

SEGURIDAD DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Seguridad de las Tecnologías de Información y Comunicaciones
Procedimiento de comunicación, gestión y respuesta
ante incidentes
Noviembre 2023



Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	1/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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- PROC - Procedimiento de comunicación, gestión y respuesta ante incidentes v1.0.docx	1.0	Primera edición del documento	12/04/2023

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	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	2/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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
Normativa de gestión de activos	FGUCM STIC-NOR - Normativa de Gestión de Activos v1.0.docx
Normativa de Gestión de Soportes	FGUCM STIC-NOR - Normativa de Gestión de Soportes v1.0. docx
Normativa de Gestión de incidentes	FGUCM STIC-NOR - Normativa de Gestión de incidentes v1.0. docx
Normativa de Gestión de autorizaciones	FGUCM STIC-NOR - Normativa de Gestión de autorizaciones 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-822 Procedimientos de Seguridad y sus Anexos	
[4] CCN-STIC-883 Implantación del ENS para Entidades Locales	
[5] CCN-STIC-817 Gestión de Ciberincidentes	
[6] CCN-STIC-403 Gestión Incidentes de Seguridad	
[7] GUÍA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES	
[8] ISO/IEC 27035-1:2016 ISO/IEC 27035-2:2016 «Information technology — Security techniques — Information security incident management»	
[9] RFC 3227 «Guidelines for Evidence Collection and Archiving» o Directrices para la recopilación de evidencias y su almacenamiento	
[10] Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad	
[11] 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)	
[12] Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales	

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	3/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

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
	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	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	4/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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	7
2. ALCANCE	7
3. INTRODUCCIÓN	7
4. DESTINATARIOS	8
5. RESPONSABILIDADES	8
6. PROCEDIMIENTO DE COMUNICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENTES	8
6.1 CONCEPTOS	8
6.2 MINIMIZACIÓN DEL NÚMERO DE INCIDENCIAS Y SU GRAVEDAD	9
6.3 CATEGORÍA DE LAS INCIDENCIAS	9
6.4 PRIORIDAD DEL TRATAMIENTO	10
6.5 GRUPOS DE COMUNICACIÓN DE INCIDENCIAS	10
6.6 PROCEDIMIENTO DE COMUNICACIÓN Y GESTIÓN DE INCIDENCIAS	10
6.6.1 Fase 1: Comunicación y detección de incidencias de seguridad	10
6.6.2 Fase 2: Identificación y registro de la incidencia	11
6.6.3 Fase 3: Análisis de la incidencia	11
6.6.4 Fase 4: Respuesta a la incidencia	12
6.6.4.1 CONTENCIÓN DEL INCIDENTE.	12
6.6.4.2 Resolución	13
6.6.5 Fase 5: Seguimiento y cierre de la incidencia	13
6.6.6 Fase 6: Mejora continua de la seguridad	14
6.7 ACCIONES ESPECIALES	14
7. PROCESO DISCIPLINARIO	17
8. REVISIÓN Y EVALUACIÓN	17
9. APROBACIÓN	18
10. ANEXO I - RECOLECCIÓN DE EVIDENCIAS	19
10.1 DEFINICIONES	19
10.2 DESARROLLO	19
10.2.1 Obtención de las autorizaciones necesarias	19
10.2.2 Principios durante la recolección de evidencias	19
10.2.3 Pasos para tener en cuenta y documentar cada paso	19
10.2.4 Principios durante la recolección de evidencias	20
10.2.5 Cadena de custodia – Procedimiento de almacenamiento	20
11. ANEXO II - CLASIFICACIÓN DE LAS INCIDENCIAS	21
12. ANEXO III - CRITICIDAD DE LOS INCIDENTES	23
13. ANEXO IV - BRECHAS DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL	26
13.1 NOTIFICACIÓN A LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS	26
13.1.1 Descriptivo de notificación a la AEPD	27
13.1.2 Canal de Notificación a la AEPD	28
13.2 NOTIFICACIÓN A LOS AFECTADOS	29
13.2.1 Modelo de notificación a los afectados	30
14. ANEXO V – NOTIFICACIONES	31
14.1 EVALUACIÓN DEL DEBER DE NOTIFICAR AL CCN-CERT	31
14.2 EVALUACIÓN DEL DEBER DE NOTIFICAR A LA AUTORIDAD DE CONTROL EN MATERIA DE PROTECCIÓN DE DATOS	31
14.3 EVALUACIÓN DEL DEBER DE NOTIFICAR A LAS PERSONAS INTERESADAS	32

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	5/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

14.4	EVALUACIÓN DEL INCIDENTE COMO DELITO	32
14.5	NOTIFICAR AL CCN-CERT	32
14.6	NOTIFICAR A LA AUTORIDAD DE CONTROL EN MATERIA DE PROTECCIÓN DE DATOS	32
14.7	NOTIFICAR A LAS PERSONAS INTERESADAS	32
14.8	DENUCIAR DELITO	33

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	6/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

Establecer los flujos de comunicación, y los pasos para contener, tratar y reparar las incidencias de Seguridad de los Sistemas de Información de la FUNDACIÓN GENERAL DE LA UNIVERSIDAD COMPLUTENSE DE MADRID (en adelante, FGUCM) en el ámbito del Esquema Nacional de Seguridad (ENS).

2. Alcance

La gestión de incidencias es aplicable a cualquier elemento de la infraestructura, servicios o actividades de la FGUCM, en concreto los activos y recursos:

- Hardware, Software, equipos y software de comunicaciones, software de sistemas, aplicaciones de sistemas
- Toda la información gestionada por la FGUCM.

El presente procedimiento de gestión de incidentes se lleva a cabo en los entornos de Preproducción y Producción. En el entorno de desarrollo, son los propios grupos de trabajo en dicho entorno quienes los lleven a cabo directamente, según convenga en cada situación, para lo cual, se les asignan los permisos suficientes.

3. Introducción

Este procedimiento describe el tratamiento de los sucesos que tienen la consideración de incidentes de seguridad en los sistemas de información del Instituto. A través de su aplicación práctica, se trata de lograr una capacidad de respuesta ante incidentes de seguridad de la información, definiendo protocolos de actuación e identificando responsabilidades, recursos humanos y materiales para resolver en el menor tiempo posible y del modo más efectivo un incidente.

La finalidad última de este tratamiento es doble. Por un lado, lograr una reacción efectiva ante el incidente para la salvaguarda de los activos y, por otro, generar nuevo conocimiento para la mejora proactiva de la seguridad, ya que el Instituto 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.

La FGUCM instruye al personal de la organización para que reporten, no sólo incidentes funcionales u operativos, sino incidentes de seguridad que les puedan estar afectando directamente, o de los que tengan conocimiento de cualquier forma posible.

Siempre que el personal de la organización detecte una posible incidencia de seguridad, debe comunicarlo lo antes posible.

La FGUCM pone a disposición de los empleados varios puntos de contacto y atención, siendo el principal la herramienta de tickets, y distintas vías de comunicación y herramientas, debiéndose usar en cada caso el medio más adecuado, según la naturaleza y urgencia del hecho a comunicar.

