STIC-PROC_01: Procedimiento de Actuación frente a Incidentes Lógicos

---

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

Servicio de
Informática
y Comunicaciones
Universidad Zaragoza

(Página en blanco intencionadamente)

Ficha de control documental

Información del documento	
Archivo	20210708 - STIC-PROC_01: Procedimiento.de.Actuación.Incidente.Lógico [Versión.Pública]
Autor/es	Víctor Pérez Roche, Francisca Baldira, Pascual Pérez
Creado	08/07/2021
Actualizado	14/09/2022
Versión	v1.0 (Pública)
Clasificación	Público
Aprobación	28 de Marzo de 2022, Comité de Seguridad

Documentos asociados
Estado de la Seguridad IT en la Universidad de Zaragoza
Guía: Buenas prácticas en la Gestión de Crisis de Ciberseguridad - CCN-CERT

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 actual redacción

Control de revisiones			
Fecha	**Revisado por**	**Área**	**Próxima revisión**
28/04/2022	Comité de Seguridad	n/a	

Servicio de Informática y Comunicaciones
Universidad Zaragoza

Protocolo de actuación en caso de incidente lógico

Introducción

En este documento se recoge el plan de actuación en caso de compromiso de carácter lógico de un o varios Sistemas o Servicios de la Universidad de Zaragoza, y de forma específica se valora la respuesta ante un compromiso de tipo HOR - Human Operated Ransomware.

Se contempla también el plan de actuación en caso de que el incidente 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 UZ (terceros).

Agentes implicados

- **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.

- **Técnicos de Continuidad:** Son Técnicos de Continuidad el personal encargado de la realización de guardias de monitorización de los Sistemas.

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

- **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.

- **Responsable de Seguridad**: Es Responsable de Seguridad el Vicegerente de Tecnologías de la Información y la Comunicación.

  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.

- **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.

- **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.

- **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
- **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 detectar el posible problema lógico en el menor tiempo posible, y transmitir la información asociada cuanto antes.

- **Incidentes detectados por Usuarios**: Tan pronto tengan constancia de un incidente de seguridad deberán comunicarlo creando un parte en https://ayudica.unizar.es (Incidencias de seguridad y privacidad), 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.

- **Incidentes detectados por l**os **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 Vicegerente TIC, a través de los medios adecuados a la gravedad de la misma (teléfono, canal de Telegram, etc).

- **Incidentes detectados por entidades externas o terceros**, incluídos los distintos organismos de gestión de seguridad como el Instituto Nacional de Ciberseguridad (INCIBE), el Centro Criptológico Nacional (CCN), 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, utilizando el sistema federado LUCIA o como consideren oportuno.

Más allá de la detección de incidencias por parte de agentes, la detección automática de incidentes de seguridad se basa actualmente en los siguientes sistemas de monitorización, que nos permitirían conocer un fallo en la dimensión de la disponibilidad de alguno de los servicios:

- UptimeRobot: Monitoriza algunos sistemas desde el exterior
- PandoraFMS: Dispone de más de 7000 monitores sobre muchos sistemas.

Hay que tener en cuenta que estos sistemas de monitorización **no son específicos** para por ejemplo detectar un ataque de ransomware - ej. que afecte a los contenidos de psfunizar0 o equipos de usuario - ya que eso no afectaría a ninguno de los servicios actualmente monitorizados.

El equipo de continuidad - operadores - puede tener dificultades para llevar a cabo una detección en un tiempo breve debido a:

- Solamente cubre una franja horaria
- No dispone de suficientes conocimientos para poder hacer esta detección

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 sin actuación de agentes externos ya sea: ● De modo accidental o fortuito (como pérdida de un dispositivo) ● Mediante una metodología automatizada (como un. Virus, un Bot o un Gusano). Un ejemplo sería la corrupción de una base de datos, o la infección por un virus automatizado.
Nivel 2	Compromiso de uno o varios Servicios con actuación de agentes externos. Un ejemplo sería el *defacement* o compromiso de un servidor Web, un ransomware sobre un Servicio no crítico o una brecha de datos personales que no afecte a datos de especial protección ni, de modo significativo, a los derechos y libertades de los interesados.
Nivel 3	Compromiso muy grave de Servicios. Un ejemplo sería un compromiso masivo de Servicios críticos (Moodle, Correo, Identidad, eAdmon, …) o una brecha de seguridad de datos personales que afecte a datos de especial protección y, de modo significativo, a los derechos y libertades de los interesados.

