunión anual con un acta informativa donde son tratados los siguientes puntos:
 - Designación de los roles para el próximo ciclo anual.
 - Normativa vigente que aplica.

- Revisión de los análisis de Impacto.
- Categorización del sistema.
- Los resultados del análisis de riesgos y la eficacia de las medidas adoptadas para gestionar los riesgos.
- Mapas de las instalaciones y diagramas de red.
- Tráfico externo e interno de SIGMA.
- Cambios en el Inventario de Activos y licenciamiento.
- Incidentes de seguridad detectados.
- Cambios en los procedimientos, políticas, instrucciones, planes y normativas.
- Resultados y acciones de seguimiento de Auditorías.
- Oportunidades de mejora.
- Estado de las acciones preventivas y correctivas
- Compromiso con las políticas de gestión de servicios

6.2. Dirección General

Su función es proporcionar los recursos necesarios para garantizar la correcta implementación de la Política de Seguridad de la Información de SIGMA y nombrar a los encargados de los diferentes roles presentes en el Comité de Continuidad y Seguridad (CCyS).

6.3. Responsable de la Información

Las responsabilidades del Responsable de la Información son las siguientes:

- Establecer los requisitos de la información en materia de seguridad de la información.
- Determinar los niveles de seguridad de la información.

Aunque la aprobación formal de los niveles corresponde al Responsable de la Información, puede consultar al Responsable de Seguridad si fuera necesario.

6.4. Responsable del Servicio

Las responsabilidades del Responsable del Servicio son las siguientes:

- Establecer los requisitos del servicio en materia de seguridad de la información.
- Garantizar el servicio y su calidad.
- Verificar que el correcto funcionamiento de los servicios.

Aunque la aprobación formal de los requisitos corresponde al Responsable de la Servicio, podrá consultar al Responsable de Seguridad si fuera necesario.

6.5. Responsable de Seguridad

Las responsabilidades del Responsable de Seguridad son las siguientes:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad.

- Realizar o promover las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de SIGMA Gestión Universitaria, A.I.E (M.P).
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Verificar que las medidas de seguridad establecidas son las adecuadas para la protección de la información manejada y los servicios prestados.
- Aprobación de la Declaración de aplicabilidad.
- Aprobación de la Categorización del sistema.
- Comunicación directa con el CCN.
- Comunicación directa con el Responsable de Seguridad de las instituciones.
- Llevar a cabo el preceptivo proceso de análisis y gestión de riesgos en el Sistema.

6.6. Responsable del Sistema

Las responsabilidades del Responsable del Sistema son las siguientes:

- Desarrollar, operar y mantener el Sistema durante todo su ciclo de vida, incluyendo 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 de este.
- Implantar y controlar las medidas específicas de seguridad del Sistema y cerciorarse de que estas 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.
- 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.
- Investigar los incidentes de seguridad que afecten al Sistema, y en su caso, comunicación al responsable de Seguridad o a quién este determine.

6.7. Delegado de Protección de Datos

Las responsabilidades del Delegado de Protección de Datos son las siguientes:

- Evaluación de impacto de las operaciones de tratamiento de datos.
- Comunicación directa con la AEPD.
- Responsabilidades derivadas del tratamiento de datos de carácter personal.

- Comunicación directa con los Delegados de Protección de Datos de las instituciones.

6.8. Designación y Coordinación

Los diferentes roles dentro de la organización deberán ser adjudicados por la Dirección General.

El nombramiento será revisado de forma periódica o cuando el puesto quede vacante.

La coordinación entre los diferentes comités y los diferentes responsables o delegados, se realizará siempre a través de la Dirección General, quien, en caso de conflictos, será el ente encargado de resolverlos.

6.9. Gestión de personal y profesionalidad

La gestión del personal, así como su profesionalidad quedará supeditada a la evaluación que realice el responsable directo, basándose siempre en:

- Cumplimiento de Política de Seguridad y Normativa
- Formación y Capacitación
- Relación de tareas asignadas al puesto de trabajo

6.10. Datos de Carácter Personal

SIGMA Gestión Universitaria, A.I.E (M.P.) trata datos de carácter personal, en base a ello y ajustándose a la legalidad vigente, la organización realiza:

- AARR Datos de Carácter Personal
- Registro de Actividades de Tratamiento
- Cláusulas Informativas (actualizadas)
- Evaluación de Impacto

Con el fin de proteger y garantizar la confidencialidad e integridad de los datos de carácter personal.