Los datos de los mencionados puntos de contacto son distribuidos a todos los implicados cada vez que sufran alguna modificación. Igualmente, son publicados física y electrónicamente en lugares de acceso común para los usuarios.

Se mantiene mediante la herramienta de tickets de la que se disponga un “Registros de Incidencias” gestionado por el Departamento de Sistemas y que el Responsable de Seguridad verifica, y que está disponible para auditorías externas relativas a la legislación en protección de datos vigente, así como a su normativa de desarrollo. Este registro almacena todas las resoluciones efectuadas a las incidencias

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	7/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

ocurridas, de forma que puedan ser consultados posteriormente para facilitar y agilizar la resolución de futuras incidencias similares.

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

Los roles participantes o involucrados en este procedimiento son los siguientes:

- ComSeg: Comité de Seguridad interior y seguridad TIC de la FGUCM.
- PUIECA: Agrupa a todas las personas usuarias (internas/externas) que realizan sus actividades dentro de la FGUCM.
- PUEX: Agrupa a todas las personas usuarias que no pertenecen a la FGUCM y utilizan sus servicios. Pueden ser personas ciudadanas o bien personas que pertenecen a otras entidades tanto públicas como privadas que utilizan los servicios de la FGUCM.
- 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 de la Información de la FGUCM.
- RIS/RTDDPP: 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. Procedimiento de comunicación, gestión y respuesta ante incidentes

6.1 Conceptos

Evento: cualquier ocurrencia instantánea, no perteneciente a las operaciones estándares, que pueden afectar (cambiar) al estado global en la seguridad de un sistema. Puede ser persistente o temporal.

Incidencia: Cualquier evento o conjunto de eventos que afecta o puede afectar al correcto funcionamiento, rendimiento o seguridad (confidencialidad, integridad y disponibilidad) de un sistema y que hace necesario llevar a cabo alguna acción determinada.

Incidente: Incidencia o conjunto de incidencias que causan un impacto real sobre la seguridad del sistema.

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	8/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

A efectos del presente procedimiento se considerarán igualmente incidentes e incidencias, y se referirá siempre como incidencias.

6.2 Minimización del número de incidencias y su gravedad

La mejor manera de gestionar las incidencias de seguridad es evitarlas, aunque esto no siempre es posible. Las acciones que, en general, se deben llevar a cabo para minimizar el número de incidencias y su repercusión sobre los activos de la organización, están recogidas en las políticas, normas y procedimientos de seguridad.

Cabe destacar las siguientes:

- Poner en práctica todas las políticas, normativas y procedimientos de la organización.
- Evaluar de forma regular las vulnerabilidades de los sistemas y servicios. Las evaluaciones deben ser realizadas por personal experto en seguridad.
- Comprobar con regularidad todos los sistemas y servicios para garantizar que tienen instalados los parches de seguridad más recientes.
- Establecer programas de capacitación sobre la seguridad, tanto para el personal de TI como para los usuarios finales (concienciación).
- Elaborar notificaciones o trípticos de seguridad que recuerden a los usuarios sus responsabilidades y restricciones.
- Poner en práctica una política de contraseñas seguras.
- Instalar herramientas automáticas para analizar con regularidad el tráfico de red y el rendimiento de los sistemas, y supervisarlos.
- Comprobar periódicamente todos los registros de eventos del sistema operativo, de aplicaciones, servicios, Cortafuegos, etc.
- Llevar a cabo revisiones de los procedimientos de copia de seguridad y restauración.
- Categorizar y documentar las acciones emprendidas a raíz de los incidentes de seguridad, para poder realizar revisiones y consultas posteriores. Estos pueden ayudar a resolver nuevos incidentes futuros similares y a implementar las medidas de seguridad más adecuadas.
- Realizar auditorías y pruebas de penetración periódicamente.
- Estar al día sobre las nuevas vulnerabilidades y estrategias de ataque empleadas por los atacantes.
- Investigar acerca de nuevas revisiones de software.

6.3 Categoría de las incidencias

Establecer la categorización de todas las incidencias de seguridad que ocurren ayuda a asignarles la prioridad con la que deben ser tratadas y hace posible el establecimiento de indicadores (cuadro de mando) que muestre posteriormente el estado del tratamiento de éstas y los puntos necesarios a reforzar.

A continuación, se exponen los principales grupos de incidencias de seguridad que se pueden producir. Se pueden categorizar, según distintos conceptos:

- Por su origen: Interno | Externo; Humano | Físico | Lógico.
- Por alcance: Intento de ataque | Ataque consumado | No intencionado (error).
- Provoca pérdida de: Confidencialidad | Integridad | Disponibilidad | Imagen
- Vulneración legal: RGPD | LOPDgdd | Otros

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora	
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20	
Observaciones		Página	9/34	
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

Una incidencia podrá pertenecer a uno o varios, de los anteriores grupos y categorías.

6.4 Prioridad del tratamiento

La prioridad del tratamiento y resolución de la incidencia indica el orden de ejecución en el tiempo (o con respecto a otras tareas a realizar en el sistema) según el impacto sobre los sistemas de no ser llevado a cabo en tiempo y forma.

- Alta: Tienen un gran impacto. Son incidencias que afectan a aspectos tales como pérdida total del servicio, problemas de uso a una gran cantidad de usuarios, mal funcionamiento en sistemas críticos, etc. Debe ser tratada y resuelta de forma prioritaria.
- Media: No tienen un gran impacto. No obstante, deben ser tratadas cuanto antes para evitar que derive en daños mayores.

6.5 Grupos de comunicación de incidencias

En general, el personal a quien se realiza la comunicación de la incidencia recabará del usuario toda la información posible acerca de la incidencia:

- Persona que ha comunicado la incidencia
- Fecha/hora de la incidencia.
- Descripción detallada de la incidencia.
- Descripción del impacto.

Los grupos de comunicación y/o de gestión de incidencias establecerán:

- Prioridad de la incidencia y,
- Categoría de la incidencia

Una vez resuelta se completará la siguiente información:

- Fecha/hora de resolución
- Acciones y medidas aplicadas para su resolución.

Cuando se trate de una incidencia que implique recuperación de datos de carácter personal, se indicará, además:

- Persona que realiza la recuperación de datos.
- Datos recuperados con éxito (SI/NO).
- Descripción de datos recuperados manualmente (si procede) y,
- Se notificará al RSEG.

A cada incidencia se le asignará un número de identificación único.

6.6 Procedimiento de comunicación y gestión de incidencias**6.6.1 Fase 1: Comunicación y detección de incidencias de seguridad**

La detección y comunicación de comportamientos anómalos en la infraestructura tanto física como lógica 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.

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	10/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

El mecanismo de detección puede ser manual, notificado directamente por una persona (interna o externa a la FGUCM), para lo cual el Instituto dispone de los canales adecuados (correo electrónico csi.fundacion@ucm.es, telefónico 91 394 1561, la herramienta de ticket de la FGUCM) para esta comunicación.

Además, la FGUCM dispone de 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 son entidades externas como CCNCert, 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 el Instituto.

