

# **STIC-PROC\_001: Procedimiento de Gestión de Ciberincidentes**

---

Procedimientos de Seguridad de las Tecnologías  
de la Información y las Comunicaciones,  
Universidad de Zaragoza



(Página en blanco intencionadamente)





## Ficha de control documental

Información del documento	
Archivo	20230829 - STIC-PROC_01: Procedimiento.de.Gestión.de.Ciberincidentes.v2.2 [Versión.Pública]
Autor/es	Víctor Pérez Roche, Francisca Baldira, Pascual Pérez
Creado	08/07/2021
Actualizado	19/03/2024
Versión	v2.0 (Borrador)
Clasificación	Público
Aprobación	VIII CSIPD – 20/03/2024

Documentos asociados
<a href="#">Estado de la Seguridad IT en la Universidad de Zaragoza</a>
<a href="#">Guía: Buenas prácticas en la Gestión de Crisis de Ciberseguridad – CCN-CERT</a>
<a href="#">Guía de Seguridad de las TIC - CCN-STIC 817</a>

Registro de cambios			
Versión	Fecha	Autor	Descripción
v0.1	08/07/2021	Víctor Pérez Roche	Versión inicial del documento
v0.2	01/12/2021	Víctor Pérez Roche	Retirada de la Fase 0
v0.3	15/12/2021	Víctor Pérez Roche, Pascual Pérez	Matriz de contacto y varias correcciones
v0.4	13/01/2022	Francisca Baldira, Víctor Pérez Roche	Inclusión de todos los aspectos relacionados con protección de datos personales y revisión de los puntos tratados en la 9ª Reunión del Comité de Seguridad
v1.0	28/04/2022	Comité de Seguridad	Aprobación de la versión v1.0
V2.0	29/08/2023	Víctor Pérez Roche	Modificación del título del



			documento Revisión general del documento para alinearlo a la guía CCN-STIC 817 Inclusión de la obligación de comunicación a terceros potencialmente implicados
V2.1	18/03/2024	Víctor Pérez Roche	Adecuación con el documento de Buenas Prácticas del CCN-CERT Generalización de las tecnologías utilizadas.
V2.2	20/03/2024	Víctor Pérez Roche	Versión aprobada por el CSIPD



Control de revisiones			
Fecha	Revisado por	Área	Próxima revisión
20/03/2024	Comité de Seguridad	n/a	



# Procedimiento de Gestión de Ciberincidentes

Introducción.....	6
Ámbito de aplicación.....	6
Agentes implicados.....	6
Notificación de incidentes a terceros.....	9
Procedimiento.....	10
Fase 1: Detección/Notificación.....	10
Fase 2: Evaluación del impacto.....	10
Fase 3: Activación Comité de Crisis.....	15
Fase 4: Contención.....	18
Fase 5: Plan de comunicación notificaciones.....	18
Fase 6: Análisis.....	20
Fase 7: Erradicación.....	21
Fase 8: Recuperación.....	21
Fase 7: Post-Incidente.....	22
Registro de incidentes.....	22
Matriz de contacto de los roles implicados.....	23

## Introducción

En el presente documento se recoge el Procedimiento de Gestión de Ciberincidentes de la Universidad de Zaragoza. Terminológicamente se entenderán sinónimos ciberincidente y ciber crisis, aunque se admite que este último puede tener un ámbito de alcance mayor que el del ciberincidente. De forma específica se valorará la respuesta ante un compromiso de tipo HOR - Human Operated Ransomware.

Este documento contempla igualmente en este mismo contexto, el plan de actuación en caso de que el ciberincidente afecte a información que contenga datos de carácter personal y ocasione una brecha de seguridad, de acuerdo con lo dispuesto en el Reglamento General de Protección de Datos (RGPD).

## Ámbito de aplicación

Este procedimiento es de obligado cumplimiento para toda la comunidad universitaria y el personal con algún tipo de relación con la Universidad de Zaragoza (terceros).

## Agentes implicados

- **Rector:** Máximo responsable de la Universidad. Preside el Comité de Crisis personalmente o por delegación.



- **Responsable de la Información:** Es responsable de la Información la Secretaria General de la Universidad.
- **Responsable de los Servicios:** Es responsable de los Servicios el Gerente de la Universidad de Zaragoza.
- **Responsable de Seguridad:** Es Responsable de Seguridad el Vicegerente de Tecnologías de la Información y la Comunicación.

Es el primer conocedor del incidente y debe determinar si es preciso trasladarlo o no al Comité de Crisis. Tiene responsabilidades sobre la notificación de forma inmediata al CERT de referencia. Determina cuáles son las primeras acciones operativas para su contención

Le corresponde supervisar y coordinar la investigación de los incidentes de seguridad, desde su comunicación hasta su resolución. También la supervisión de las operaciones de registro del incidente.

