Seguridad de las Tecnologías de Información y Comunicaciones

Política de Seguridad de la Información

Noviembre 2023

SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Babel Group	Responsable de Seguridad y DPD	Dirección General de la FGUCM
firma:	firma:	firma:

HISTORIAL DE CAMBIOS

NOMBRE DEL FICHERO	VERSIÓN	RESUMEN DE CAMBIOS PRODUCIDOS	FECHA
FGUCM STIC-POL - Política de Seguridad de la Información v1.0.docx	1.0	Primera edición del documento	14/04/2023
FGUCM STIC-POL - Política de Seguridad de la Información v1.1.docx	1.1		01/10/2023

CLASIFICACIÓN DEL DOCUMENTO

USO INTERNO
Nota de confidencialidad: La información contenida en este documento es de USO INTERNO y sólo se puede utilizar de acuerdo con la cláusula de CONTROL DE DISTRIBUCIÓN. Es responsabilidad del Área o Departamento receptor de este documento su distribución interna en base a la necesidad de conocer la información aquí contenida.

CONTROL DE DISTRIBUCIÓN

AUTOR(ES): Babel Group
DISTRIBUCIÓN: FUNDACIÓN GENERAL DE LA UNIVERSIDAD COMPLUTENSE DE MADRID

REFERENCIAS

DOCUMENTOS INTERNOS	
Título	**Nombre del fichero**
[1] Marco Normativo de FUCM	FGUCM STIC-POL - Marco normativo v1.00.docx

DOCUMENTOS EXTERNOS
[1] CCN-STIC-801 ENS. Responsabilidades y funciones
[2] CCN-STIC-805 ENS-Política de Seguridad de la Información
[3] CCN-STIC-402: Organización y Gestión para la Seguridad de los Sistemas TIC. 2006
[4] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad
[5] 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 (Reglamento general de protección de datos)
[6] Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales
[7] ISO/EIC ISO 27001 Information security, cybersecurity and privacy protection - Information security management systems - Requirements

CUMPLIMIENTO	
ENS	RGPD
org.1 Política de seguridad	

Contenido

1. Introducción

Este documento constituye la Política de Seguridad de la Información de la **FUNDACIÓN GENERAL DE LA UNIVERSIDAD COMPLUTENSE DE MADRID (FGUCM)**, en cumplimiento del artículo 12 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, por el que se establece los requisitos mínimos de Seguridad en el ámbito de la Administración Electrónica, y de la medida de seguridad org.1 contemplada en el Anexo II de dicho Real Decreto.

En este sentido, el mencionado artículo 12, en su apartado 2, establece que "*Cada administración pública contará con una política de seguridad formalmente aprobada por el órgano competente. Asimismo, cada órgano o entidad con personalidad jurídica propia comprendido en el ámbito subjetivo del artículo 2 deberá contar con una política de seguridad formalmente aprobada por el órgano competente.*"

La estructura de este documento sigue las pautas establecidas por la guía CCN-STIC-805 para la redacción de la Política de Seguridad de la Información en el ámbito del Esquema Nacional de Seguridad.

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.

2. La Fundación General de la Universidad Complutense de Madrid (FGUCM)

La Fundación General es una institución sin ánimo de lucro, constituida en 1984 como resultado de la fusión de dieciocho Fundaciones de la Universidad Complutense de Madrid (UCM), fruto de donaciones privadas, tanto monetarias como patrimoniales. Los objetivos y fines coinciden con los de la UCM, por lo que sus actividades esenciales se identifican con la gestión de la investigación, la formación y de la transferencia del conocimiento, a partir de fondos mayoritariamente públicos y también procedentes de instituciones privadas.

3. Marco Normativo

Esta política se enmarca en el marco regulatorio especificado en el documento *Marco Normativo de FGUCM*.

4. Política General de Seguridad

El objeto de la presente Política es establecer la postura de la FGUCM respecto a la Seguridad que afecta a los procesos relacionados con el desempeño de sus funciones y, muy particularmente, con los relacionados con la administración electrónica, tanto desde el punto de vista de los usuarios de los servicios, como desde el punto de vista interno, para la gestión de la propia Entidad.

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).

La política de la FGUCM es la de contrarrestar las amenazas mencionadas anteriormente con los medios suficientes, dentro de las posibilidades presupuestarias. Para este fin, se establecerá una estructura de seguridad, junto con los mecanismos apropiados para su gestión, y un conjunto de instrumentos de apoyo de forma que se garantice:

- el cumplimiento de los objetivos de su misión y de prestación de servicios.
- el cumplimiento de la legislación y normativa aplicables.

