

SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Seguridad de las Tecnologías de Información y Comunicaciones
Normativa de Gestión de incidentes
Noviembre 2023



Código Seguro De Verificación	N0DsqrTNeNawC0hb00nmw==	Estado	Fecha y hora	
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 14:37:57	
Observaciones		Página	1/11	
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/N0DsqrTNeNawC0hb00nmw%3D%3D			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).			

SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Babel Group	DPD y Responsable de Seguridad	Comité de Seguridad de la Información
firma:	firma:	firma:

HISTORIAL DE CAMBIOS

NOMBRE DEL FICHERO	VERSIÓN	RESUMEN DE CAMBIOS PRODUCIDOS	FECHA
FGUCM STIC-NOR - Normativa de Gestión de incidentes v1.0.docx	1.0	Primera edición del documento	11/04/2023

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

Código Seguro De Verificación	NODsqURTNeNawC0hb00nmw==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 14:37:57
Observaciones		Página	2/11
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/NODsqURTNeNawC0hb00nmw%3D%3D		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		



SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
REFERENCIAS

DOCUMENTOS INTERNOS	
Título	Nombre del fichero
Política de Seguridad de la Información	FGUCM STIC-POL - Política de Seguridad de la Información v1.0.docx
DOCUMENTOS EXTERNOS	
[1] CCN-STIC-804 ENS. Guía de implantación	
[2] CCN-STIC-805 ENS-Política de Seguridad de la Información	
[3] CCN-STIC-821 Normas de Seguridad en el ENS y sus Anexos	
[4] CCN-STIC-883 Implantación del ENS para Entidades Locales	
[5] CCN-STIC-815 Esquema Nacional de Seguridad. Métricas e Indicadores	
[6] CCN-STIC-403 Gestión de incidentes de seguridad informáticos	
[7] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad	
[8] 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)	
[9] Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales	
[10] Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía	

CUMPLIMIENTO	
ENS	RGPD
op.exp.7 Gestión de incidentes	Artículo 12 - Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado
op.exp.9 Registro de la gestión de incidentes	Artículo 31 - Cooperación con la autoridad de control
	Artículo 33 - Notificación de una violación de la seguridad de los datos personales a la autoridad de control
	Artículo 34 - Comunicación de una violación de la seguridad de los datos personales al interesado
	Artículo 36 - Consulta previa

Código Seguro De Verificación	NODsqURTNeawC0hb00nmw==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 14:37:57
Observaciones		Página	3/11
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/NODsqURTNeawC0hb00nmw%3D%3D		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		



SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

	Artículo 51 Autoridad de control
	Artículo 82 Derecho a indemnización y responsabilidad
	Artículo 83 Condiciones generales para la imposición de multas administrativas

Código Seguro De Verificación	NODsqURTNeNawC0hb00nmw==	Estado	Fecha y hora	
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 14:37:57	
Observaciones		Página	4/11	
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/NODsqURTNeNawC0hb00nmw%3D%3D			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).			

SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES**Contenido**

1. OBJETO	6
2. ALCANCE	6
3. INTRODUCCIÓN	6
4. DESTINATARIOS	6
5. RESPONSABILIDADES	6
6. NORMATIVA DE GESTIÓN DE INCIDENTES	7
6.1 CICLO DE VIDA DE LA GESTIÓN DE INCIDENTES	7
6.1.1 Fase 1: Comunicación y detección de incidentes de seguridad	7
6.1.2 Fase 2: Identificación y registro de la incidencia	8
6.1.3 Fase 3: Análisis de la incidencia	8
6.1.4 Fase 4: Respuesta a la incidencia	8
6.1.5 Fase 5: Seguimiento y cierre de la incidencia	9
6.1.6 Fase 6: Mejora continua de la seguridad	10
7. PROCESO DISCIPLINARIO	10
8. REVISIÓN Y EVALUACIÓN	10
9. APROBACIÓN	11

Código Seguro De Verificación	NODsqURTNeNawC0hb00nmw==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 14:37:57
Observaciones		Página	5/11
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/NODsqURTNeNawC0hb00nmw%3D%3D		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		



SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES**1. Objeto**

- Asegurar que los incidentes y debilidades detectadas en los sistemas de información son gestionados y comunicados adecuadamente, de forma que se puedan tomar a tiempo las acciones correctivas adecuadas, evitando así, posibles daños.
- Generar nuevo conocimiento para la mejora proactiva de la seguridad, ya que la FUNDACIÓN GENERAL DE LA UNIVERSIDAD COMPLUTENSE DE MADRID (en adelante, FGUCM) debe aprender de todos y cada uno de los incidentes que se hayan producido en ella para mejorar los mecanismos de protección y, con ello, prevenirlos en el futuro.