- **Responsable de Comunicación:** Es la persona responsable de la comunicación de la Universidad

Le corresponde en caso de incidente de seguridad transmitir la información relativa a dicho incidente a la Comunidad Universitaria y en el caso de que sea preciso, al resto de la sociedad. Decide cuáles son los mensajes clave, el formato y el canal más adecuado, en función de los grupos de interés. Activa el seguimiento y repercusión de la crisis en los diferentes medios de comunicación y redes sociales Mantiene el contacto con los medios de comunicación

- **Usuarios de los Sistemas:** Son usuarios todas aquellas personas que tienen acceso controlado a los sistemas de información de la UZ incluyendo todos aquellos relacionados con los tratamientos de datos de carácter personal de los que sea responsable, corresponsable o encargada del tratamiento la Universidad de Zaragoza.

Les corresponde notificar al Servicio de Informática y Comunicaciones (SICUZ), de manera inmediata, todos los incidentes de seguridad detectados en la utilización de los mismos, incluyendo aquellos que afecten a equipos personales utilizados para la gestión administrativa, académica o científica.

- **Equipo de Continuidad:** Forman parte del Equipo de Continuidad los técnicos encargados de la realización de guardias de monitorización de los Sistemas.

Le corresponde detectar fallos de funcionamiento que pudieran deberse a incidentes de seguridad.

- **Técnicos del CAU:** Son Técnicos del Centro de Atención a Usuarios.

Pueden ser el primer canal técnico capaz de detectar un ciberincidente en sus estadios iniciales.

- **Administradores de los Sistemas:** Son Administradores de los Sistemas el personal con capacidad de actuación sobre los mismos.



Les corresponde aplicar las medidas técnicas a fin de garantizar la resolución del incidente.

- **Responsables Internos de los Servicios TIC:** Son responsables internos de los Servicios TIC aquellas personas con capacidad técnica de decisión sobre los mismos.

Para Servicios TIC de Información dependientes del SICUZ esta figura será llevada a cabo por los Directores de Área.

En el caso de tratamientos de carácter personal autorizados por la Universidad de Zaragoza tienen dicha consideración, a estos efectos, las personas que hayan sido designadas por el gerente como responsables internos de cada tratamiento de datos.

Corresponde al Responsable Interno de cada Servicio TIC llevar a cabo la evaluación preliminar del incidente y decidir cómo proceder de cara a su resolución.

- **Jefe de Proyecto de Seguridad de la Información:** Es el técnico informático perteneciente al SICUZ y encargado de hacer seguimiento y colaborar en la implementación y mantenimiento de las medidas de seguridad aplicables a los sistemas de información de la Universidad.

Le corresponde contactar con las partes implicadas, coordinar la resolución, registrar el incidente, realizar el informe de seguridad y comunicar a quien corresponda el fin del incidente si fuera necesario.

- **Terceros:** Se consideran terceros todas aquellas personas individuales, empresas o entidades externas que tengan acceso a los sistemas de información de la UZ (bien sea como proveedores de servicios informáticos, proveedores de servicios de internet o fabricantes de soluciones de seguridad, organismos públicos, empresas etc.).

Se consideran también terceros, a estos efectos, todos aquellos que en virtud de contrato, convenio o acuerdo tengan acceso a los tratamientos de datos personales de los que la Universidad tenga la consideración legal de responsable, corresponsable o encargada del tratamiento.

Les corresponde notificar a la Universidad, de manera inmediata o en el plazo más breve posible, los incidentes de seguridad detectados en la utilización de los sistemas y/o en los tratamientos de datos personales.

- **Delegado/a de Protección de Datos:** Es la persona designada por el Rector para llevar a cabo las funciones legalmente encomendadas a los Delegados de Protección de Datos.

Le corresponde informar y asesorar al responsable/encargado del tratamiento sobre sus obligaciones y responsabilidades con relación a los incidentes de seguridad que afecten a datos personales.

Le corresponde también actuar como punto de contacto con la Agencia Española de Protección de Datos (AEPD) y cooperar con ella en las cuestiones relativas a la gestión de dichos incidentes.



- **Comité de Crisis:** Comité dinámico conformado por los Agentes implicados en la gestión de un incidente de seguridad de acuerdo al nivel de categorización del mismo.

Le corresponde conocer el análisis preliminar del incidente, concretar las acciones inmediatas de contención, evaluar el riesgo (en particular determinar si afecta o no a datos personales y, si fuera así, si puede tener o no consecuencias sobre los derechos y libertades de los afectados) y acordar las medidas adecuadas para restaurar y asegurar el acceso, confidencialidad, integridad, trazabilidad, autenticidad, disponibilidad y conservación de los datos, informaciones y servicios afectados.