Para ello,

- se preverán y desplegarán medidas para evitar incidentes de seguridad que pudieran afectar al cumplimiento de objetivos o poner en riesgo la información.
- se diseñarán medidas de respuesta ante incidentes de seguridad, física o lógica, de forma que se minimice el impacto de estos, en caso de que ocurrieran.

Como norma general, se tendrá un enfoque de orientación al riesgo a la hora de diseñar las medidas de seguridad necesarias, poniendo más foco y esfuerzo en la mitigación de lo que suponga un mayor riesgo.

Las distintas áreas bajo cuya responsabilidad se encuentran los servicios prestados deberán contemplar la seguridad desde el mismo momento en que se concibe un nuevo sistema o servicio, aplicando para estos y para los ya existentes, las medidas de seguridad prescritas por el Esquema Nacional de Seguridad para garantizar la disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad de los servicios y de la información.

Los requisitos de seguridad de los sistemas, las necesidades de formación de los usuarios, administradores y operadores y las necesidades de financiación deben ser identificados e incluidos en la planificación de los sistemas y en los pliegos de prescripciones utilizados para la realización de proyectos que involucren a las TIC.

Se deben articular mecanismos de prevención, reacción y recuperación con objeto de minimizar el impacto de los incidentes de seguridad.

En cuanto a la prevención, se debe evitar que los servicios y la información resulten afectados por un incidente de seguridad. Para ello, La FGUCM implementará las medidas de seguridad establecidas en el

Anexo II del ENS, así como medidas adicionales que pudieran ser identificadas en el proceso de análisis de riesgos.

En cuanto a la detección, se establecerán mecanismos de detección, comunicación y gestión de incidentes de seguridad, de forma que cualquier incidente pueda ser tratado en el menor plazo posible. Siempre que sea posible, se detectarán de forma automática los incidentes de seguridad, utilizando elementos de monitorización de los servicios o de detección de anomalías y poniendo en marcha los procedimientos de respuesta al incidente en el menor plazo posible. Para los incidentes detectados por los usuarios, ya sean internos o externos, se establecerán los pertinentes canales de comunicación de incidentes.

En cuanto a la respuesta, se establecerán medidas que se gestionarán en tiempo oportuno y estarán orientadas a la restauración de la información y los servicios que pudieran haberse visto afectados por un incidente de seguridad. Para aquellos servicios que se consideren críticos, en base a la valoración que de los mismos realicen sus responsables, se deberán desarrollar planes que permitan la continuidad de dichos servicios en el caso de que, a raíz de un incidente de seguridad, quedaran indisponibles.

En cuanto a la conservación, el sistema de información garantizará la conservación de los datos e información en soporte electrónico una vez solventado el incidente de seguridad.

5. Alcance

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.

6. Organización de la seguridad de la información

La seguridad en la FGUCM está soportada sobre las estructuras y roles que se describen a continuación:

- Estructura de especificación, que es la que se encarga de establecer los requisitos de seguridad asociados a los servicios prestados.
- Estructura de supervisión, que es la que se encarga de verificar el cumplimiento de los requisitos de seguridad y el alineamiento continuo con los objetivos de la organización.
- Estructura de operación, que se encarga de implantar las medidas de seguridad identificadas.

6.1 Estructura de especificación

Esta estructura es la encargada de determinar los requisitos de seguridad que serán de aplicación a los servicios prestados por la FGUCM y a garantizar el cumplimiento normativo asociado que le es de aplicación, en concreto el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

Forman parte de esta estructura:

- Los Responsables de la Información y del Servicio.

6.1.1 Responsables de Información y Servicio

La figura de los Responsables de la Información y del Servicio establecerán el nivel de seguridad que la información y los servicios prestados por la FGUCM requieren, en base a sus exigencias en cuanto a

disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad considerando el impacto que tendría en la ciudadanía y en la propia Organización la falta de alguno de esos aspectos.

Los Responsables de la Información y del Servicio será nombrados por la Dirección General de la FGUCM.

6.2 Estructura de supervisión

La estructura de supervisión de la seguridad se encarga de verificar la correcta implantación y operación de los requisitos de seguridad que se hayan establecido, de cara a mantener la alineación con los objetivos y de cumplir con las normas y legislación aplicable.

