

Resumen de acciones realizadas para la adecuación al ENS (Esquema Nacional de Seguridad)

ANTECEDENTES NORMATIVOS

La Política de Seguridad de la Información recoge la postura de la FGUCM en cuanto a la seguridad de la información y establece los criterios generales que deben regir la actividad del organismo en cuanto a la seguridad.

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 de información deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad, 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 se deben aplicar las **Cláusulas de la norma ISO/IEC 27001, las medidas de seguridad exigidas por el Esquema Nacional de Seguridad, el Reglamento (UE) 2016/679 General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante SGSI, ENS, RGPD y LOPDGDD)**, 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 FGUCM utiliza las Tecnologías de la Información y las Comunicaciones para prestar sus servicios, por lo que es consciente de que estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados.

Asimismo, también es consciente de que los incidentes de seguridad pueden estar provocados desde lugares remotos, a través de las conexiones a redes de comunicaciones de las que se dispone y, muy concretamente, a través de las conexiones a la internet (ciberataques).

Esta Política de Seguridad de la Información se aplica a todos los servicios prestados por la FGUCM que se apoyen en las Tecnologías de la Información y las Comunicaciones, así como a todo el personal, sin excepciones.

Todo el personal de la FGUCM que tenga algún tipo de relación con el uso, la gestión, mantenimiento y explotación de la información y de los servicios prestados sobre ella, tiene la obligación de conocer la Política de Seguridad de la Información y cumplirla. El Comité de Seguridad de la Información dispondrá los medios para que esta Política llegue a los interesados.

ACCIONES REALIZADAS PARA LA ADECUACIÓN AL ENS

1. Contratación de una consultora para la implantación del ENS en la Fundación Complutense.

Como entidad del sector público estamos obligados en aplicación de las **SGSI, ENS, RGPD y LOPDGDD**, y la propia UCM nos exige estar certificados en el ENS para poder continuar con el encargo de gestión de las actividades de la UCM que la FGUCM gestiona. La empresa contratada para la adecuación al ENS es BABEL

2. Establecimiento de roles y responsabilidades

Comité de Seguridad de la Información

- Dirección de la entidad
- Responsable de Sistemas
- Responsable de Seguridad
- Delegada de Protección de Datos
- Responsables de la Información y del Servicio

3. Aprobación de un marco normativo

Está conformado por la Política de Seguridad, normativas y procedimientos para dar soporte al cumplimiento del ENS y al RGPD y, por consiguiente, a la protección de los sistemas de información. Aprobado por la Dirección de la Fundación y por el Comité de Seguridad de la Información.

Desarrollo de la Política de Seguridad de la Información

Esta Política de Seguridad de la Información se desarrollará mediante la elaboración de otras políticas o normativas de seguridad que abordan aspectos específicos. A raíz de dichas políticas y normativas se podrán desarrollar procedimientos que describan la forma de llevarlas a cabo.

Este marco normativo se encontrará a disposición de todo el personal de la organización que necesite conocerla y, en particular, el personal que utilice, opere o administre los sistemas de información y comunicaciones o la información misma albergada en dichos sistemas o los servicios prestados por la FGUCM.

La Política de Seguridad de la Información es de obligado cumplimiento y se estructura en los siguientes niveles relacionados jerárquicamente:

- 1) Primer nivel: Política de Seguridad de la Información.
- 2) Segundo nivel: Normativas de Seguridad de la Información.
- 3) Tercer nivel: Procedimientos e Instrucciones Técnicas de Seguridad de la Información.
- 4) Cuarto nivel: Informes, registros y evidencias electrónicas.

La estructura jerárquica permite adaptar con eficiencia los niveles inferiores a los cambios en los entornos operativos de la FGUCM, sin necesidad de revisar su estrategia de seguridad.

El personal de la FGUCM tendrá la obligación de conocer y cumplir, además de la Política de Seguridad de la Información, todas las Normativas, los Procedimientos e Instrucciones Técnicas de Seguridad de la Información que puedan afectar a sus funciones.