## Notificación de incidentes a terceros

- **Centro Criptológico Nacional (CCN):** Se notificarán al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información de acuerdo con lo dispuesto en la normativa reguladora del Esquema Nacional de Seguridad (ENS) y en el Real Decreto-Ley 12/2018, de 7 de septiembre, conforme al procedimiento establecido en la correspondiente Instrucción Técnica de Seguridad
  - Los mecanismos de contacto con el CCN-CERT son:
    - A través de la herramienta LUCIA, que se encuentra federada por la Universidad de Zaragoza
    - A través del correo electrónico [incidentes@ccn-cert.cni.es](mailto:incidentes@ccn-cert.cni.es)
- **Instituto Nacional de Ciberseguridad (INCIBE):** Sin perjuicio de la notificación al CCN, los terceros de carácter privado deberán notificar también los incidentes que afecten a los servicios que presten a la UZ.
  - El mecanismo de contacto con el INCIBE es a través de la siguiente URL:
    - <https://www.incibe-cert.es/notificaciones>
- **Agencia Española de Protección de Datos (AEPD):** Cuando el incidente de seguridad comporte una brecha de seguridad que afecte a los tratamientos de datos personales y que pueda suponer un riesgo para los derechos y libertades de las personas físicas, se notificará a la Agencia Española de Protección de Datos (AEPD) de acuerdo con lo dispuesto en el art. 33 RGPD, conforme al procedimiento establecido.
  - El mecanismo de notificación a la AEPD es a través de esta URL:
    - <https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/nbs/guiadoBrechasInicio.jsf>
- **Sujetos afectados:** Cuando sea probable que la brecha de seguridad entrañe un alto riesgo para los derechos y libertades de las personas físicas afectadas, comprometiendo la confidencialidad, integridad y/o disponibilidad de esos datos, se comunicará a los afectados de acuerdo con lo dispuesto en el art. 34 RGPD, conforme al procedimiento establecido
  - Los mecanismos de comunicación a los sujetos afectados se adecuarán a la gravedad de la brecha de seguridad, y a la capacidad de notificación por parte de la Universidad.



## Procedimiento

### Fase 1: Detección/Notificación

Esta fase abarca todos los aspectos relacionados con la detección y posterior notificación por parte del Agente que haya podido detectar el incidente. El objetivo es lograr aislar el posible ciberincidente en el menor tiempo posible, y transmitir la información asociada cuanto antes.

- **Ciberincidentes detectados por Usuarios:** Tan pronto tengan constancia de un incidente de seguridad deberán comunicarlo creando un parte en <https://cau.unizar.es>, informando con el mayor detalle del servicio afectado, modo de acceso al mismo, momento del incidente y toda la información que considere relevante y que permita reproducir el incidente. En este caso la atención de los Técnicos del CAU es vital, para evaluar posibles ciberincidentes de gravedad y colaborar en la obtención de información de contexto de los usuarios necesaria de acuerdo a los Procedimientos Técnicos Específicos.
- **Incidentes detectados por los Técnicos de Continuidad y/o los Administradores del Sistema:** Tan pronto tengan constancia de una incidencia de seguridad deberán comunicarla a los Directores de Área implicados y al Responsable de Seguridad de la Información a través de teléfono o sistema de mensajería. Esta comunicación deberá de ser fehacientemente verificada.
- **Incidentes detectados por entidades externas o terceros,** incluidos los distintos organismos de gestión de seguridad como el Instituto Nacional de Ciberseguridad (INCIBE), el Centro Criptológico Nacional (CCN-CERT), Fuerzas y Cuerpos de Seguridad del Estado etc.: Podrán reportar a la Universidad de Zaragoza dichas incidencias mediante correo electrónico a la dirección [abuse@unizar.es](mailto:abuse@unizar.es), utilizando el sistema federado LUCIA o como consideren oportuno.

Además de las posibles formas de detección anteriores, la Universidad de Zaragoza cuenta con sistemas de detección automática de ciberincidentes, basados en:

- Sistema SIEM
- Firewalls perimetrales
- Sistemas de análisis de métricas de Disponibilidad
- Servicio de protección de DDoS
- Sistemas de registro de actividad de usuario y casos de uso

### Fase 2: Evaluación del impacto

Los **Responsables internos de Servicios TIC** implicados, en colaboración con el **Técnico de Continuidad**, evaluarán la gravedad del incidente de acuerdo a la siguiente matriz:

Nivel	Descripción
Nivel 1	Compromiso de uno o varios Servicios IT sin interacción de un agente externo,