En la supervisión global de todas las actividades relativas a la seguridad de la información se encuentra el Responsable de Seguridad de la Información.

Para la coordinación global e integral de la seguridad se encuentra el Comité de Seguridad de la Información.

Las funciones y responsabilidades de cada una de las figuras se describen en los siguientes apartados.

6.2.1 Responsable de Seguridad de la Información

Es responsable de la definición, coordinación, difusión y verificación de los requisitos de Seguridad de la información en la Organización.

Este Responsable forma parte del Comité de Seguridad, tomando el papel de Secretario del Comité y, por tanto, es el encargado de elevar a dicho Comité los asuntos de interés relacionados con la seguridad de la información.

Sus responsabilidades comprenden:

- Convocar las reuniones del Comité de Seguridad.
- Coordinar y controlar las medidas de Seguridad de la Información y de Protección de Datos de la Organización.
- Supervisar la implantación, mantener, controlar y verificar el cumplimiento de las normas y procedimientos establecidos.
- Conseguir que se elabore el presupuesto anual de seguridad TI de la Organización.
- Definir un modelo de gestión de la seguridad alineado con la estrategia de la Organización en materia de seguridad. A este modelo de gestión se le llamará SGSI (Sistema de Gestión de Seguridad de la Información), independientemente de que esté basado en las normas internacionales que recomiendan cómo hacerlo, o se trate de un modelo diferente.
- Supervisar la implantación práctica de la estrategia de Seguridad de la Información de la Organización.
- Supervisar las situaciones excepcionales (o incidentes) de ciberseguridad producidas en la Organización.
- Promover la realización de análisis de riesgos de seguridad de la información de forma periódica.
- Solicitar al Área de Recursos Humanos la realización de programas de formación y sensibilización en materia de seguridad de la información.
- Analizar los indicadores de seguridad para medir la eficacia y eficiencia de las medidas implantadas.
- Analizar los incidentes de seguridad de la información reflejados en los registros de estos y verificar que se han establecido los planes para su resolución.
- Mantener actualizada la documentación asociada a la gestión de la seguridad de la información: normativas, procedimientos y registros.
- Autorizar por escrito la ejecución de procedimientos de recuperación de datos en los casos en que se requiera.

- Colaborar con las Auditorías externas/internas en materia de seguridad de la información, revisarlas y encargar a los responsables de los sistemas la implantación de las correcciones que se deriven.

El Responsable de Seguridad de la Información será nombrado por la Dirección General de la FGUCM.

6.2.2 Comité de Seguridad de la Información

La misión del Comité de Seguridad de la Información es la coordinación general de las actividades que tienen relación con la seguridad integral.

Un objetivo fundamental del Comité de Seguridad de la Información es la puesta en común de aspectos importantes de la seguridad entre todos los responsables. Con ello se evitará que actividades referentes a la seguridad, que puedan afectar a varias o todas las áreas de la organización, queden sin el suficiente conocimiento por parte de sus responsables, o sin el suficiente apoyo o compromiso, perjudicando su eficacia.

Las funciones del Comité de Seguridad son:

- Informar regularmente del estado de la seguridad a la Dirección General de la FGUCM.
- Revisar regularmente la Política de Seguridad de la Información y proponer cambios, si procede.
- Revisar las normativas internas de seguridad que se puedan derivar de la Política de Seguridad de la Información y proponerlas para su aprobación.
- Elaborar y proponer los requisitos de formación para el personal clave que maneja información, sistemas e infraestructuras físicas.
- Proponer para su aprobación los planes de mejora de la seguridad que surjan a raíz de los análisis de riesgos realizados.
- Seguir el desarrollo de los planes de acción aprobados.
- Coordinar las actuaciones en materia de seguridad que se puedan estar realizando en diferentes áreas de la Organización con objeto de evitar esfuerzos duplicados o desalineados con la Política de Seguridad de la Información.
- Analizar incidentes de seguridad significativos. Decidir qué hacer a raíz de ellos. Algunos pueden conllevar una actuación con gasto, en cuyo caso se propondría para su aprobación.
- Analizar información de indicadores de seguridad que pudiera haber definidos. Tomar decisiones en caso de desviación respecto a los umbrales establecidos.
- Proponer soluciones de seguridad que deban tener un presupuesto aprobado.