6.6.2 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 dispone de 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, se registra 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 procede 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 determinan las actuaciones a realizar, incluida la notificación de la incidencia fuera de la FGUCM (CCNCert, AEPD, y otros posibles interesados), o bien avanzar en el análisis y resolución de la incidencia previamente a esta notificación exterior. Debe atenderse al cumplimiento legal y contractual de los plazos de notificación aplicables (72 horas para incidencias referidas a datos de carácter personal).

6.6.3 Fase 3: Análisis de la incidencia

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

Se guarda 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 han formalizado las acciones pertinentes.

Debe 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 documenta y registra en el ticket de la incidencia todas las acciones que se realicen sobre los sistemas (fotografía, impresa, video, copia de pantallas, entre otras).

El RIS/RT o ComSeg asignan 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 permitan abordar su resolución y la recuperación de los sistemas al estado anterior a la materialización del incidente.

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	11/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

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, en el caso de incidentes graves, se solicita la participación de CCNCert, AEPD, FCSE o judicial.

Estas decisiones deben 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 desarrolla en las fases siguientes.

Para ello se intentará aclarar los siguientes puntos sobre la incidencia:

- la naturaleza (podría ser diferente a la determinada en la evaluación inicial)
- el origen
- la intención (si es aleatorio o muestra indicios de estar planificado y dirigido a algo concreto)
- los sistemas y servicios exactos a los que ha afectado
- efecto producido (la información a la que se ha tenido acceso y su grado de confidencialidad, activos perdidos o deteriorados, servicios interrumpidos o degradados, etc.)
- si ha finalizado o continúa ocurriendo en ese momento.

INFORMAR A LAS PARTES INTERESADAS acerca de los sucesos ocurridos y cómo proceder hasta que se resuelva la incidencia.

RECOLECCIÓN DE EVIDENCIAS con calidad suficiente y mantenimiento y protección de estas, especialmente cuando la incidencia ha provocado daños importantes y pueda conllevar acciones legales. La recolección de evidencias se realizará lo antes posible, teniendo en cuenta lo desarrollado en el apartado Recolección de evidencias de este procedimiento, y se almacenarán en lugar seguro. Se tendrán en consideración tanto las evidencias electrónicas como las evidencias en papel.

6.6.4 Fase 4: Respuesta a la incidencia

En esta fase se pone en marcha el Plan de actuación obtenido de la fase anterior. En caso de que así se determine se produce 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.

6.6.4.1 CONTENCIÓN DEL INCIDENTE.

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

La FGUCM dispone 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 evalúa 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 participan 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 recopilan y preservan las evidencias de la infraestructura física y tecnológica tales como fotos, videos, copias de discos, traza de registros (logs), y otros que se consideren oportunos.

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	12/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

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

Aunque detener los efectos que pueda estar causando en los sistemas y servicios es la misión de esta subfase, a la hora de la contención del incidente se establecen una serie de prioridades que pueden variar en función de éste, pero que en general debe ser:

- Proteger la vida humana
- Proteger la información clasificada
- Proteger el hardware y el software contra el ataque, la pérdida o la modificación de los archivos de sistema y contra daños físicos al hardware.

Se debe valorar la posibilidad de contactar con las autoridades en el caso de que el incidente esté provocado por un origen externo a la organización, de forma que se pueda actuar contra él y neutralizarlo. Esta decisión es responsabilidad del ComSeg o de la Dirección.

6.6.4.2 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), son los encargados de atender en primera instancia las incidencias que le sean comunicadas y resolverlas.

El liderazgo de las actuaciones la realiza 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, es el ComSeg quien lidere las actuaciones. Se cuenta 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 aplican los Planes de Emergencia, Contingencia y de Recuperación disponibles en el Instituto.

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

6.6.5 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 someten a una monitorización intensiva para identificar posibles problemas no contemplados o bien se pudieran reproducir.

La resolución de la incidencia se considera 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, es el RIS/RT o el ComSeg quien dará por cerrada la incidencia cuando la Fase 4 esté completamente realizada. Para ello deberá asegurarse que:

- 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.

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	13/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

Cuando finalice la gestión de un incidente se da 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 comunica 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 realizan las comunicaciones oportunas, y en aquellos que traten datos de carácter personal se sigue lo estipulado en la legislación vigente de protección de datos comunicando en un plazo no superior a 72h con el AEPD.

6.6.6 Fase 6: Mejora continua de la seguridad

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

Se establecen 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 deben 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 del Instituto.

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

6.7 Acciones especiales

Se recogen a continuación acciones especiales a llevar a cabo por los Administradores, durante el proceso de resolución de las incidencias, según la categoría de ésta:

- **De origen humano por un empleado de la organización:**
 - o Comunicar al Responsable del empleado, al Responsable de Seguridad y si se estima oportuno, al departamento de RRHH.
- **De origen físico o robo / Destrucción / Manipulación del Equipamiento:**
 - o Informar al Comité de Seguridad
- **De origen natural:**
 - o Notificar al Comité de Seguridad, que decidirá sobre la notificación a las autoridades y organismos públicos pertinentes.
- **De origen en la Operación (cambios)**

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	14/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

- o Si la aplicación es externa o soportada por un tercero, se le avisará
 - o Si no se puede resolver la incidencia, se volverá a la versión o configuración anterior
 - o Se instruirá al personal implicado para que se lleven a cabo los cambios de forma correcta
- **Ingeniería Social y suplantación de la identidad**
 - o Dar aviso a los empleados de la organización. Instruirles sobre las medidas de seguridad que deben tomar al respecto
 - o Forzar el cambio de contraseña
- **Ataque consumado con pérdida de Confidencialidad / Integridad / Disponibilidad sobre datos confidenciales o superiores, incluidos los datos de carácter personal**
 - o En caso de intrusión:
 - Como medida Urgente, si el Administrador de sistemas percibe que la gravedad de la intrusión lo aconseja, debe desconectar el sistema afectado de la red, antes que poner en peligro información confidencial. Siempre que sea posible, esta acción debe ser respaldada por el Comité de Seguridad
 - Si el Administrador del Sistema estima que el sistema afectado puede tener múltiples daños y no es posible su recuperación tal como estaba antes de la intrusión (limpio de virus, caballos de troya, programa de hacking ocultos, etc.) debe restaurar el sistema desde cero. Siempre que sea posible, esta acción debe ser respaldada por el Comité de Seguridad
 - o En caso de Escucha de Tráfico, si es detectado en tiempo real, se dejará de transmitir y se forzará el cambio de contraseña
 - o Realizar las acciones indicadas para el Intento de Intrusión y Ataque
 - o Informar al Comité de Seguridad, quién decidirá las acciones adicionales a llevar a cabo
- **Intento de intrusión o ataque** (intentos de intrusión aprovechando una vulnerabilidad, sin llegar a ser consumada)

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora	
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20	
Observaciones		Página	15/34	
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