	<p>como por ejemplo:</p> <ul style="list-style-type: none"><li>• Pérdida de disponibilidad accidental o no provocada.</li><li>• Compromiso de bajo impacto de cualquiera de las otras dimensiones</li></ul> <p>Ejemplos de ciberincidentes de Nivel 1:</p> <ul style="list-style-type: none"><li>• Fallo de disponibilidad de un Servicio IT</li><li>• Compromiso por virus/gusano de un equipo no crítico.</li><li>• Escaneo de la red</li></ul> <p>Declaración de Crisis: No</p> <p>Ámbito de Gestión/Gobierno de la Crisis:</p> <ul style="list-style-type: none"><li>• No requiere Comité de Crisis</li><li>• Activa:<ul style="list-style-type: none"><li>◦ Equipo de Continuidad</li><li>◦ Responsables Internos de los Servicios TIC afectados</li><li>◦ Administradores de los Sistemas afectados</li></ul></li></ul>
Nivel 2	<p>Compromiso o intento de compromiso de uno o varios servicios con interacción de agentes externos que impliquen:</p> <ul style="list-style-type: none"><li>• Impacto menor sobre alguna de las dimensiones de un Servicio IT de forma provocada.</li><li>• Publicación no intencionada de datos personales</li></ul> <p>Ejemplos de ciberincidentes de Nivel 2:</p> <ul style="list-style-type: none"><li>• Acceso no autorizado a un Servicio IT</li><li>• Compromiso de un Servicio IT por una vulnerabilidad</li><li>• Robo de credenciales de usuarios no privilegiados</li><li>• Intentos de phishing</li><li>• Intento de Denegación de Servicio.</li></ul> <p>Declaración de Crisis: No</p> <p>Ámbito de Gestión/Gobierno de la Crisis:</p> <ul style="list-style-type: none"><li>• No requiere Comité de Crisis</li></ul>



	<ul style="list-style-type: none"><li>• Activa BRONZE TEAM:<ul style="list-style-type: none"><li>◦ Responsable de la Seguridad de la Información</li><li>◦ Jefe de Proyectos de Seguridad de la Información</li><li>◦ Equipo de Continuidad</li><li>◦ Responsables Internos de los Servicios TIC afectados</li><li>◦ Administradores de los Sistemas afectados</li><li>◦ Delegado de Protección de Datos (en el caso de que el incidente incluya este tipo de información)</li></ul></li></ul>
Nivel 3	<p>Compromiso de uno o varios servicios con interacción de agentes externos que impliquen:</p> <ul style="list-style-type: none"><li>• Suplantación de la identidad de personal Universitario</li><li>• Suplantación de Servicios IT legítimos</li><li>• Acceso no autorizado a información de usuarios</li><li>• Modificación de datos con finalidad económica menor</li><li>• Brecha de datos personales</li></ul> <p>Ejemplos de ciberincidentes de Nivel 3:</p> <ul style="list-style-type: none"><li>• Acceso a buzones de personal de la Universidad, suplantación de la identidad de los mismos.</li><li>• Acciones sobre los Servicios IT con una motivación económica menor.</li><li>• Intentos de <i>spear phishing</i> dirigidos a personal con funciones directivas o responsabilidades críticas.</li><li>• <i>Defacement</i> de una web institucional</li><li>• Ataque de secuestro de datos - ransomware – en un Servicio no crítico.</li></ul> <p>Declaración de Crisis: Opcional</p> <p>Ámbito de Gestión/Gobierno de la Crisis:</p> <ul style="list-style-type: none"><li>• Requiere Comité de Crisis</li><li>• Activa SILVER TEAM:<ul style="list-style-type: none"><li>◦ Responsable de la Seguridad de la Información</li><li>◦ Jefe de Proyectos de Seguridad de la Información</li></ul></li></ul>



	<ul style="list-style-type: none"><li>○ Equipo de Continuidad</li><li>○ Responsables Internos de los Servicios TIC afectados</li><li>○ Administradores de los Sistemas afectados</li><li>○ Delegado de Protección de Datos (en el caso de que el incidente incluya este tipo de información).</li><li>○ Responsable de Comunicación</li></ul>
Nivel 4	<p>Compromiso de uno o varios servicios con interacción de agentes externos que impliquen:</p> <ul style="list-style-type: none"><li>● Compromiso de la disponibilidad de varios servicios críticos</li><li>● Suplantación de la identidad de personal de alta calificación o responsabilidad.</li><li>● Suplantación de Servicios IT críticos</li><li>● Modificación de información en Servicios IT</li><li>● Robo de datos de usuarios</li><li>● Brecha de datos personales sensibles</li></ul> <p>Ejemplos de ciberincidentes de Nivel 4:</p> <ul style="list-style-type: none"><li>• Acceso a información confidencial.</li><li>• Modificación de información.</li><li>• Incidente de carácter económico muy grave</li><li>• Ransomware sobre uno o varios sistemas críticos.</li></ul> <p>Declaración de Crisis: Si</p> <p>Ámbito de Gestión/Gobierno de la Crisis:</p> <ul style="list-style-type: none"><li>• Requiere Comité de Crisis</li><li>• Activa SILVER TEAM:<ul style="list-style-type: none"><li>○ Responsable de la Información</li><li>○ Responsable de los Servicios</li><li>○ Responsable de la Seguridad de la Información</li><li>○ Jefe de Proyectos de Seguridad de la Información</li></ul></li></ul>