Serán miembros fijos del Comité de Seguridad de la Información:

- Responsable de seguridad
- Responsable de sistemas
- Responsable de los servicios e información

Adicionalmente, podrán asistir al Comité de Seguridad de la Información los responsables de las materias específicas a tratar en las reuniones, que podrán ser invitados en función del contenido de la agenda.

6.3 Estructura de operación

La estructura de operación de la seguridad debe asumir la administración operativa de la seguridad de los sistemas de información, implantando en dichos sistemas las medidas necesarias para satisfacer los requisitos de seguridad establecidos por la estructura de especificación.

Se describen a continuación las funciones y responsabilidades de las figuras asociadas a la estructura de operación.

6.3.1 Responsable de Sistema de Información

Sus funciones y responsabilidades son:

- Definir, en coordinación con el Responsable de Seguridad de la Información, las especificaciones funcionales de seguridad de los Sistemas de Información de la Organización.
- Garantizar que en el diseño de sistemas de información y redes de comunicaciones se contemplen desde el principio los aspectos necesarios de seguridad de la información en cuanto a disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad.
- Revisar que la configuración de seguridad tras la instalación de un sistema nuevo es la adecuada.
- Revisar que la configuración de seguridad tras los cambios en un sistema sigue siendo la adecuada.
- Implantar y verificar el funcionamiento de las medidas de seguridad que resulten de los planes de tratamiento de riesgos o planes de acciones correctivas a raíz de las auditorías de seguridad de la información.
- Verificar el correcto funcionamiento de los indicadores de seguridad de la información.
- Realizar auditorías técnicas periódicas para verificar el funcionamiento de las medidas y cumplimiento de los requisitos de seguridad establecidos. Estas auditorías pueden ser llevadas a cabo por personal interno o externo a la FGUCM.

El Responsable de Sistema de Información será nombrado por la Dirección General de la FGUCM.

7. Funciones y obligaciones

Al margen de las funciones y atribuciones que atañen al personal que integra el esquema organizativo responsable de la seguridad, se establecen a continuación las obligaciones del personal de la FGUCM, así como de aquellos terceros que tengan acceso a sus sistemas de información.

7.1 Funciones y obligaciones del personal

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.

Todo este personal deberá asistir a sesiones de concienciación en materia de seguridad, las cuales se establecerán en el plan de formación y concienciación anual.

Las personas con responsabilidad en el uso, la gestión, mantenimiento o explotación de los servicios soportados en las 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.

7.2 Funciones y obligaciones de terceras partes

Las terceras partes que estén relacionadas con la gestión, mantenimiento o explotación de los servicios prestados por la FGUCM serán hechos partícipes de esta Política de Seguridad de la Información. Las

terceras partes quedarán obligadas al cumplimiento de esta Política y a las normativas que se puedan derivar de ella.

Las terceras partes podrán desarrollar sus propios procedimientos operativos para satisfacer la Política.

Se deberán establecer procedimientos específicos de comunicación de incidencias para que los terceros afectados puedan reportarlas.

El personal de las terceras partes deberá recibir sesiones de concienciación, tal como se exige para el personal propio.

Cuando algún aspecto de esta Política no pueda ser satisfecho por una tercera parte, el Responsable de Seguridad de Información deberá realizar un informe del riesgo en que se incurre. Ese riesgo deberá ser aceptado por el Comité de Seguridad de la Información.

7.3 Resolución de conflictos

En caso de conflicto entre los diferentes responsables de información o de servicio que componen la estructura organizativa de la Política de Seguridad de la Información, éste será resuelto por el superior jerárquico de los mismos con la mediación del Responsable de Seguridad de la Información, elevándose para su resolución al Comité de Seguridad de la Información en caso de no llegar a un acuerdo.

En la resolución de estas controversias se tendrán siempre en cuenta las exigencias derivadas de la protección de datos de carácter personal.

8. Formación y concienciación

Con carácter anual se realizará, al menos, una acción de formación y concienciación en materia de seguridad.

El objetivo de la acción formativa y de concienciación es doble:

- Mantener informado al personal más directamente relacionado con el manejo de información y los sistemas que la tratan sobre los procedimientos existentes de seguridad, riesgos, medidas de protección, planes de protección, etc.
- Concienciar al personal, en general, de la importancia de la seguridad y de los procedimientos básicos de manejo e intercambio de información.

El primer objetivo se asocia a Formación y el segundo a Concienciación.

Las áreas responsables determinarán el formato de la acción de Formación y Concienciación, así como sus contenidos.