2. Alcance

Tiene consideración de "incidencia" todo evento que no forma parte de la operación estándar de un servicio y la infraestructura tecnológica que lo soporta, de los presentes en la FGUCM dentro del ámbito del Esquema Nacional de Seguridad (ENS).

3. Introducción

El objetivo de la gestión de incidencias es el de recuperar o corregir los fallos del sistema ante cualquier alteración o evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad de este.

La gestión de incidencias va más lejos de la resolución en si misma de los problemas a los que se enfrentan los sistemas, siendo una palanca de mejora de la productividad, control de procesos y optimización de recursos disponibles.

4. Destinatarios

Todo el personal que, de manera permanente o eventual, realice actividades para la FGUCM, incluyendo el personal de proveedores externos cuando realicen actividades para la FGUCM.

5. Responsabilidades

Todo el personal que, de manera permanente o eventual, realice actividades para la FGUCM, incluyendo el personal de proveedores externos cuando realicen estas actividades para la FGUCM tienen la responsabilidad individual de cumplir con esta normativa.

Los responsables de dicho personal deben ser diligentes en el cumplimiento de esta normativa por parte de éstos.

Además, estos responsables y el personal de la FGUCM tienen la obligación en caso de incumplimiento por parte de cualquier persona que, de manera permanente o eventual, preste servicio en la FGUCM de comunicarle su incumplimiento y en caso de persistencia de éste o de gravedad del incumplimiento elevar esta situación al Responsable de Seguridad y a Recursos Humanos para que inicien las acciones pertinentes.

Los roles participantes o involucrados en esta normativa son los siguientes:

- ComSeg: Comité de Seguridad de la Información de la FGUCM.

Código Seguro De Verificación	NODsqURTNeNawC0hb00nmw==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 14:37:57
Observaciones		Página	6/11
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/NODsqURTNeNawC0hb00nmw%3D%3D		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		



SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

- DepExp: Departamento de Explotación de la FGUCM.
- DepSis: Departamento de Sistemas de la FGUCM.
- RSIS: Persona Responsable de Sistemas de la FGUCM.
- RSEG: Persona Responsable de Seguridad TIC de la FGUCM.
- RFIS: Responsable de la seguridad física.
- RIS/RT: Persona Responsable de la Información y Servicio y/o Responsable del Tratamiento de Datos Personales de la FGUCM.
- ET: Personas Encargadas de Tratamiento pertenecientes a EExt.
- EExt: Entidad Externa colaboradora de la FGUCM.

Las responsabilidades concretas de cada rol se describen en el siguiente apartado que describe las fases o ciclo de vida de gestión de incidencias de seguridad de la información.

6. Normativa de Gestión de incidentes

Todos los incidentes y vulnerabilidades de seguridad detectados por los usuarios deben ser comunicados lo más rápidamente posible y por los canales adecuados. Se establecerá por tanto en los contratos con terceros la obligación y los medios para la comunicación y gestión de las incidencias de seguridad.

Adicionalmente a los incidentes y vulnerabilidades que el personal pueda detectar de forma manual, deberán establecerse, siempre que sea posible, los mecanismos y herramientas para su detección automática o ayudar en su detección manual, especialmente en entornos de sistemas críticos. El objetivo de estas herramientas será la detección temprana de incidentes de seguridad mediante la recolección y análisis de todos los eventos que ocurren en los sistemas.

El *Procedimiento de comunicación, gestión y respuesta ante incidentes* se encuentra disponible para todo el personal y se encuentra alineado con la normativa vigente de protección de datos (artículos 33 y 34 del RGPD).

6.1 Ciclo de vida de la gestión de incidentes

6.1.1 Fase 1: Comunicación y detección de incidentes de seguridad

La detección y comunicación de comportamientos anómalos en la infraestructura de la FGUCM es fundamental a la hora de su protección ya que, cuanto más se demoren, mayor puede ser su impacto en su funcionamiento.