	<ul style="list-style-type: none"><li>○ Equipo de Continuidad</li><li>○ Responsables Internos de los Servicios TIC afectados</li><li>○ Administradores de los Sistemas afectados</li><li>○ Delegado de Protección de Datos (en el caso de que el incidente incluya este tipo de información).</li><li>○ Responsable de Comunicación</li></ul>
Nivel 5	<p>Compromiso masivo de los Servicios IT de la Universidad de Zaragoza</p> <ul style="list-style-type: none"><li>● Compromiso masivo de la disponibilidad de los Servicios IT Univesitarios</li><li>● Suplantación muy grave de personal</li><li>● Suplantación de Servicios IT críticos</li><li>● Acceso/Modificación de información crítica</li><li>● Robo masivo de datos de usuarios</li><li>● Brecha masiva de datos personales sensibles</li></ul> <p>Ejemplos de ciberincidentes de Nivel 5:</p> <ul style="list-style-type: none"><li>• Destrucción masiva de Servicios e Información, así como de sus mecanismos de respaldo.</li><li>• Robo de información crítica</li><li>• Modificación de información crítica.</li><li>• Incidente de carácter económico muy grave</li></ul> <p>Declaración de Crisis: Si</p> <p>Ámbito de Gestión/Gobierno de la Crisis:</p> <ul style="list-style-type: none"><li>• Requiere Comité de Crisis</li><li>• Activa GOLD TEAM:<ul style="list-style-type: none"><li>○ Rector</li><li>○ Responsable de la Información</li><li>○ Responsable de los Servicios</li><li>○ Responsable de la Seguridad de la Información</li><li>○ Jefe de Proyectos de Seguridad de la Información</li></ul></li></ul>



	<ul style="list-style-type: none"><li>○ Equipo de Continuidad</li><li>○ Responsables Internos de los Servicios TIC afectados</li><li>○ Administradores de los Sistemas afectados</li><li>○ Delegado de Protección de Datos (en el caso de que el incidente incluya este tipo de información).</li><li>○ Responsable de Comunicación</li></ul>
--	---

En esta fase se tendrá en cuenta si el incidente ha producido una afectación a los datos personales tratados ocasionando su destrucción, pérdida o alteración accidental o ilícita o la comunicación o acceso no autorizado a dichos datos. Se seguirá para ello la metodología descrita por la AEPD en la guía: [“Gestión del riesgo y evaluación de impacto en tratamientos de datos personales”](#)

En este sentido, NO tendrán la consideración de brechas de datos personales sujetas a los arts. 33 y 34 del Reglamento General de Protección de Datos (RGPD) aquellos incidentes de seguridad que:

- No afecten a datos personales; es decir, que no sean personas físicas identificadas o identificables.
- No afecten a tratamientos de datos personales llevados a cabo por la Universidad de Zaragoza ya sea en calidad de responsable, corresponsable o de encargada del tratamiento.

### Fase 3: Activación Comité de Crisis

Una vez confirmado el incidente de seguridad, y atendiendo a su clasificación, se procederá a la constitución de un **Comité de Crisis** adecuado a la naturaleza del incidente a gestionar:

Nivel	Descripción de los agentes implicados	Canales de comunicación
N1	<ul style="list-style-type: none"><li>● Equipo de continuidad</li><li>● Administradores de Sistema implicados</li><li>● Responsables Internos de Servicio implicados</li></ul>	<ul style="list-style-type: none"><li>● Mensajería instantánea</li></ul>
N2	<ul style="list-style-type: none"><li>● Responsable de la Seguridad de la Información</li></ul>	<ul style="list-style-type: none"><li>● Mensajería instantánea</li><li>● Videconferencia habilitada de forma</li></ul>