9. Gestión de riesgos

Los servicios e infraestructuras bajo el alcance de la presente Política deberán estar sometidos a un análisis de riesgos para orientar las medidas de protección a minimizar los mismos.

Como metodología base para la realización de los análisis de riesgos se utilizará Magerit, siendo esta metodología la más recomendable para el sector público nacional.

Se utilizarán, como punto de partida, el catálogo de amenazas de seguridad previsto en la metodología.

El análisis se realizará:

- Regularmente, una vez al año.

- Cuando haya cambios significativos en la información manejada.
- Cuando haya cambios en los servicios esenciales prestados o cambios significativos en las infraestructuras que los soportan.
- Cuando ocurra un incidente de seguridad grave.
- Cuando se identifiquen amenazas severas que no hubieran sido tenidas en cuenta o vulnerabilidades graves que no estén contrarrestadas por las medidas de protección implantadas.

De acuerdo con la escala de riesgos de la metodología Magerit, el nivel de riesgo deberá situarse por debajo de nivel ALTO para considerarse de forma automática como aceptable (el riesgo residual máximo debe ser MEDIO). Valores de riesgo residual mayores a MEDIO deberán ser aceptados explícitamente por el Comité de Seguridad de la Información, previa justificación de la conveniencia de su aceptación.

Para los valores de riesgo residual que no sean aceptables se deberá elaborar el correspondiente Plan de Tratamiento que permita llevar los valores de riesgo a valores aceptables.

10. Datos de carácter personal

La FGUCM aplicará los principios incluidos en el RGPD cuando realice tratamientos datos de carácter personal:

- Principio de “licitud, transparencia y lealtad”: los datos deberán ser tratados de manera lícita, leal y transparente para el interesado.
- Principio de “limitación de la finalidad”: implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, que se prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines.
- Principio de “minimización de datos”: la FGUCM solo recogerá datos de carácter personal cuando sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
- Principio de “exactitud”: los datos deben ser exactos y, si fuera preciso, actualizados, debiendo adoptarse por parte de la FGUCM todas las medidas razonables para que se rectifiquen o supriman los datos inexactos en relación con los fines que se persiguen.
- Principio de “limitación del plazo de conservación”: solo pueden tratarse los datos adecuados, pertinentes y necesarios para una finalidad, la conservación de esos datos debe limitarse en el tiempo al logro de los fines que el tratamiento persigue. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados o, al menos, desprovistos de todo elemento que permita identificar a los interesados.
- Principio de “integridad y confidencialidad”: obligación de actuar proactivamente con el objetivo de proteger los datos que manejan frente a cualquier riesgo que amenace su seguridad.
- Principio de “responsabilidad proactiva”: implica aplicar por parte de la FGUCM las medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con el RGPD.

La FGUCM aplicará medidas de seguridad para garantizar el derecho fundamental a la protección de datos garantizando la confidencialidad, la integridad y la disponibilidad de los datos personales. Para garantizar estos tres factores de la seguridad la FGUCM aplicará las medidas de seguridad necesarias adecuadas al nivel de los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas conforme al artículo 32 del RGPD.

En relación con las medidas de seguridad en el ámbito del sector público, la FGUCM cumplirá con la disposición adicional primera de la LOPDGDD, que se señala que los responsables enumerados en el artículo 77.1 de la citada ley orgánica, entre los que se encuentran las fundaciones del sector público como la FGUCM , deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.

La FGUCM dispondrá de un Registro de Actividades del Tratamiento de datos de carácter personal que incluirá los contenidos regulados en el artículo 30 del RGPD y lo hará público en su portal de transparencia en aplicación del artículo 31.2 de la LOPDGDD.

11. Terceras partes

Cuando la FGUCM utilice servicios o maneje información de terceros, les hará partícipes de esta Política de Seguridad de la Información. El Comité de Seguridad de la Información establecerá canales para reporte y coordinación de los respectivos Comités de Seguridad y establecerá procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la FGUCM preste servicios a otros organismos o ceda información a terceros, les hará partícipe de esta Política de Seguridad de la Información y de las Instrucciones y Procedimientos que atañan 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 exigirá que el personal de terceros esté 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 de la Información 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.

12. 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 aborden aspectos específicos. A raíz de dichas políticas y normativas se podrán desarrollar procedimientos que describan la forma de llevarlas a cabo.