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 integrantes del Comité de Crisis	Canales de comunicación
N1	• Técnicos de continuidad • Administradores de Sistema implicados • Responsables Internos de Servicio implicados	• Canal de Telegram • Meet permanente de seguimiento de la incidencia
N2	• Técnicos de continuidad • Administradores de Sistema implicados • Responsables Internos de Servicio implicados. • Jefe de Proyecto de Seguridad de la Información • Responsable de Seguridad • Jefa del Gabinete del Rector • Responsable de Comunicación • Apoyo externo de empresa, según la gravedad del incidente	• Canal de Telegram • Meet permanente de seguimiento de la incidencia • Comunicación de la situación a la Comunidad Universitaria por los canales que el Gabinete de Comunicación estime adecuados.
N3	• Técnicos de continuidad • Administradores de Sistema implicados	• Canal de Telegram • Meet permanente de seguimiento de la incidencia

	• Todos los Responsables Internos de Servicio • Jefe de Proyecto de Seguridad de la Información • Responsable de Seguridad • Jefa del Gabinete del Rector • Responsable de Comunicación • Gerencia de la Universidad • Secretario General • Apoyo externo de empresa	• Comunicación de la situación a la Comunidad Universitaria por los canales que el Gabinete de Comunicación estime adecuados.

Por defecto en cada comité el liderazgo en la operativa IT estará a cargo del Vicegerente TIC 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, 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: Contramedidas de contención iniciales

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:

- **Desconexión de la red de los sistemas que integran el servicio afectado**[1] en caso de sospecha de un agente automatizado externo - ej. C2 de una Botnet
    - Bloqueo del rango de IPs del servicio afectado en el FW para la salida y la entrada
    - Desconexión de las máquinas virtuales
- **Auditoría de los sistemas afectados**:
    - Si está encendido[2]:
        - 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]
        - 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[3]
    - 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 la actividad de red** de los Servicios afectados en las franjas de compromiso y previas
    - NetFlow
    - PaloAlto
- **Implantación de medidas de protección** en los FW perimetrales de todos los IOC - direcciones IP - externos.
    - Revisión de los IOC en el resto de la red en las 24 últimas horas

Nivel 2:

- **Desconexión de la red** del servicio o servicios afectados

[1] 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.
[2] Proyecto WinTriaje para UNIZAR
[3] http://www.virustotal.com

    - Bloqueo del rango de IPs del servicio afectado en el FW para la salida y la entrada
    - Desconexión de las máquinas virtuales
- **Auditoría** con el mismo procedimiento descrito para Nivel 1
    - Revisión de los IOC en el resto de la red en las 48 últimas horas

Nivel 3:

- **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
- **Auditoría** con el mismo procedimiento descrito para Nivel 1/2

Fase 5: Plan de comunicación notificaciones

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
VG TIC	**Gerencia de la Universidad** a través de Teléfono/WhatsApp
Responsables Internos de Servicios	**Personal del SICUZ** a través del canal de Telegram de Contingencia SICUZ
Jefe de Proyecto de Seguridad de la Información	**CERT de referencia (CCN-CERT)** ○ Apertura de un ticket de Incidencia en LUCIA - Responsable Jefe de Proyecto de Seguridad de la Información ○ Comunicación telefónica
Gerente/ Delegado de Protección de Datos	**Agencia Española de Protección de Datos (AEPD)**:

	• Cuando el incidente afecte a datos personales y sea probable que constituya un riesgo para los derechos y libertades de las personas afectadas. • Cumplimentación del **formulario de Notificación de brechas** de datos personales establecido por la AEPD en su Sede Electrónica o modelo que lo sustituya. • El plazo de notificación será dentro de las **72 horas siguientes** desde que se haya tenido conocimiento del incidente (incluyendo las horas transcurridas durante fines de semana y festivos). • Si en el momento de la notificación se dispone ya de toda la información y documentación relevante para la gestión y resolución del incidente, incluída la decisión sobre la comunicación o no de la misma a los afectados, se realizará una **notificación "completa"** • De no ser así, podrá efectuarse una **notificación "inicial"** 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 **"modificación" de la notificación anterior** que incluirá, junto con la información y documentación relevante, la decisión tomada sobre comunicación o no a los afectados.
Gerente/ Delegado de Protección de Datos	**Responsable del tratamiento de datos personales** • 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. • La notificación, deberá realizarse sin dilación indebida dentro del plazo establecido en el documento de encargo de tratamiento. • Sólo si en el documento de encargo así se hubiera establecido, procederá además notificarlo a la AEPD.
Gerente/ Delegado de	**Comunicación a las Personas afectadas**

Protección de Datos	● 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. ● 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). ● Se utilizará la herramienta Comunica-Brecha RGPD de la AEPD como ayuda para la toma de decisiones a este respecto.
Jefe de Gabinete de Comunicación	● **Comunidad Universitaria** ○ Información en la Web Corporativa ○ Información a través de la cuenta de Twitter @unizar ● **Comunicación externa a la Universidad** ○ Redes y medios de comunicación social

Fase 6: Plan de 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 VG-TIC 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: 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

Matriz de contacto de los roles implicados

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