	<ul style="list-style-type: none"><li>● Jefe de Proyectos de Seguridad de la Información</li><li>● Equipo de Continuidad</li><li>● Responsables Internos de los Servicios TIC afectados</li><li>● Administradores de los Sistemas afectados</li><li>● Delegado de Protección de Datos (en el caso de que el incidente incluya este tipo de información)</li></ul>	permanente hasta la resolución del ciberincidente.
N3	<ul style="list-style-type: none"><li>● Responsable de la Seguridad de la Información</li><li>● Jefe de Proyectos de Seguridad de la Información</li><li>● Equipo de Continuidad</li><li>● Responsables Internos de los Servicios TIC afectados</li><li>● Administradores de los Sistemas afectados</li><li>● Delegado de Protección de Datos (en el caso de que el incidente incluya este tipo de información).</li><li>● Jefa del Gabinete del Rector</li><li>● Responsable de Comunicación</li><li>● Apoyo externo de empresa, según la gravedad del incidente</li></ul>	<ul style="list-style-type: none"><li>● Mensajería instantánea</li><li>● Videconferencia habilitada de forma permanente hasta la resolución del ciberincidente.</li><li>● Comunicación de la situación a la Comunidad Universitaria por los canales que el Gabinete de Comunicación estime adecuados.</li><li>● Comunicación al CERT de referencia</li><li>● Comunicación a la AEPD si procede</li></ul>
N4	<ul style="list-style-type: none"><li>● Responsable de la Información</li><li>● Responsable de los Servicios</li><li>● Responsable de la Seguridad de la Información</li><li>● Jefe de Proyectos de Seguridad de la Información</li><li>● Equipo de Continuidad</li><li>● Responsables Internos de los Servicios TIC afectados</li><li>● Administradores de los Sistemas afectados</li><li>● Delegado de Protección de Datos (en el caso de que el incidente incluya este tipo de información).</li><li>● Jefa del Gabinete del Rector</li><li>● Responsable de Comunicación</li><li>● Apoyo externo de empresa, según la gravedad del incidente</li></ul>	<ul style="list-style-type: none"><li>● Mensajería instantánea</li><li>● Videconferencia habilitada de forma permanente hasta la resolución del ciberincidente.</li><li>● Comunicación de la situación a la Comunidad Universitaria por los canales que el Gabinete de Comunicación estime adecuados.</li><li>● Comunicación al CERT de referencia</li><li>● Comunicación a la AEPD si procede</li></ul>



N5	<ul style="list-style-type: none"><li>● Rector</li><li>● Responsable de la Información</li><li>● Responsable de los Servicios</li><li>● Responsable de la Seguridad de la Información</li><li>● Jefe de Proyectos de Seguridad de la Información</li><li>● Equipo de Continuidad</li><li>● Responsables Internos de los Servicios TIC afectados</li><li>● Administradores de los Sistemas afectados</li><li>● Delegado de Protección de Datos (en el caso de que el incidente incluya este tipo de información).</li><li>● Jefa del Gabinete del Rector</li><li>● Responsable de Comunicación</li><li>● Apoyo externo de empresa, según la gravedad del incidente</li></ul>	<ul style="list-style-type: none"><li>● Mensajería instantánea</li><li>● Videconferencia habilitada de forma permanente hasta la resolución del ciberincidente.</li><li>● Comunicación de la situación a la Comunidad Universitaria por los canales que el Gabinete de Comunicación estime adecuados.</li><li>● Comunicación al CERT de referencia</li><li>● Comunicación a la AEPD si procede</li></ul>
----	---	--

Por defecto en cada comité el liderazgo en la operativa IT estará a cargo del Responsable de Seguridad asesorado por el resto de los integrantes del comité o, en el Nivel 1, por el Director de Área responsable del servicio afectado

En las incidencias de Nivel 3 o superior, en función de la naturaleza y gravedad de la incidencia, será el Rector, o persona en quien delegue, quien presidirá el Comité de Crisis.

Sea cual sea el nivel de la incidencia, cuando afecte a datos de carácter personal, se convocará al Comité de Crisis al Delegado/a de Protección de Datos.

Una vez detectado el incidente y su Nivel se procederá a efectuar y documentar la evaluación de los riesgos que comporta para los sistemas de información y/o para la seguridad de los datos personales, estableciendo las medidas de contención que se estimen adecuadas para gestionar el incidente.

#### Factores para evaluar el riesgo de una brecha de datos personales

- Tipo de brecha
- Naturaleza, carácter sensible o no y volumen de los datos afectados
- Facilidad de identificación de las personas afectadas
- Gravedad de las consecuencias para los derechos y libertades de las personas afectadas
- Número de personas afectadas
- Características particulares del responsable del tratamiento
- Consideraciones Generales



## Fase 4: Contención

Una vez aislada la situación y con los miembros del Comité de Crisis activos - o al menos aquellos con capacidad operativa - se procederá a poner en marcha las contramedidas de contención que pueden implicar:

### Nivel 1-3:

- Bloqueo en el FW perimetral de los sistemas externos que puedan estar implicados.
- Pausado – no apagado - de las máquinas virtuales afectadas.
- Desconexión de la red de los sistemas afectados en caso de que no sean virtuales
- Bloqueo de los usuarios comprometidos
  - Bloqueo de credenciales Administrativas
  - Bloqueo de credenciales de Correo
  - Bloqueo de servicios

### Nivel 4-5:

- **Desconexión completa de la red:** Ante una situación de compromiso muy grave de servicios donde no se conoce con seguridad el vector de ataque habría que desconectar toda la red de la Universidad. Posteriormente se podría proveer de servicios básicos de acceso a Internet para los equipos universitarios como:
  - DNS
  - Salida a internet de redes de usuarios

## Fase 5: Plan de comunicación notificaciones

Nota: Esta fase – aunque se sitúe en este punto - se identifica como transversal a la duración de todo el proceso de gestión del ciberincidente.