La documentación de políticas y normativas de seguridad, así como esta Política de Seguridad de la Información 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 aprobada 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 afectaran 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.

13. Compromiso de la Dirección General

La Dirección General de la FGUCM manifiesta su compromiso formal con el apoyo a los planes de seguridad que se deriven de la aplicación de esta Política. Dicho apoyo se concretará en:

- Proporcionar los recursos humanos y económicos necesarios, dentro de las posibilidades presupuestarias;
- Asignar roles y responsabilidades a las personas asociadas a los planes de seguridad;
- Apoyar la formación de los recursos humanos implicados en los planes de seguridad para que adquieran el nivel de concienciación y las competencias necesarias;
- Velar por el correcto funcionamiento del Sistema de Gestión de Seguridad de la Información;
- Facilitar las comunicaciones con otras organizaciones en materia de Seguridad de la Información;
- Promover la mejora continua en el ámbito de Seguridad de la Información.

El compromiso con el apoyo a los planes se manifiesta con la aprobación del presente documento.

14. Revisión y aprobación

La Política de Seguridad de la Información se revisará, al menos, cada dos años.

La presente Política de Seguridad de la Información fue aprobada por la Dirección General de la FGUCM en sesión celebrada el día 02 de noviembre de 2023.

Firma: _____

Fdo.: María Paz García Vera

Cargo: Directora General de FGUCM

15. Anexo I – Requisitos mínimos

Para la correcta implementación y cumplimiento de la presente Política de Seguridad es necesario aplicar una serie de requisitos de obligado cumplimiento:

15.1 La seguridad en la Organización

La seguridad debe comprometer a todos los miembros de la FGUCM, sin excepción.

En el artículo 6 (Descripción) del presente documento, se especifica la Organización de la seguridad con la definición de la estructura organizativa.

Asimismo, la implementación de dicha organización está en el marco normativo cubierto por el establecimiento de un sistema de Gestión de la Seguridad, basado en el ENS.

15.2 Análisis y Gestión de riesgos

Los servicios e infraestructuras bajo el alcance de la presente Política deberán estar sometidos a un análisis de riesgos para orientar las medidas de protección a minimizar los mismos.

La descripción de la metodología y evaluación del riesgo están desarrollados en “Metodología de análisis y gestión de riesgos”.

El análisis de riesgos se realizará igualmente cuando se vaya a iniciar o a modificar un tratamiento de datos de carácter personal, en línea a lo establecido en el Reglamento General de Protección de Datos. En estos casos se contemplarán en el alcance del análisis todos aquellos activos que intervengan en el tratamiento, considerando tanto activos relacionados con los sistemas de información, como humanos, locales o terceros.

A raíz de los resultados obtenidos en los mencionados análisis de riesgos se determinarán las medidas necesarias para proteger dichos datos.

15.3 Gestión de personal

En el punto 6.1 Caracterización del puesto de trabajo de la Normativa sobre los Recursos Humanos se detalla la obligatoriedad de conocimiento y concienciación en materia de seguridad según sus responsabilidades. Los recursos necesarios para la implementación del sistema de seguridad, así como aquellos que lleven a cabo su operación, mantenimiento, supervisión, o tenga relación con el sistema se establece en los planes estratégicos de la FGUCM, y son aprobados por el Comité de Dirección a propuesta del Comité de Seguridad de la Información.

La selección de personal se lleva a cabo, aplicando estos criterios por parte del Responsable de Formación y Selección del Área de Profesionales de la FGUCM.

Periódicamente se realizarán evaluaciones de desempeño y seguimiento del personal vía DPD.

15.4 Profesionalidad

En el punto 1 de la Normativa sobre los Recursos Humanos se detallan los objetivos de las acciones de formación y concienciación y en el 6.2 se detallan los deberes y obligaciones del personal.

Con periodicidad bianual se diseña un plan de formación específico en el que se tiene en cuenta las necesidades de profesionalización del sistema de seguridad.

15.5 Autorización y control de Acceso

El acceso a los sistemas de información estará restringido y limitado a aquellos usuarios o procesos que lo necesiten para el desarrollo de su actividad y estén previamente autorizados.

El acceso a la información seguirá el principio de “necesidad de conocer”, de forma que los privilegios otorgados a cada entidad sean los mínimos imprescindibles para el desarrollo de su actividad.

La identificación de los usuarios será tal que se pueda conocer en todo momento quién recibe derechos de accesos y quién ha realizado alguna actividad, por lo que los identificadores deberán ser personales, no compartidos, e intransferibles.