- o Impedir que el intruso continúe, siempre que se pueda detectar en tiempo real, bloqueando el paso a su dirección IP
- o Corregir lo antes posible la vulnerabilidad que se está aprovechando para ello
- o Si se realiza a través de un puerto no necesario, éste se cerrará
- o Si el Administrador percibe que es potencialmente peligroso se debe obtener información exhaustiva, dentro de lo posible:
 - Fecha y hora de cada intento de ataque
 - Dirección IP con resolución inversa de DNS, identificando el dominio
 - Vulnerabilidad encontrada y tipo de exploit o programa que se está usando para el ataque
 - Informe de la estrategia de ataque seguida por el atacante
 - Servicios que se han visto afectados por el atacante
 - Historia anterior de ataques procedentes del mismo lugar (misma dirección IP)
- **Legal:**
 - o Notificar al Comité de Seguridad, que decidirá sobre las comunicaciones o denuncias a las autoridades pertinentes
 - o En caso de datos de carácter personal notificar al DPD
- **De origen interno y destino externo a la organización.** Este tipo de incidencias suele detectarse por aviso del destino atacado:
 - o Reconocimiento: cuando el atacante está buscando información y posibles vulnerabilidades, pero sin realizar aún ninguna acción de ataque que aproveche dichas vulnerabilidades:
 - No se envía respuesta alguna al dominio atacado. Si en algún caso particular se considera necesario emitir una respuesta, evitar explícitamente dar cualquier in-

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	16/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

formación acerca de las infraestructuras de seguridad de la organización, servicios, políticas, procedimientos, o en general, cualquier detalle más allá de una mera respuesta de cortesía

o Intento:

- El Administrador de sistemas informa al Comité de Seguridad que decide si se responde a la notificación del dominio atacado, en cuyo caso se tiene en consideración lo anteriormente mencionado respecto a la divulgación de información sensible de la organización.

o Consumado:

- Se informa al Comité de Seguridad
- Se obtiene información exhaustiva del incidente.
- Se impide la salida a Internet del sistema atacante
- A criterio del Comité de Seguridad, se cooperará con el dominio atacado para esclarecer los hechos
- El Comité de Seguridad informa del incidente a la Dirección
- A criterio de la Dirección se informa del incidente a otras organizaciones que pudieran verse afectados por el mismo.

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 este procedimiento corresponde al Responsable de Seguridad de la Información, que es competente para:

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora	
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20	
Observaciones		Página	17/34	
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

- Interpretar las dudas que puedan surgir en su aplicación.
- 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 Responsable de Seguridad de la Información revisará el presente procedimiento, 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 Responsable de Seguridad de la Información el encargado de la custodia y divulgación de la versión aprobada de este documento.

9. Aprobación

El presente procedimiento ha sido aprobado por el Responsable 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 Responsable de Seguridad de la Información.

Firma: _____

Responsable de Seguridad de la Información

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	18/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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**10. Anexo I - Recolección de evidencias****10.1 Definiciones**

Análisis forense: el análisis forense de un ordenador o de un sistema de información consiste en la recopilación, preservación y análisis de información contenida en el equipo o los equipos que constituyen el sistema de información para descubrir el origen de un delito.

10.2 Desarrollo

El análisis forense de ordenadores se realiza después que el sistema haya sufrido algún ataque informático o se haya visto involucrado en uno y sea objeto de investigación, o bien si se tienen indicios de que se haya cometido un delito informático. Este examen se realiza para saber qué ha pasado, cómo ha ocurrido y obtener las pruebas e información necesaria.

Para realizar un análisis forense de un ordenador es necesario seguir una serie de pasos para asegurarse que se realiza de forma correcta y no se invalida ninguna prueba.

10.2.1 Obtención de las autorizaciones necesarias

Antes de comenzar este procedimiento, es imprescindible tener la autorización tanto del propietario del dispositivo como del usuario o responsable del departamento o empresa. En caso contrario, se estaría violando la privacidad de la persona y eso podría constituir un delito.

La autorización para empezar un análisis forense de un ordenador puede proceder tanto por parte de la empresa como de un juez, si fuera el caso que se estuviera llevando a cabo una investigación judicial.

10.2.2 Principios durante la recolección de evidencias

El procedimiento de recolección de evidencias debe ser lo más detallado posible, transparente y reproducible, así como reducir al mínimo la toma de decisiones.

Principios guía:

- Preservación
- Adquisición
- Análisis
- Documentar
- Presentación de resultados

10.2.3 Pasos para tener en cuenta y documentar cada paso

- Capturar una imagen del sistema tan precisa como sea posible.
- Realizar notas detalladas, incluyendo fechas y horas indicando si se utiliza horario local o UTC.
- Minimizar los cambios en la información que se está recolectando y eliminar los agentes externos que puedan hacerlo.
- En el caso de enfrentarse a un dilema entre recolección y análisis elegir primero recolección y después análisis.
- Recoger la información según el orden de volatilidad (de mayor a menor).

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	19/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

- Tener en cuenta que por cada dispositivo la recogida de información puede realizarse de distinta manera.
- ¿Dónde está la evidencia? > Listar qué sistemas están involucrados en el incidente y de cuáles de ellos se deben adquirir evidencias.
- Establecer qué es relevante. En caso de duda es mejor recopilar cuanta más información mejor.
- Fijar el orden de volatilidad para cada sistema.
- Obtener la información de acuerdo con el orden establecido.
- Comprobar la hora del sistema.
- Personal involucrado. Tomar nota del personal implicado en el incidente, personal con el que mantienes reunión, etc.
- Cálculo de HASHES de todas las evidencias.

10.2.4 Principios durante la recolección de evidencias**Si el sistema a analizar está encendido:**

Establecer el orden de volatilidad:

- El orden de volatilidad hace referencia al período de tiempo en el que está accesible cierta información. Es por ello por lo que se debe recolectar en primer lugar aquella información que vaya a estar disponible durante el menor período de tiempo, es decir, aquella cuya volatilidad sea mayor.
- No apagar el ordenador hasta que se haya recopilado toda la información.
- Registros y contenido de la caché.
- Tabla de enrutamiento, caché ARP, tabla de procesos, estadísticas del kernel, memoria.
- Información temporal del sistema.
- Disco
- Logs del sistema.
- Configuración física y topología de la red.
- Documentos

No confiar en la información proporcionada por los programas del sistema ya que pueden haberse visto comprometidos.

No ejecutar programas que modifiquen la fecha y hora de acceso de todos los ficheros del sistema.

Si el sistema a analizar está apagado:

Obtener una imagen de disco mediante clonado bit a bit de todas las particiones existentes en el disco.

10.2.5 Cadena de custodia – Procedimiento de almacenamiento

Se define este término como el procedimiento oportunamente documentado, que permite constatar la identidad, integridad y autenticidad de los elementos adquiridos en la adquisición, desde que son encontrados hasta que se finaliza el proceso o, en caso necesario, se aporten al proceso judicial como pruebas.

En ésta se deben detallar los siguientes puntos:

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora	
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20	
Observaciones		Página	20/34	
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

- Dónde, cuándo y quién llevó a cabo el proceso de adquisición de evidencias.
- Dónde, cuándo y quién manejó la evidencia.
- Quién ha custodiado la evidencia, cuánto tiempo y cómo ha sido almacenada.

En el caso de que la evidencia cambie de custodia se debe documentar el proceso de intercambio de ésta, así como anexar toda la información necesaria.

El almacenamiento de los elementos adquiridos se debe realizar en dispositivos cuya seguridad esté demostrada, permita detectar intentos de acceso no autorizados y cuente con las medidas de seguridad necesarias para tal fin.