7. Política de Seguridad de la Información

La Política de Seguridad se desarrolla mediante políticas, normativas, procedimientos, planes e instrucciones que definen la forma en la que se aplica a los distintos procesos y activos de SIGMA, de forma que se puedan alcanzar en cada ámbito los niveles necesarios para el cumplimiento global de los objetivos de Negocio y de Seguridad de la compañía.

Las políticas, normativas, procedimientos, planes e instrucciones del sistema de gestión de la seguridad de la información han sido revisados y aprobados por los miembros del comité (CCyS), junto con la dirección, manteniendo el siguiente compromiso:

- Promover las nuevas medidas en materia de Seguridad al resto de la compañía.

- Cumplir con los controles requeridos por el Esquema Nacional de Seguridad – ENS
- Cumplir con los controles previstos en la directiva europea Network and Information Security - NIS2.
- Asegurar que se cumplen todos los requisitos legales aplicables.
- Impulsar la mejora continua y la innovación en los servicios y el modelo de gestión.
- Facilitar la formación al personal de la compañía en materia de Seguridad de la Información.
- Mejorar la eficiencia de los procesos, controlando los costes.
- Incrementar la calidad de los Servicios.
- Verificar el correcto tratamiento de los datos personales.

Los diferentes departamentos deben cerciorarse de que la seguridad es una parte integral del ciclo de vida de los sistemas y servicios propios de SIGMA.

En esta línea, deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

- **Prevenir:** Se 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.
- **Detectar:** Se debe monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia.
- **Reaccionar:** Se debe establecer mecanismos para responder eficazmente a cualquier incidente que pueda afectar a la seguridad.
- **Recuperarse:** Se debe garantizar la disponibilidad de los servicios críticos

7.1. Incidentes de Seguridad y Continuidad de la Actividad

En el marco de las obligaciones previstas en el RD 311/2022, SIGMA pondrá en conocimiento del Centro Criptológico Nacional los incidentes de seguridad que puedan comprometer de forma significativa la gestión de la seguridad de la información y los servicios prestados.

Asimismo, cuando como consecuencia de un incidente se produzca una posible vulneración de datos personales, se llevará a cabo la comunicación pertinente a la Agencia Española de Protección de Datos, respetando el plazo máximo de 72 horas establecido por la normativa aplicable.

7.2. Gestión de riesgos

La información se expone a riesgos y amenazas dinámicas que pueden ser: internas o externas y accidentales o intencionadas. La materialización de alguna de estas amenazas puede provocar pérdidas materiales, económicas, daños en la imagen, confianza en los clientes, incumplimientos etc.

La Dirección de SIGMA asume la seguridad de la información como una responsabilidad asociada a la protección de esta en las dimensiones de: integridad, confidencialidad, disponibilidad, trazabilidad y autenticidad.

Para ello, SIGMA cuenta con una metodología de Análisis y gestión de Riesgos basada en las mejores prácticas.

Durante la ejecución del Análisis de Riesgos se realiza:

- Identificación y evaluación de activos.
- Identificación y evaluación de amenazas.
- Identificación y evaluación de salvaguardas.
- Identificación y valoración del riesgo inherente.
- Identificación y valoración del riesgo residual.

7.3. Terceras Partes

Una buena gestión de los recursos externos permitirá a reducir en gran parte los riesgos asociados a dichos servicios. Es por ello que:

Cuando SIGMA haga uso de servicios de terceros deberá, en la medida de lo posible:

- Hacer partícipes a los colaboradores externos de la Normativa de Seguridad, así como de los procedimientos que se consideren oportunos según el tipo de servicio que presten, en caso de usar los recursos tecnológicos de SIGMA. Por lo que, dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa.
- Establecer canales de comunicación, reporte y resolución de incidencias.
- Garantizar que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos con los niveles exigidos en esta Política.

Cuando alguno de los puntos establecidos en la Normativa de Seguridad de SIGMA o en alguno de los procedimientos facilitados no puedan ser satisfechos por las terceras partes, se requerirá un informe del Responsable de Seguridad identificando los riesgos asociados y la forma de tratarlos.