El mecanismo de detección puede ser manual, notificado directamente por una persona (interna o externa a la FGUCM), para lo cual la FGUCM establecerá los canales adecuados (correo electrónico, telefónico, herramientas de ticket u otros) para esta comunicación.

Además, la FGUCM establecerá los mecanismos y herramientas automáticas necesarias para esta detección como pueden ser sistemas de detección de intrusiones, sistemas de gestión de eventos u otros similares.

Otra fuente de comunicación y detección pueden ser entidades externas como CCNert, fabricantes y proveedores desde el punto de vista tecnológico, o bien la Agencia Española de Protección de Datos (AEPD), si se trata de incidencias sobre tratamientos o datos de carácter personal, o incluso las Fuerzas y Cuerpos de Seguridad del Estado (FCSE) en el caso de fraudes u otras actividades delictivas que puedan impactar en la FGUCM.

Código Seguro De Verificación	NODsqURTNeNawC0hb00nmw==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 14:37:57
Observaciones		Página	7/11
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/NODsqURTNeNawC0hb00nmw%3D%3D		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		



SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES**6.1.2 Fase 2: Identificación y registro de la incidencia**

La identificación de incidencia y su clasificación consiste en evaluar inicialmente la información proporcionada por las fuentes de comunicación y detección (Fase 1) para confirmar su existencia y abordar un primer análisis que permita tener una aproximación inicial sobre la naturaleza y amplitud de la incidencia y, ampliar y mejorar la información para las fases siguientes; para ello, se definirá un árbol de clasificación y definición de criticidad de la incidencia siguiendo las guías del CCN.

En el caso de que en la Fase 1 no se produjera el registro de la incidencia mediante la herramienta definida por la FGUCM para tal fin, se procederá a su registro por parte del departamento receptor de la incidencia (DepExp o DepSis) y completar la información recibida con la obtenida de esta Fase 2.

De este análisis previo se procederá a la notificación interna de la incidencia y su evaluación previa de las partes interesadas dentro de la FGUCM (RSEG, RSIS, DPD, RFIS, RSI/RT, ComSeg), que determinarán las actuaciones que se deberán acometer, incluida la notificación de la incidencia fuera de la FGUCM (CCNCert, AEPD, y otros posibles interesados), o bien se deberá avanzar en el análisis y resolución de la incidencia previamente a esta notificación exterior. Deberá atenderse al cumplimiento legal y contractual de los plazos de notificación aplicables.

6.1.3 Fase 3: Análisis de la incidencia

El objetivo de esta fase es obtener la información suficiente para responder a la incidencia. Se deberán recopilar las evidencias apoyadas por mecanismos de integridad que incluyan marca horaria (timestamp) de fuente fiable.

Se deberá guardar una descripción detallada de cada evidencia recopilada incluyendo datos de identificación de personas que han recopilado la prueba, fecha y hora de obtención, lugar de almacenamiento de la evidencia. El objetivo es la recopilación de evidencias con validez legal para el caso de que se inicien acciones legales respecto a la incidencia. Para ello se deberán formalizar las acciones pertinentes.

Deberá evitarse la manipulación directa de los soportes de información y de los sistemas, trabajando, siempre que sea posible, sobre copias de las evidencias para evitar la pérdida irreversible de los datos originales.

Se deberá documentar y registrar en el ticket de la incidencia todas las acciones que se realicen sobre los sistemas (fotografía, impresa, video, copia de pantallas, entre otras).

Se asignarán por parte del RIS/RT o ComSeg los recursos para investigar las causas y consecuencias del incidente, estudiar en detalle todas las evidencias recogidas, y, tras su análisis, establecer las actuaciones (Plan de actuación) que permitirán abordar su resolución y la recuperación de los sistemas al estado anterior a la materialización del incidente.

En su caso puede ser necesaria la participación de EExt, como pueden ser fabricantes, proveedores para que colaboren en el análisis de la incidencia y preparación del Plan de actuación.

También podrá requerirse, en el caso de incidentes graves, de la participación de CCNCert, AEPD, FCSE o judicial.