De acuerdo a la naturaleza del compromiso, especialmente en casos de:

- Robo masivo de información
- Ransomware
- Otros compromisos de gravedad

Se deberán de realizar comunicaciones con la siguiente responsabilidad:

Responsable	Destinatario
Responsable de Seguridad	<b>Gerencia de la Universidad</b> a través de Teléfono/Mensajería instantánea.  <b>Terceras partes implicadas</b> <ul style="list-style-type: none"><li>• Organismos o empresas que puedan verse afectados por el ciberincidente, ya sea por sus datos o sus sistemas.</li></ul>
Responsables	<b>Personal del SICUZ</b> a través del canal de Telegram de Contingencia



Internos de Servicios	SICUZ
Jefe de Proyecto de Seguridad de la Información	<b>CERT de referencia (CCN-CERT)</b> <ul style="list-style-type: none"><li>○ Apertura de un ticket de Incidencia en LUCIA - Responsable Jefe de Proyecto de Seguridad de la Información</li><li>○ Comunicación telefónica</li></ul>
Gerente/ Delegado de Protección de Datos	<b>Agencia Española de Protección de Datos (AEPD):</b> <ul style="list-style-type: none"><li>● Cuando el incidente afecte a datos personales y sea probable que constituya un riesgo para los derechos y libertades de las personas afectadas.</li><li>● Cumplimentación del <b>formulario de Notificación de brechas</b> de datos personales establecido por la AEPD en su Sede Electrónica o modelo que lo sustituya.</li><li>● El plazo de notificación será dentro de las <b>72 horas siguientes</b> desde que se haya tenido conocimiento del incidente (incluyendo las horas transcurridas durante fines de semana y festivos).</li><li>● Si en el momento de la notificación se dispone ya de toda la información y documentación relevante para la gestión y resolución del incidente, incluida la decisión sobre la comunicación o no de la misma a los afectados, se realizará una <b>notificación “completa”</b></li><li>● De no ser así, podrá efectuarse una <b>notificación “inicial”</b> antes de las 72 horas con la información preliminar que se disponga. Antes del plazo máximo de 30 días hábiles desde dicha notificación se completará toda la información sobre la incidencia mediante una <b>“modificación” de la notificación anterior</b> que incluirá, junto con la información y documentación relevante, la decisión tomada sobre comunicación o no a los afectados.</li></ul>
Gerente/ Delegado de Protección de Datos	<b>Responsable del tratamiento de datos personales</b> <ul style="list-style-type: none"><li>● Cuando la Universidad de Zaragoza sea encargada del tratamiento por cuenta de un tercero, se procederá a notificar a éste el incidente acaecido, junto con toda la información que sea relevante.</li><li>● La notificación, deberá realizarse sin dilación indebida dentro del plazo establecido en el documento de encargo de tratamiento.</li></ul>



	<ul style="list-style-type: none"><li>● Sólo si en el documento de encargo así se hubiera establecido, procederá además notificarlo a la AEPD.</li></ul>
Gerente/ Delegado de Protección de Datos	<p><b>Comunicación a las Personas afectadas</b></p> <ul style="list-style-type: none"><li>● Cuando tras la evaluación efectuada se considere probable que el incidente entrañe un alto riesgo para los derechos y libertades de los afectados o bien sea por la pérdida de confidencialidad, integridad o disponibilidad de los datos (como por ej., daños reputacionales o exposición a fraudes), por la irreversibilidad de los mismos, etc.</li><li>● No será necesaria esta comunicación si se han adoptado medidas de protección que mitigan total o parcialmente el posible impacto y se estime que ya no hay posibilidad de afectación (Por ej., revocando o bloqueando credenciales de acceso o certificados digitales comprometidos; restablecimiento de los servicios y copias de seguridad, etc).</li><li>● Se utilizará la herramienta Comunica-Brecha RGPD de la AEPD como ayuda para la toma de decisiones a este respecto.</li></ul>
Jefe de Gabinete de Comunicación	<ul style="list-style-type: none"><li>● <b>Comunidad Universitaria</b><ul style="list-style-type: none"><li>○ Información en la Web Corporativa</li><li>○ Información a través de la cuenta de Twitter @unizar</li></ul></li><li>● <b>Comunicación externa a la Universidad</b><ul style="list-style-type: none"><li>○ Redes y medios de comunicación social</li></ul></li></ul>

## Fase 6: Análisis

- **Auditoría de los sistemas afectados:**
  - Si está encendido<sup>1</sup>:
    - No se Apaga
    - Volcado de memoria RAM
    - Listado de conexiones abiertas
    - Listado de procesos activos
    - Listado de usuarios logueados en el sistema
    - Listado de ficheros abiertos
    - [Se puede proceder al apagado del sistema]

<sup>1</sup> La desconexión de la red puede realizarse a distintos niveles, como norma general se realizará en el entorno de vmware o en el FW perimetral.