11. Anexo II - Clasificación de las incidencias

Para su correcta gestión, todos los incidentes deberán ser clasificados. La clasificación de incidentes de seguridad dependerá de factores tales como:

- La naturaleza del incidente,
- La criticidad del/los sistema/s afectado/s,
- El número de sistemas afectados,
- El impacto que el incidente puede tener en el Instituto desde un punto de vista legal, de imagen pública, y de prestación de servicio,
- Los requerimientos legales y regulativos.

Un incidente que contenga múltiples clases o tipologías debe ser clasificado por el evento de seguridad original que fue detectado inicialmente. Esto no quita para que, en ciertos casos, en una fase posterior se pueda realizar un cambio de clasificación en caso de que, a la luz de los nuevos datos que puedan obtenerse, fuera conveniente hacerlo.

Con objeto de hacer más efectiva la comunicación tanto interna como otros agentes externos que puedan colaborar en el proceso de identificación y gestión de incidentes, es necesario establecer un modelo de referencia según el cual se realice la clasificación de los incidentes, con idea de que todos los involucrados empleen una terminología lo más afín posible. En la siguiente tabla, se ilustra el modelo de referencia empleado en la guía CCN-STIC-817 (apartado 6.1.) para la clasificación de incidentes de seguridad.

Clase	Descripción	Tipo
Código dañino	Software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas.	Virus
		Gusanos
		Trojanos
		Spyware
		Rootkit
		Ransomware
		Herramienta para acceso remoto (RAT – Remote Access Tool)
Disponibilidad	Ataques dirigidos a poner fuera de servicio los sistemas, al objeto de causar daños en	Denegación [Distribuida] del Servicio DoS / DDoS

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	21/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

Clase	Descripción	Tipo
	la productividad y/o la imagen de las instituciones atacadas.	Fallo (Hardware/Software)
		Error humano
		Sabotaje
Obtención de información	Ataques dirigidos a recabar información fundamental que permita avanzar en ataques más sofisticados, a través de ingeniería social o de identificación de vulnerabilidades.	Identificación de activos y vulnerabilidades (escaneo)
		Sniffing
		Ingeniería social
		Phishing
Intrusiones	Ataques dirigidos a la explotación de vulnerabilidades de diseño, de operación o de configuración de diferentes tecnologías, al objeto de introducirse de forma fraudulenta en los sistemas de una organización.	Compromiso de cuenta de usuario
		Defacement (desfiguración)
		Cross-Site Scripting (XSS)
		Cross-Site Request Forgery (CSRF)
		Falsificación de petición entre sitios cruzados
		Inyección SQL
		Spear Phishing
		Pharming
		Ataque de fuerza bruta
		Inyección de Ficheros Remota
Compromiso de la información	Incidentes relacionados con el acceso y fuga (Confidencialidad), modificación o borrado (Integridad) de información no pública.	Explotación de vulnerabilidad software
		Explotación de vulnerabilidad hardware
		Acceso no autorizado a red
		Acceso no autorizado a información
Fraude	Incidentes relacionados con acciones fraudulentas derivadas de suplantación de identidad, en todas sus variantes.	Modificación y borrado no autorizada de información.
		Publicación no autorizada de información
		Exfiltración de información
		Suplantación / Spoofing
Contenido abusivo		Uso de recursos no autorizado
		Uso ilegítimo de credenciales
		Violaciones de derechos de propiedad intelectual o industrial
		Spam (Correo Basura)

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	22/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

Clase	Descripción	Tipo
	Ataques dirigidos a dañar la imagen de la organización o a utilizar sus medios electrónicos para otros usos ilícitos (tales como la publicidad, la extorsión o, en general la ciberdelincuencia).	Acoso/extorsión/ mensajes ofensivos Pederastia/ racismo/ apología de la violencia/delito, etc.
Política de seguridad	Incidentes relacionados por violaciones de usuarios de las políticas de seguridad aprobadas por la organización.	Abuso de privilegios por usuarios Acceso a servicios no autorizados Sistema desactualizado Otros
Otros	Otros incidentes no incluidos en los apartados anteriores	

12. Anexo III - Criticidad de los incidentes

Conviene destacar que los niveles de criticidad (o peligrosidad) son generales, pudiendo afectar, a la hora de determinar la criticidad de un incidente concreto, factores como la existencia de pérdidas en los servicios TIC, el número de usuarios afectados, el impacto económico, o la habilidad del equipo local de respuesta a incidentes de seguridad. A continuación, se describe cada uno de los niveles:

Nivel de criticidad o peligrosidad	Descripción
BAJO / NULO	Se clasifican con este nivel de criticidad los casos de incidentes en que se tiene constancia de la existencia de una amenaza que ha afectado o está afectando a sistemas TIC del Instituto pero que los controles de seguridad desplegados están funcionando y contrarrestan adecuadamente la misma y, por tanto, su impacto es nulo o insignificante para el Instituto.
MEDIO	Se clasifican con este nivel de criticidad los casos de incidentes en que se tiene constancia de la existencia de una amenaza que ha afectado o está afectando a sistemas TIC del Instituto y se sabe que ha tenido un impacto limitado en información considerada no crítica para la misión del Instituto y/o sistemas TIC no críticos en la arquitectura de los sistemas TIC del Instituto (por ejemplo, equipos de usuario).
ALTO	Se clasifican con este nivel de criticidad los casos de incidentes en que se tiene constancia de la existencia de una amenaza que ha afectado o está afectando a sistemas TIC del Instituto y se sabe que ha tenido un impacto considerable (afectación a la confidencialidad, disponibilidad o integridad) en información considerada no crítica para la misión del Instituto y/o sistemas TIC no críticos en la arquitectura de los sistemas TIC del Instituto (por ejemplo, equipos de usuario).
MUY ALTO	Se clasifican con este nivel de criticidad los casos de incidentes en que se tiene constancia de la existencia de una amenaza que ha afectado o está afectando a sistemas TIC del Instituto y se sabe que ha tenido un impacto considerable (afectación a la confidencialidad, disponibilidad o integridad) en información considerada crítica para la misión del Instituto

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	23/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

Nivel de criticidad o peligrosidad	Descripción
	y/o sistemas TIC críticos en la arquitectura de los sistemas TIC del Instituto (por ejemplo, elementos de seguridad perimetral de red, sistemas de autenticación centralizada, etc.).
CRÍTICO	Se clasifican con este nivel de criticidad los casos de incidentes en que se tiene constancia de la existencia de una amenaza que ha afectado o está afectando a sistemas TIC del Instituto y se sabe que ha tenido un impacto muy considerable (afectación total de la confidencialidad, disponibilidad o integridad) en información considerada crítica para la misión del Instituto y/o sistemas TIC críticos en la arquitectura de los sistemas TIC del Instituto (por ejemplo, elementos de seguridad perimetral de red, sistemas de autenticación centralizada, etc.).

La tabla siguiente muestra el **Nivel de Peligrosidad de los Ciberincidentes**, atendiendo a la repercusión que la materialización de la amenaza de que se trate podría tener en los sistemas de información de las entidades del ámbito de aplicación del ENS.