Estas decisiones deberán tomarse por parte del RSI/RT y del ComSeg, con el soporte de RSEG, RSIS, RFIS, DPD.

Como resultado de esta fase se obtendrá el Plan de Actuación que se desarrollará en las fases siguientes.

6.1.4 Fase 4: Respuesta a la incidencia

En esta fase se pondrá en marcha el Plan de actuación obtenido de la fase anterior. Este Plan de actuación puede contemplar la invocación del Plan de Contingencia de la FGUCM.

Esta respuesta a la incidencia se puede dividir en dos fases diferenciadas, la contención y la resolución.

Código Seguro De Verificación	NODsqURTNeawC0hb00nmw==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 14:37:57
Observaciones		Página	8/11
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/NODsqURTNeawC0hb00nmw%3D%3D		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		



SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES**6.1.4.1 Contención**

Este Plan de actuación se iniciará con las actividades de contención cuya principal finalidad es limitar, en la medida de lo posible, la extensión de la incidencia.

La FGUCM deberá disponer de procedimientos de contención específicos para los diversos tipos de incidencia (denegación de servicio, código malicioso, acceso no autorizado, extracción de datos, etc.).

Para los casos no contemplados, se evaluará la conveniencia de tomar medidas urgentes que pueden incluir la desconexión. Completa de servicios, el aislamiento del sistema afectado, la recogida de evidencias, la protección de registros o en referencia al acceso a determinados recursos, instalaciones o servicios de la FGUCM, pudiendo desconectar, deshabilitar o impedir el acceso.

En estas actuaciones deberán participar los RSI/RT asesorados por el RSEG, RSIS, RFIS y DPD, si es necesaria con la aprobación de ComSeg si las acciones afectan a la FGUCM en su conjunto de forma importante.

Durante esta fase, si fuese necesario, se realizará la recopilación y preservación de evidencias de la infraestructura física y tecnológica tales como fotos, videos, copias de discos, trazar de registros (logs), y otros que se consideren oportunos.

También se documentará cualquier tipo de medida de contención aplicada de manera que ésta pueda desactivarse tan pronto deje de ser necesaria.

6.1.4.2 Resolución

El objetivo de esta subfase es el restablecimiento de la información, servicios y recursos afectados por la incidencia. Se realizarán las actividades para que se restablezca la operatividad efectiva de la FGUCM.

El DepExp o el DepSis o ambos, dependiendo del ámbito de la incidencia (puestos de trabajo, CPD, servidores departamentales o comunicaciones), serán los encargados de atender en primera instancia las incidencias que le sean comunicadas y resolverlas.

El liderazgo de las actuaciones la deberá realizar el RIS/RT del sistema afectado. En el caso de que la incidencia afectase a la FGUCM en su totalidad o una parte importante de él, será el ComSeg quien lidere las actuaciones.

Se contará con el RSEG, RSIS, RFIS y el DPD dependiendo de la naturaleza y ámbito de la incidencia que se trate.

Dependiendo del impacto, tipo de incidencia y ámbito de la FGUCM afectado se aplicarán los Planes de Emergencia, Contingencia y de Recuperación disponibles en la FGUCM.

En el caso que se estime necesario, o bien sea obligatorio, se comunicará con AndalucíaCERT, CCNCert, AEPD, CTPD o las FCSE o judiciales con el fin no sólo informativo, sino también para solicitar su colaboración activa.

6.1.5 Fase 5: Seguimiento y cierre de la incidencia

Una vez resuelto el incidente y recuperada la operatividad de la FGUCM bajo el criterio del RIS/RT o del ComSeg, si es el caso, y con el asesoramiento del RSEG, RSIS, RFIS y DPD, los elementos de la infraestructura física y tecnológica recuperados se someterán a una monitorización intensiva para identificar posibles problemas no contemplados o bien se pudieran reproducir.

La resolución de la incidencia se considerará completada cuando el o los elementos de la infraestructura física y tecnológica estén recuperados y en funcionamiento, y se consiga un conocimiento completo o razonable de qué ha pasado, por qué, las pérdidas y consecuencias ocasionadas, y qué o quiénes han sido los causantes.