De igual forma, en el caso de que SIGMA preste servicios o maneje información de otras organizaciones, se les hará partícipe de la Normativa de Seguridad y se tratarán de establecer canales para el reporte y coordinación con la organización, así como procedimientos o procesos de actuación en caso de incidentes de seguridad.

7.4. Concienciación y formación

Todos los miembros de SIGMA deberán disponer de la formación adecuada para el desempeño de sus funciones.

Además, deberá asegurarse la adecuada concienciación de los miembros de SIGMA en términos de Seguridad de la Información y buenas prácticas.

7.5. Aplicabilidad de la Política de Seguridad

El cumplimiento de la presente política es obligatorio para todo el personal de SIGMA tanto interno como externo y cualquier excepción deberá ser comunicada y aprobada por parte de la Dirección o por aquellos que la Dirección haya establecido.

La dirección general de SIGMA se compromete a proporcionar los medios necesarios para la comunicación de la Política de Seguridad de la Información.

SIGMA implementará controles para detectar posibles incumplimientos, así como comportamientos o usos indebidos de los recursos de la empresa. Dichos controles se efectuarán de manera aleatoria o en casos en los que se tenga sospecha de mal uso, no implicando en ningún caso una violación de la privacidad de los usuarios.

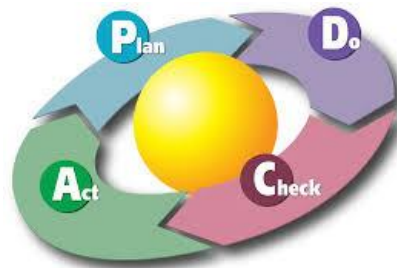
El incumplimiento de la Política de Seguridad podrá suponer sanciones y, en caso de que se considere oportuno, acciones legales.

7.6. Mejora Continua

La protección de una organización no sólo requiere la implementación de medidas de seguridad y su documentación, sino que es necesario la aplicación de un proceso de mejora continua.

Por tanto, la mejora continua es un eje principal en la evolución y progreso de la seguridad en la organización y, consecuentemente, en la disminución de los riesgos a los que se expone. Por ese motivo, SIGMA cuenta con un procedimiento de Mejora Continua que establece las actividades específicas a realizar por parte de los diferentes equipos con la finalidad de conseguir dicha mejora.

El proceso de mejora continua de SIGMA se fundamenta en las mejores prácticas nacionales e internacionales y está basado en el ciclo de Deming, o ciclo PDCA (Plan-Do-Check-Act), que es una metodología de gestión de cuatro pasos —planificar, hacer, verificar y actuar— enfocada en la mejora continua de procesos, productos y servicios.



- **P (Plan-Planificar):** se planifica cómo se implementa la seguridad dentro de la compañía.
- **D (Do-Hacer):** se implementan las medidas de seguridad y procedimientos para responder a las necesidades de la organización.
- **C (Check-Verificar):** se controla cómo están funcionando las medidas de seguridad y procedimientos implementados y si se están alcanzando los resultados esperados.

- **A (Act-actuar):** en base a los controles realizados, se analiza qué aspectos deben mejorarse y se proponen las acciones necesarias para corregir las desviaciones encontradas.

SIGMA promueve:

- Que todo el personal colabore en la identificación de mejoras. Personal interno, proveedores y clientes son partes fundamentales de la seguridad de la organización y deben participar en la mejora de esta.
- Todas las mejoras propuestas, serán analizadas y valoradas según los criterios establecidos para priorizarlas.
- Las propuestas de mejora formuladas deben estar directa o indirectamente relacionadas con la gestión de la seguridad de la organización.
- Cualquier acción preventiva o correctiva que se detecte se tratará como una posible propuesta de mejora.

8. Revisión y mantenimiento

La presente Política deberá ser revisada de manera anual o siempre que se produzcan cambios significativos dentro de la organización.

9. Aprobación del documento

El presente documento (v.7.0) ha sido aprobado por el Comité de Continuidad y Seguridad (CCyS) a fecha 28/01/2026.



helping universities succeed

Política de Seguridad de la Información

28/01/2026