Nivel	Amenaza(s) subyacente(s) más habituales	Vector de ataque	Características potenciales del ciberincidente
BAJO / NULO	- Ataques a la imagen - Menosprecio - Errores y fallos	- Políticas. - Spam sin adjuntos. - Software desactualizado. - Acoso / coacción / comentarios ofensivos. - Error humano / Fallo HW-SW.	- Escasa capacidad para exfiltrar un volumen apreciable de información. - Nula o escasa capacidad para tomar el control de sistemas.
MEDIO	- Logro o incremento significativo de capacidades ofensivas - Desfiguración de páginas web - Manipulación de información	- Descargas de archivos sospechosos. - Contactos con dominios o direcciones IP sospechosas. - Escáneres de activos y vulnerabilidades. - Códigos dañinos de Bajo Impacto (adware, spyware, etc.) - Sniffing / Ingeniería social.	- Capacidad para exfiltrar un volumen apreciable de información. - Capacidad para tomar el control de algún sistema.
ALTO	- Toma de control de los sistemas - Robo y publicación o venta de información sustraída - Ciberdelito - Suplantación	- Códigos dañinos de Medio Impacto (virus, gusanos, troyanos). - Ataques externos – compromiso de servicios no esenciales (DoS / DDoS). - Tráfico DNS con dominios relacionados con APTs o campañas de malware. - Accesos no autorizados / Suplantación / Sabotaje. - Cross-Site Scripting / Inyección SQL.	- Capacidad para exfiltrar información valiosa. - Capacidad para tomar el control de ciertos sistemas.

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	24/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

Nivel	Amenaza(s) subyacente(s) más habituales	Vector de ataque	Características potenciales del ciberincidente
		- Spear phishing / pharming	
MUY ALTO	- Interrupción de los Servicios IT - Exfiltración de datos - Compromiso de los servicios	- Códigos dañinos confirmados de Alto Impacto (RAT, troyanos enviando datos, rootkit, etc.) - Ataques externos con éxito.	- Capacidad para exfiltrar información valiosa, en cantidad apreciable. - Capacidad para tomar el control de los sistemas sensibles, en cantidad considerable.
CRÍTICO	Ciberspionaje	- APTs, campañas de malware, interrupción de servicios, compromiso de sistemas de control industrial, incidentes especiales, etc.	- Capacidad para exfiltrar información muy valiosa, en cantidad considerable y en poco tiempo. - Capacidad para tomar el control de los sistemas sensibles, en cantidad y en poco tiempo.

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	25/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

En función del nivel de criticidad se establecen unos tiempos límite para el registro e inicio de la gestión del incidente:

Nivel de criticidad o peligrosidad	Tiempo para registro interno e inicio de la gestión del incidente
BAJO / NULO	Lo antes posible, pero no más de 1 mes desde la detección.
MEDIO	Lo antes posible, pero no más de 1 semana desde la detección.
ALTO	En las 48 horas siguientes a la detección.
MUY ALTO	En las 12 horas siguientes a la detección.
CRÍTICO	En 4 hora tras la detección.

13. Anexo IV - Brechas de seguridad de datos de carácter personal

El objetivo de este procedimiento específico es cumplir con lo establecido en el Reglamento General de Protección de Datos (**RGPD**) en lo relativo a la notificación a la autoridad de control de brechas de seguridad de datos personales (artículo 33 del RGPD) así como la comunicación a los afectados o interesados (artículo 34 del RGPD) en caso de que proceda.

Conforme al RGPD, se considerarán “brechas de seguridad” a todo percance que origine la destrucción, pérdida o modificación accidental o ilícita de datos personales cedidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos. Incidentes como la pérdida de un ordenador portátil, el acceso no autorizado a las bases de datos (incluso por su propio personal) o el borrado accidental de algunos registros que no puedan ser recuperadas son consideradas brechas de seguridad, y son de aplicación para este procedimiento.

El responsable de tratamiento podrá elaborar procedimientos específicos de actuación, enfocados a tratamientos de datos personales y escenarios de brechas de seguridad específicos, que incluirán en todo caso referencias a este procedimiento en lo referido a las notificaciones a la AEPD y a los afectados en caso de que proceda. Dichos procedimientos podrán incluir aspectos como restringir el acceso a los servicios, parar los servicios, cortar las comunicaciones, etc.

13.1 Notificación a la Agencia Española de Protección de Datos

En caso de producirse una brecha de la seguridad de los datos personales, el Director del Instituto la notificará a la Agencia Española de Protección de Datos (AEPD) de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

En caso de que la brecha se haya producido por parte de un encargado de tratamiento, este último notificará sin dilación indebida al responsable del tratamiento (FGUCM), la brecha de la seguridad de los datos personales de las que tenga conocimiento.

La notificación a la AEPD deberá contener como mínimo:

- Descripción de la naturaleza de la brecha de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	26/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

- b) Nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- c) Descripción de las posibles consecuencias de la brecha de la seguridad de los datos personales.
- d) Descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la brecha de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no fuera posible facilitar toda la información a la vez o de forma completa porque aún se desconozca el origen de la brecha, u otros aspectos, se irán realizando notificaciones a la AEPD, con los aspectos que se vayan conociendo o los avances que se vayan realizando.

El responsable del tratamiento asesorado por el DPD documentará cualquier brecha de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la AEPD, en caso de requerirlo, verificar el cumplimiento de lo exigido en el artículo 33 del RGPD.

13.1.1 Descriptivo de notificación a la AEPD

Datos identificativos y de contacto de:

1. Nombre del responsable del tratamiento:

[FUNDACIÓN GENERAL DE LA UNIVERSIDAD COMPLUTENSE DE MADRID, CIF:..., dirección]

2. Identidad y datos de contacto del responsable de protección de datos:

[Nombre y apellidos del Delegado de Protección de Datos, teléfono de contacto, y correo electrónico]

3. Indicación de si se trata de una primera, segunda notificación Información inicial sobre el caso de violación de datos personales (en su caso, complétese en notificaciones posteriores):

[Notificación inicial, primera notificación de seguimiento, segunda notificación de seguimiento, etc. Breve descripción de qué se trata. Ejemplos:

- Notificación inicial de fuga de datos de usuarios de JORNADAS Y EVENTOS y BOLETINES.
- Notificación de seguimiento (1): Detectado origen de la fuga en vulnerabilidad web, y bloqueado el acceso a la web.
- Notificación de seguimiento (2): Notificación a los afectados.
- Notificación de seguimiento (3): Corrección de la vulnerabilidad web.
- Notificación de seguimiento (4): Desbloqueo de acceso web, y se informa a los afectados para que cambien sus contraseñas de acceso.
- Notificación de seguimiento (5): Establecimiento de procedimientos para que no vuelva a ocurrir.]

Información sobre la brecha de seguridad de datos personales:

4. Fecha y hora del incidente y de detección de este:

[Completar solo en la notificación inicial, y si se desconocen la fecha y hora en la que se produjo el incidente o se detectó, tratar de realizar una estimación, indicando que se trata de una estimación]

5. Circunstancias en que se ha producido la violación de datos personales:

[Completar. Por ejemplo, pérdida, robo, copia, etc.]