Los lugares con acceso restringido igualmente deben estar controlados y previamente autorizados por los responsables asignados.

15.6 Protección de las instalaciones

Los sistemas de información deberán estar ubicados en zonas protegidas, con acceso restringido, habilitado únicamente al personal autorizado. La protección de las instalaciones recae en la UCM.

15.7 Adquisición de productos

Para el proceso de adquisición de nuevos productos, sistemas o servicios se establecen protocolos de análisis de riesgos con proveedores y se mantienen actualizados los listados de proveedores habituales. Las adquisiciones deben ser autorizadas por los responsables del área implicada y el Área de Suministros a través de informes favorables del proveedor, en caso de requerirse.

15.8 Seguridad por Defecto

Los sistemas y aplicaciones se diseñarán y construirán bajo el principio de seguridad por defecto, de tal forma que:

- El sistema ofrecerá la funcionalidad mínima necesaria, y ninguna adicional. Cualquier función que no sea de interés o innecesaria será deshabilitada o no implementada.
- La operación y explotación de los sistemas estará limitada a aquellas personas o ubicaciones que se autoricen, quedando prohibidas para el resto.
- El uso del sistema ha de ser seguro, de tal forma que el uso inseguro requiera intención por parte del usuario.

La seguridad estará presente desde la concepción de un sistema o aplicación y permanecerá presente durante todo su ciclo de vida.

En la concepción de un nuevo sistema o aplicación, o modificación sustancial de un sistema o aplicación existentes, se contará siempre, y desde el inicio, con la participación del Responsable de Seguridad de la Información

15.9 Integridad y actualización del sistema

Se deberán seguir en todo momento las informaciones acerca de las vulnerabilidades que afectan a los sistemas de información.

Se seguirán las recomendaciones de los fabricantes de equipos y software en cuanto a actualizaciones de seguridad, que deberán ser analizadas en cuanto a su idoneidad y conveniencia, y aplicadas en caso positivo con la menor dilación.

15.10 Protección de la Información Almacenada y en Tránsito

Se deberán proteger los entornos que contienen información almacenada y en tránsito entre entornos inseguros. En este sentido se deberán proteger convenientemente los equipos portátiles que puedan contener información, así como los soportes extraíbles (lápices de memoria, discos duros extraíbles, etc.)

15.11 Prevención ante otros sistemas de información interconectados

Se desplegarán las protecciones necesarias para proteger el perímetro de la red corporativa de FGUCM, de forma que se neutralicen las posibles intrusiones procedentes del exterior, ya sea iniciadas malintencionadamente por terceros o como consecuencia de la interconexión con sistemas de terceros.

15.12 Registro de Actividad

Los sistemas y aplicaciones generarán los registros de actividad necesarios para conocer la actividad en los sistemas, de forma que se pueda determinar en todo momento qué persona actúa, sobre qué datos, con qué operaciones y sus privilegios de acceso.

15.13 Gestión de Incidentes de Seguridad

FGUCM definirá e implantará procedimientos de gestión de incidentes de seguridad que aseguren la correcta gestión y respuesta efectiva que permita anular o minimizar el impacto del incidente en la información, los servicios, los empleados, los usuarios y, en general, en la actividad de FGUCM.

El procedimiento de gestión y respuesta a incidentes de seguridad contemplará la comunicación y notificación de los incidentes a los organismos receptores de dicha información, de acuerdo con la legalidad vigente.

15.14 Continuidad de Negocio

Para asegurar la disponibilidad de los servicios y sistemas de información, FGUCM diseñará e implantará Planes de Continuidad de Servicio que eviten las interrupciones de las actividades de la FGUCM y garanticen, ante una contingencia, la reanudación de los servicios y sistemas de información a los niveles adecuados de operatividad.

15.15 Gestión de la Seguridad y Mejora Continua

Se deberá establecer un Sistema de Gestión de la Seguridad que permita conocer en cada momento el estado de la seguridad, mediante la definición y medida de indicadores, y permita tomas las decisiones informadas pertinentes para cumplir los requisitos de seguridad establecidos.

Se establecerá un proceso de mejora continua mediante el análisis de la situación, la implantación de nuevas medidas de seguridad, la mejora de las existentes y la aportación de mejoras sugeridas por el Comité de Seguridad de la Información y por toda la FGUCM en su conjunto.