- Si se considera necesario se realizará una imagen de los sistemas de ficheros afectados
- Revisión con un antivirus Live de los sistemas de ficheros afectados
- Recolección de muestras de ficheros maliciosos.
- Si está apagado
  - No se enciende
  - Si se considera necesario se realizará una imagen de los sistemas de ficheros afectados
  - Revisión con un antivirus Live de los sistemas de ficheros afectados
  - Recolección de muestras de ficheros maliciosos, validación con el servicio de Virustotal
- **Revisión de registros de actividad**
  - Revisión de actividad de las direcciones IP de los Sistemas Internos afectados
  - Revisión de actividad de las direcciones IP de los Sistemas Externos implicados
  - Revisión de la actividad de los usuarios potencialmente comprometidos

## Fase 7: Erradicación

Durante la fase de erradicación se buscará retirar de la red o limitar todos los recursos afectados, lo que puede incluir:

- Eliminación de servicios, binarios, archivos de configuración de los Servicios IT comprometidos.
- Eliminación de Servicios IT completos vulnerados tanto internos como externos.
- Actualización de Servicios IT potencialmente vulnerables
- Limpieza de sistemas de usuario potencialmente comprometidos

## Fase 8: Recuperación

El plan concreto de recuperación tendrá que ser desarrollado por el Comité de Crisis y adecuado a cada caso en concreto atendiendo a la naturaleza del incidente, podrá incluir posteriores análisis del incidente, y probablemente requiera de procesos de recuperación de Backup.

El liderazgo y la coordinación del plan de recuperación será llevada a cabo por el Responsable de Seguridad o de forma delegada en alguno de los Responsables Internos de los Servicios implicados. Las responsabilidades operativas en el plan de recuperación recaerá en los Directores de Área implicados, junto con sus técnicos.

Se deberá trabajar sobre el inventario de activos - listado de servicios - para evaluar cuales están afectados y cuáles no, y desarrollar un plan de recuperación.



## Fase 7: Post-Incidente

En la etapa post-incidente se realizará la recopilación sistemática y exhaustiva de los detalles del ciberincidente, incluyendo las lecciones aprendidas y los obstáculos enfrentados durante su resolución. Como resultado de este análisis se pretende obtener un plan de mejoras sobre los procesos de gestión del ciberincidente, mecanismos de detección, contención, análisis y respuesta, todos ellos orientados a fortalecer las defensas de la organización en el futuro.

El informe final del ciberincidente deberá de incluir como mínimo:

- Nivel de peligrosidad
- Resumen de las acciones realizadas para:
  - Análisis del incidente
    - Línea temporal
    - Análisis de Servicios IT afectados
    - Vector de compromiso
    - Vulnerabilidades explotadas
    - Técnicas utilizadas
  - Contención del incidente
  - Erradicación del incidentes
  - Recuperación de los sistemas afectados
- Impacto del incidente
- Efectividad de los protocolos de respuesta, posibles fallos y mejoras.
- Medidas de mejora propuestas

## Registro de incidentes

Se registrarán todas las actuaciones relacionadas con la gestión de incidentes incluyendo:

- Todos los reportes iniciales, intermedios y finales, las actuaciones de emergencia y las modificaciones del Sistema derivadas del incidente.
- Se registrarán aquellas evidencias que puedan dirimirse en un ámbito jurisdiccional, especialmente cuando el incidente pueda comportar acciones sobre el personal interno (por ej. disciplinarias), sobre terceros externos (por ej. proveedores y prestadores de servicios, terceros encargados del tratamiento de datos, etc.), o en la persecución de delitos. También cuando el incidente haya comportado una brecha de datos personales.
- Las notificaciones practicadas al CCN-CERT y, en su caso, al INCIBE-CERT.
- Las notificaciones practicadas a la AEPD y, en su caso, a los afectados en los supuestos de brechas de seguridad de datos personales.



El registro de toda la información de las citadas actuaciones será responsabilidad del Jefe de Proyecto de Seguridad de la Información

## Relación de contactos de los roles implicados

[El contenido de este epígrafe ha sido eliminado de esta versión pública del documento]