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	27/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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. Naturaleza y contenido de los datos personales en cuestión:

[Completar en la notificación inicial, y en sucesivas notificaciones si se detecta cambios o aumento de la gravedad de la brecha de seguridad. Por ejemplo, datos de menores, de salud]

7. Medidas técnicas y de organización que han aplicado (o aplicarán) para proteger los datos personales en cuestión:

[Completar en cada notificación indicando el estado de las medidas y su eficacia si fuera posible. Especificar si las medidas las debe implantar un tercero encargado de tratamiento]

8. Información suplementaria sobre el caso de violación de datos personales:

[Completar]

9. Resumen del incidente que ha causado la violación de datos personales (con indicación de la ubicación física de la violación y del soporte de almacenamiento):

[Completar]

10. Número de usuarios, registros o particulares afectados:

[Completar. Si no se conoce tratar de realizar una estimación]

11. Posibles consecuencias y efectos negativos en los abonados o particulares:

[Completar]

12. Posible notificación adicional a los usuarios o particulares:

[Completar. Por ejemplo, de medidas de seguridad a tomar por los usuarios, como podría ser cambiar la contraseña de acceso actual de acceso al servicio en caso de que se hubieran filtrado dichas contraseñas, así como cambiarlas también en aquellos servicios de Internet en los que el usuario estuviera usando las mismas contraseñas que la filtrada]

13. Contenido de la notificación a los afectados:

[Completar]

14. Medios de comunicación utilizados para la notificación a los afectados:

[Completar. Por ejemplo, por mail o por teléfono]

15. Número de usuarios o particulares a los que se ha remitido la notificación

[Completar. Indicar además si son solo usuarios españoles o si también hay de otros países]

16. Caso de violación de datos personales que afecta a usuarios o particulares de otros Estados miembros:

[Completar]

17. Notificación a otras autoridades nacionales competentes:

[Completar. Por ejemplo, a Guardia Civil con el Grupo de Delitos Telemáticos y la Policía con la Brigada de Investigación Tecnológica]

13.1.2 Canal de Notificación a la AEPD

La notificación a la AEPD se realizará a través del formulario destinado a tal efecto publicado en la sede electrónica de la Agencia.

A cada notificación se le asignará una referencia que el responsable deberá mantener e incluir en las sucesivas comunicaciones relacionadas si las hubiera, con el fin de proporcionar un seguimiento completo del incidente.

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	28/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

Este trámite electrónico está dirigido exclusivamente a responsables del tratamiento, que tienen la obligación de notificar sus brechas de seguridad a la AEPD. No es un trámite dirigido a los ciudadanos que disponen de procedimientos en la Sede Electrónica para poner en conocimiento de la AEPD posibles vulneraciones de la normativa de protección de datos, en particular de posibles incumplimientos del RGPD.

La persona que vaya a realizar la presentación de la notificación de quiebra de seguridad deberá:

- 1.- Acceder al formulario, en la siguiente dirección web:

<https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/tipoSolicitud/solicitudClave.jsf#>

Método de Identificación:

- DNle / Certificado electrónico
 - Cl@ve PIN
 - Cl@ve permanente
 - Ciudadanos UE
- 2.- Rellenar el formulario tras acceder al mismo mediante el botón '**Acceso al trámite**':
 - Indicar si se trata de una notificación inicial a la que se añadirá información en el futuro.
 - Introducir los datos del Delegado de Protección de Datos (DPD). En caso de no tener designado un DPD, introducir los datos de una persona de contacto.
 - Introducir los datos del responsable del tratamiento.
 - Introducir los datos del encargado del tratamiento e indicar la existencia de más encargados del tratamiento.
 - Introducir la información relativa a la brecha de seguridad, datos afectados.
 - Introducir la información relativa a los sujetos afectados y las posibles consecuencias.
 - Indicar las posibles implicaciones transfronterizas de la brecha.
 - 3.- Una vez relleno el formulario, pulse 'Enviar' para presentar la notificación.
 - 4.- El sistema le ofrecerá la posibilidad de descargar un archivo PDF con el justificante de haber realizado la notificación.

13.2 Notificación a los afectados

Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento, y coordinado por el DPD, la comunicará a los interesados sin dilación indebida.

La comunicación al interesado se hará por el medio que se considere más adecuado según los datos disponibles del afectado y del tratamiento o tratamientos afectados por la brecha, y describirá en un lenguaje claro y sencillo la naturaleza de la brecha de la seguridad de los datos personales, que contendrá como mínimo:

- a) Nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- b) Descripción de las posibles consecuencias de la brecha de la seguridad de los datos personales.
- c) Descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la brecha de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	29/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

La comunicación al interesado **no será necesaria si se cumple alguna de las condiciones siguientes:**

- El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.
- El responsable del tratamiento hubiera tomado medidas previas a la brecha que garantizan que no existe la probabilidad de que se concrete el alto riesgo para los derechos y libertades del interesado, por ejemplo, si los datos se encontraban cifrados.
- Suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

En la notificación a la AEPD, deberá indicarse si se considera no notificar a los afectados basándose en alguno de los supuestos indicados anteriormente. La AEPD podrá considerar adecuada la decisión o no, en cuyo caso podrá exigirle a la FGUCM que lo haga.

13.2.1 Modelo de notificación a los afectados**NOTIFICACIÓN DE BRECHA DE SEGURIDAD A LOS AFECTADOS**

1. Nombre del responsable del tratamiento:

[FUNDACIÓN GENERAL DE LA UNIVERSIDAD COMPLUTENSE DE MADRID, CIF:....., dirección]

2. Identidad y datos de contacto del responsable de protección de datos:

[Nombre y apellidos del Delegado de Protección de Datos, teléfono de contacto, y correo electrónico]

3. Resumen del incidente que ha causado la violación de datos personales:

[Completar]

4. Fecha estimada del incidente:

[Completar]

5. Naturaleza y contenido de los datos personales en cuestión:

[Completar. ¿Qué tipo de datos personales han sido modificados de forma no autorizada, accedidos de forma no autorizada, eliminados sin autorización]

6. Posibles consecuencias de la violación de datos personales para el usuario o particular afectado:

[Completar]

7. Circunstancias en que se ha producido la violación de datos personales:

[Completar]

8. Medidas adoptadas por el responsable del tratamiento para subsanar la violación de datos personales:

[Completar]

9. Medidas recomendadas por el proveedor para paliar los posibles efectos negativos:

[Completar]

En Madrid a ____ de ____ de 20 ____

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	30/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

Firma (Delegado de Protección de Datos)

14. Anexo V – Notificaciones

14.1 Evaluación del deber de notificar al CCN-CERT

- La evaluación del deber de notificar al CCN-CERT se realiza en función del “IMPACTO en la organización” (ficha GESTION-INCIDENTE01).
- El nivel de impacto no tiene que ser concluyente para determinar si se notifica el incidente de seguridad, pero es obligatorio notificar al CCN-CERT en los casos que se determine que el nivel sea Alto, Muy Alto o Crítico. Esta notificación al CCN-CERT se realizará mediante la instancia de la herramienta LUCIA.