Por tanto, será el RIS/RT o el ComSeg quien dará por cerrada la incidencia cuando la Fase 4 esté completamente realizada. Para ello deberá asegurarse que:

Código Seguro De Verificación	NODsqURTNeawC0hb00nmw==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 14:37:57
Observaciones		Página	9/11
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/NODsqURTNeawC0hb00nmw%3D%3D		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		



SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

- Las medidas correctoras adoptadas han sido las adecuadas para la resolución de la incidencia y se ha minimizado la posibilidad de que se produzca otra incidencia de similares características.
- Las actividades de notificación interna y externa pertinente han concluido.
- El informe de la incidencia, responsabilidad del RSEG, está presentado, comunicado y aprobado por el RIS/RT o ComSeg.

Cuando finalice la gestión de un incidente se dará a conocer su cierre de forma retroactiva a todos los participantes en su gestión, en sus distintos niveles de escalado y hasta al origen de la comunicación, así como a las personas afectadas por ella. Solo cuando se estime oportuno, se comunicará también el resultado y acciones llevadas a cabo.

En caso de incidentes que pudieran conllevar la obligatoriedad de comunicar con autoridades de control pertinentes se realizarán las comunicaciones oportunas, y en aquellos que traten datos de carácter personal se seguirá lo estipulado en la legislación vigente de protección de datos comunicando en un plazo no superior a 72h con el CTPD.

6.1.6 Fase 6: Mejora continua de la seguridad

El objetivo de esta fase es impulsar la seguridad de la FGUCM en base a las experiencias y lecciones aprendidas a partir de las incidencias que se produzcan.

Se establecerán los indicadores necesarios para conocer y medir el volumen, tipo, origen, destino y coste de los incidentes de seguridad, de forma que ayude en la toma de decisiones y a efectos de mejorar o agregar controles para limitar la frecuencia, daño y costes.

Las acciones de mejora deberán contemplar dos ámbitos de aplicación:

- Mejora de la seguridad de la infraestructura física y tecnológica de la FGUCM.
- Mejora de la seguridad en la atención a las personas integrantes de la FGUCM y de personas externas que utilizan los servicios de la FGUCM.

El RSEG con la colaboración del RSIS, RFIS y DPD analizará los indicadores, evidencias y registros generados en la gestión, análisis y resolución de la incidencia para preparar un "Informe de medidas recomendadas" y un "Plan de implantación de medidas" que será aprobado por el ComSeg, siendo el RSEG el encargado de su ejecución y el ComSeg de su seguimiento y validación.

7. Proceso disciplinario

Las infracciones por el incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado se clasificarán de acuerdo con lo previsto en la legislación aplicable.

En el supuesto de que un usuario no observe alguno de los preceptos señalados en la presente normativa, sin perjuicio de las acciones disciplinarias y administrativas que procedan y, en su caso, las responsabilidades legales correspondientes, se podrá acordar la suspensión temporal o definitiva del uso de los recursos informáticos asignados a tal usuario.

8. Revisión y evaluación

La gestión interna de esta normativa corresponde al Comité de Seguridad de la Información, que es competente para:

- Interpretar las dudas que puedan surgir en su aplicación.

Código Seguro De Verificación	NODsqURTNeNawC0hb00nmw==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 14:37:57
Observaciones		Página	10/11
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/NODsqURTNeNawC0hb00nmw%3D%3D		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		



SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

- Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ellos.
- Verificar su efectividad.

Anualmente, o siempre que existan circunstancias que así lo aconsejen, el Comité de Seguridad de la Información revisará la presente normativa, que se someterán, si hubiera modificaciones, a su aprobación.

La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.

Será el Comité de Seguridad de la Información el encargado de la custodia y divulgación de la versión aprobada de este documento.

9. Aprobación

La presente normativa ha sido aprobada por el Comité de Seguridad de la Información estableciéndose así las directrices generales para el uso adecuado de los recursos de tratamiento de la información que la FGUCM pone a disposición de sus usuarios para el ejercicio de sus funciones.

La FGUCM asume así las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en sus epígrafes.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte del Comité de Seguridad de la Información.

Firma: 

La persona Secretaria del Comité de Seguridad de la Información

Código Seguro De Verificación	NODsqURTNeawC0hb00nmw==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 14:37:57
Observaciones		Página	11/11
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/NODsqURTNeawC0hb00nmw%3D%3D		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