La Política, las Normativas, los Procedimientos e Instrucciones Técnicas de Seguridad de la Información estarán disponibles para todos los empleados en la Intranet de la FGUCM según vaya siendo aprobadas.

1) Primer nivel: Política de Seguridad de la Información

Este documento es de obligado cumplimiento por todas las personas, internas y externas, de la FGUCM, recogido en el presente documento y aprobado por la Dirección General de la FGUCM.

2) Segundo nivel: Normativas de Seguridad de la Información

De obligado cumplimiento de acuerdo con el ámbito organizativo, técnico o legal correspondiente.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Comité de Seguridad de la Información con el asesoramiento del Responsable de Seguridad de la Información.

3) Tercer nivel: Procedimientos e Instrucciones Técnicas de Seguridad de la Información

Documentos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.

La responsabilidad de aprobación de estos procedimientos técnicos es del Responsable del Sistema de Información correspondiente, bajo la supervisión y asesoramiento del Responsable de Seguridad de la Información.

En caso de que los procedimientos afectarán a varios sistemas de información será responsabilidad del Responsable de Seguridad de la Información aprobarlos.

4) Cuarto Nivel: Informes, registros y evidencias electrónicas

El cuarto nivel está constituido por documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una valoración; documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información, así como también evidencias electrónicas generadas durante todas las fases del ciclo de vida del sistema de información.

La responsabilidad de que existan este tipo de documentos es de cada uno de los Responsables de los Sistemas de Información en su ámbito.

5) Otra documentación

Se podrá seguir en todo momento los procedimientos, normas e instrucciones técnicas STIC, así como las guías CCN-STIC de las series 400, 500, 600 y 800.

Las normativas UNE-ISO/IEC 27001 y demás relacionadas.

Los reglamentos, órdenes, decretos y resto de legislación relativa a la protección de datos personales tanto procedentes de la Unión Europea como del Estado Español.

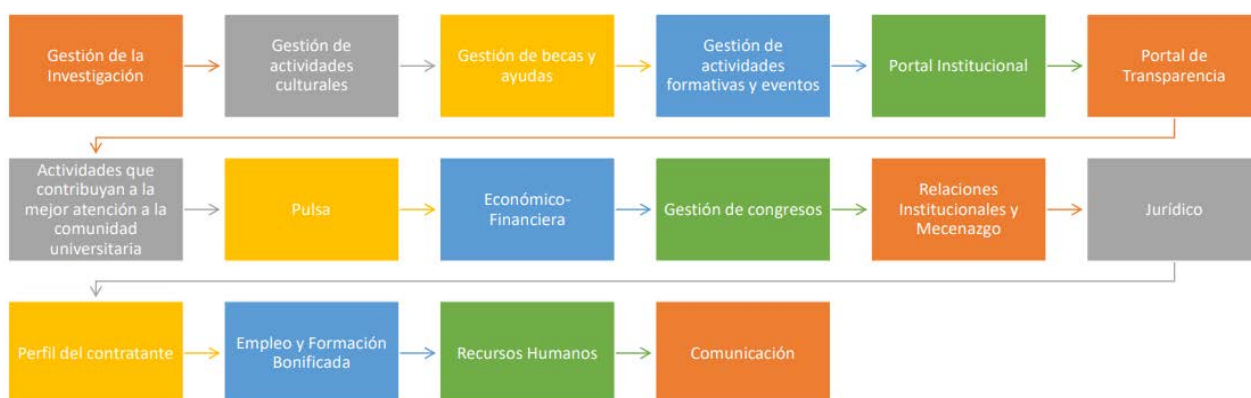
[Políticas y procedimientos sobre Protección de Datos](#)

Desde el año 2016, que se realizó la primera auditoría en Protección de datos, se aprobó el **Protocolo de uso de información** que fue actualizado en el 2021, y difundido entre todo el personal a través de los canales habituales, correo electrónico institucional e incorporaciones a la intranet

4. Realización del Análisis de Riesgos y elaboración de un Plan Director de Seguridad ENS por parte de Babel.

Establecimiento de 16 Servicios en la Fundación, que no tienen correspondencia directa con los departamentos pero en los que se han tenido en cuenta las actividades y fines definidos en los Estatutos de la Fundación y en el Encargo de gestión firmado con la UCM.