IMPACTO en la organización	CRÍTICO	Notificar al CCN-CERT (LUCIA)
	MUY ALTO	
	ALTO	
	MEDIO	NO ES OBLIGATORIO notificar al CCN-CERT
	BAJO	

14.2 Evaluación del deber de notificar a la Autoridad de Control en materia de Protección de Datos

- El RGPD establece que, en caso de brecha de la seguridad de los datos personales, RT la notificará a la autoridad de control competente en materia de protección de datos sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha brecha de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.
- Por tanto, la evaluación del deber de notificar a la Autoridad de Control en Protección de Datos en cumplimiento del RGPD (AEPD), se realizará en función del “NIVEL DE CRITICIDAD con respecto a la privacidad de los datos personales”.

NIVEL DE CRITICIDAD con respecto a la privacidad de los datos personales	CRÍTICO	OBLIGATORIO notificar a la Autoridad de Control en materia de Protección de Datos en 72 horas
	MUY ALTO	
	ALTO	
	MEDIO	NO ES OBLIGATORIO notificar a la Autoridad de Control en materia de Protección de Datos
	BAJO	

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	31/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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
14.3 Evaluación del deber de notificar a las personas interesadas

- El RGPD también establece los casos en los que una brecha de seguridad se debe comunicar al afectado, en concreto cuando sea probable que la brecha de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas.
- Por tanto, la evaluación del deber de notificar a las personas afectadas se realizará en función de la "SEVERIDAD de las CONSECUENCIAS para las personas interesadas".

SEVERIDAD de CONSECUENCIAS para las personas interesadas	MUY ALTA	OBLIGATORIO notificar a las personas interesadas
	ALTA	OBLIGATORIO notificar a las personas interesadas
	MEDIA	OBLIGATORIO notificar a las personas interesadas
	BAJA	NO ES OBLIGATORIO a las personas interesadas

- Si se prevé que la comunicación a los afectados puede comprometer el resultado de una investigación en curso, la comunicación podría posponerse siempre bajo la supervisión de la autoridad de control (AEPD).

14.4 Evaluación del incidente como delito

- Para evaluar que el Incidente de Seguridad TIC se haya determinado la constitución invariable de un delito debe haber una valoración como tal.
- Dicha valoración de la constitución del delito vendrá dada por los RIS/RT y RSEG con el apoyo en materia normativa y legislativa del DPD, el cual podrá solicitar apoyo al Gabinete Jurídico.
- En estos casos, la valoración y escalado al RIS/RT deberá tener un carácter urgente. En los casos donde la constitución del delito es evidente, el escalado y la denuncia del delito deberá realizarse de forma inmediata.

14.5 Notificar al CCN-CERT

- El RIS realizará la notificación del incidente según los canales definidos por CCN-CERT, contando con el soporte del RSEG.

14.6 Notificar a la Autoridad de Control en materia de protección de datos

- El RT afectados notificará a la Autoridad de Control en materia de protección de datos en un plazo no superior a 72 horas el incidente.

14.7 Notificar a las personas interesadas

- Si así se hubiera estimado pertinente, el RT afectados notificará a las personas interesadas cuyos derechos se hayan visto afectados, preferentemente de forma directa, ya sea por teléfono, correo electrónico, SMS, correo postal, u otro medio adecuado.
- La comunicación a los afectados se realizará a la mayor brevedad posible, en un lenguaje claro y sencillo y en el caso en que exista una investigación en curso, se hará en estrecha cooperación

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	32/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

con la autoridad de control competente en materia de protección de datos (AEPD) y las autoridades policiales, de acuerdo con sus orientaciones.

- Esta comunicación, debería contener como mínimo:
 - Datos de contacto del DPD.
 - Descripción general del incidente y momento en que se ha producido.
 - Las posibles consecuencias de la brecha de la seguridad de los datos personales.
 - Descripción de los datos e información personal afectados.
 - Resumen de las medidas implantadas hasta el momento para controlar los posibles daños.
 - Otras informaciones útiles a los afectados para proteger sus datos o prevenir posibles daños.
- La notificación indirecta, a través de avisos públicos en sitios web como blogs corporativos, o comunicados de prensa, se utilizará cuando para la notificación directa los costos sean excesivos o cuando no sea posible contactar con las personas afectadas (por ejemplo porque se desconocen, o los datos de contacto no están actualizados).

14.8 Denunciar delito

- Los pasos a seguir para la denuncia de delito son los siguientes:

1	Evaluación del incidente	RIS/RT
	Evaluación del incidente, en el que se continuará con el procedimiento de denuncia cuando se trate de: - Agresiones. - Ataques. - Interceptación o intrusiones. - Accesos no autorizados. - Utilización fraudulenta contra/de activos intangibles tales como: - Sistemas de comunicaciones o de información. - Aplicaciones. - Datos. - Elementos de soporte de cualesquiera de los items anteriores. - Servicios prestados por los items anteriores.	
2	Operaciones técnicas reactivas	RSEG
	La persona RSEG realizará las recomendaciones técnicas reactivas necesarias para que el incidente no se continúe produciendo. Las medidas se comunicarán al RIS/RT, y en el caso de que hayan sido afectados Datos Personales, se comunicará conjuntamente al DPD.	
3	Informe completo del Incidente de Seguridad TIC	RSEG
	La persona RSEG generará un informe completo con los detalles del incidente:	

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	33/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%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

	• Hechos detectados. • Daños recibidos. • Cualquier otra información que pueda contribuir al esclarecimiento del caso. A su vez, la persona RSEG pondrá a disposición del RIS/RT dicho el informe, al igual que al DPD y a CCN-CERT en el caso de que se realice la notificación a este organismo.	
4	Crear escrito con informe sobre el incidente	RIS/RT
	La denuncia adoptará la forma de un escrito de remisión firmado (preferentemente de forma digital) por el titular del centro directivo o equivalente (RIS/RT), al que acompañará un Informe completo de la persona RSEG. Se incluirá un teléfono de contacto para que el grupo policial que finalmente lleve la investigación pueda obtener aclaraciones o informes suplementarios.	
5	Interponer Denuncia ante las Fuerzas de Seguridad del Estado	RIS/RT
	Interponer denuncia ante la Unidad de la Policía Nacional o de la Guardia Civil. Se aportarán los siguientes datos: • Informe completo del activo creado por la persona RSEG. • Informe de los hechos detectados. • Informe de los daños recibidos. • Cualquier otra información que pueda contribuir al esclarecimiento del caso. • Se incluirá un teléfono de contacto para que el grupo policial pueda obtener aclaraciones e informes suplementarios. La interposición de esta denuncia es independiente de las eventuales comunicaciones o notificaciones a organismos de control a las que se esté obligado en virtud del Real Decreto 3/2010, de 8 de enero, del Reglamento (UE) 2016/679, de la Ley 8/2011, de 28 de abril o de otra normativa que requiera estas notificaciones.	

Código Seguro De Verificación	aJGtx0PCr50V0RS1JI4BYA==	Estado	Fecha y hora
Firmado Por	Irene Garcia Gonzalez-Posada	Firmado	03/11/2023 15:05:20
Observaciones		Página	34/34
Url De Verificación	https://firma.fundacioncomplutense.com/verifirma/code/aJGtx0PCr50V0RS1JI4BYA%3D%3D		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