• Servicios esenciales de la Fundación



Declaración de aplicabilidad de **categoría del sistema: MEDIA**, habiendo categorías baja, media y alta. Esto supone la adopción de 68 medidas en diferentes ámbitos. Marco organizativo, marco operacional y medidas de protección.

Análisis de riesgos consistente en:

- Identificación: Identifica los activos que hay que proteger, las amenazas, las vulnerabilidades y su grado de exposición.
- Análisis: Evalúa los riesgos que afectan a la seguridad de la información. Para ello se ha tomado como referencia el ENS.
- Tratamiento: Establece medidas para reducir los riesgos a niveles aceptables.

Una vez conocidos los riesgos se ha elaborado un

5. Plan Director de Seguridad que es el conjunto de acciones que se ha diseñado para cumplir con los requisitos mínimos del ENS y para reducir los riesgos identificados en la FGUCM.

6. Formación y concienciación

- Formación anual
 - Sesión formativa ENS 10 y 11 de octubre de 2023
 - Sesión formativa Protección de Datos 11 y 13 de diciembre de 2023

Anualmente se ofrecerá a todos los trabajadores de la Fundación cursos de formación relativos a la Seguridad de la Información y Protección de Datos, en 2024 está previsto impartirla en otoño.

- Concienciación

Envío mensual de consejos de seguridad por correo electrónico al personal de la Fundación y publicación en la [intranet](#)

7. Elaboración del Análisis de impacto realizado por Babel.

- Objetivo: evaluar el impacto financiero, operativo y legal de una interrupción de los servicios y la pérdida de la información.
- Proceso: identifica los procesos de negocio críticos, los sistemas de información que los soportan y los activos de datos asociados.
- Resultados: permite priorizar las medidas de recuperación y establecer planes de contingencia en caso de desastres.

8. Programada la Auditoría interna que realizará Babel en el último cuatrimestre de este año.

Es una revisión que se lleva a cabo para evaluar si se cumplen con los requisitos del ENS y si los riesgos existentes están controlados. Para ello se realizarán entrevistas con los responsables de las diferentes áreas y por lo tanto se requiere de la colaboración de la FGUCM. El resultado es un informe dónde se identificarán las deficiencias, las cuales habrá que solventar.

9. Programada la Auditoría externa que realizará Bureau Veritas tras la adjudicación de un contrato menor.

Es una revisión que se lleva a cabo para evaluar si se cumplen con los requisitos del ENS y si los riesgos existentes están controlados. Pero es realizada por una entidad certificadora externa. Se realizarán entrevistas con los responsables de las diferentes áreas y por lo tanto se requiere de la colaboración de la FGUCM. El resultado es un informe dónde se identifican las deficiencias, las cuales hay que documentar, presentar a la entidad certificadora externa y solventar. Objetivo final: obtención de CERTIFICACIÓN DE CONFORMIDAD CON EL ENS (categoría MEDIA), representando que se cumplen con las exigencias mínimas establecidas en el ENS.

OTRAS ACTUACIONES

1. Presentación del **informe INES** (Informe Nacional del Estado de Seguridad de la Administración pública) ante el Centro Criptológico Nacional. Dicho informe permite evaluar regularmente el estado de la seguridad de los sistemas TIC de las entidades, organismos y organizaciones, además de su adecuación e implantación al Esquema Nacional de Seguridad (ENS) adaptándose a otros estándares o normas reguladoras en caso necesario.

2. Implantación de la obligatoriedad del **doble factor (2FA)** para las conexiones a los servicios de la UCM (Gmail, Drive, web UCM, etc.)

3. **Migración y suscripción anual a Fundanet Cloud.** Servicios mantenimiento, actualización y soporte técnico del sistema de gestión integrado de Fund@net, al objeto de que dicha herramienta se mantenga operativa en todo momento, así como en la distribución de las evoluciones que se realicen sobre dicho sistema en el tiempo.

4. **Verificación en 2 pasos de WhatsApp** para aquellos que dispongan de un teléfono móvil de la Fundación y los que utilicen la aplicación desde sus teléfonos móviles particulares pero para temas laborales, deberán abstenerse de compartir datos de la Fundación o datos de carácter personal a través de esa vía; utilizando de forma preferente el correo electrónico o Google Drive para compartir documentación.

5. **Fomento del uso de las carpetas compartidas en Google Drive**

6. **Campaña del uso de certificados digitales FNMT de ciudadano** entre todos los trabajadores de la Fundación.

7. **Uso de los programas de AutoFirma y Portafirmas** para la firma de documentos de una forma directa, segura y con sello de tiempo tanto a nivel interno de la Fundación como en las relaciones con terceros (firma de convenios, acuerdos marco, contratos resultado de licitaciones...)

8. **Inventario sistematizado y actualizado de los equipos informáticos y dispositivos móviles,**

9. Adquisición del **software MDM** (*Mobile Device Management*) para la gestión de dispositivos portátiles, así como móviles que acceden a Sistemas de Información corporativos. Es un software que permite asegurar, monitorizar y administrar dispositivos móviles sin importar el operador de telefonía o proveedor de servicios. La mayoría de las MDM permiten instalar aplicaciones, actualizaciones, localizar y rastrear equipos, sincronizar archivos, reportar datos y acceder a dispositivos, todo esto de manera remota, con un enfoque principalmente orientado a incrementar su seguridad, y mejorando colateralmente la productividad del usuario final.

10. Adquisición del **software Epulpo** solución GRC (Governance, Risk, and Compliance: gobierno, riesgo y conformidad) que proporciona una gestión integral de los procesos TI (tecnología de la información) y de la seguridad de la información de la Fundación. Permitirá

automatizar y centralizar el proceso completo de gestión y compliance de la Seguridad IT en apoyo al cumplimiento del ENS, RGPD y SGSI, además de la gestión de servicios conforme a ISO 20000/ITIL.

11. Continua comunicación de la Fundación a sus trabajadores donde se está informando sobre el desarrollo de las medidas de implantación para la adecuación del ENS.

12. Actualización y desarrollo de las secciones de Protección de Datos y Seguridad de la Información en la intranet de la Fundación incluyendo la definición, objetivos, responsabilidades, funciones, datos de contacto, concienciación, legislación nacional, normativa y procedimientos internos, enlaces de interés.

13. Revisión y actualización de los formularios utilizados por los diferentes departamentos de la Fundación cuidando especialmente la información relativa a la protección de datos. Dichos formularios están disponibles en la sección correspondiente de la intranet y comunicado a todo el personal de la Fundación.

14. Actualización y desarrollo de las secciones de Protección de Datos y Seguridad de la Información en la página web de la Fundación

15. Envío por correo, publicación en la intranet de la Fundación y petición de la firma de los trabajadores de una serie de documentos de seguridad con el fin de que quede constancia de que conocen y van a adoptar las medidas necesarias para preservar la información y los datos personales que manejan, al igual que la Fundación Complutense está implantando todos los medios materiales y tecnológicos requeridos para preservar la seguridad de la información. Esto es un proceso progresivo en el que la Fundación Complutense está invirtiendo una cantidad de tiempo, recursos personales y materiales importantes, pero en el que es imprescindible la colaboración de todos.

Madrid, a 1 de julio de 2024