NP.01 NORMAS DE GESTIÓN DE INCIDENCIAS

Documento de uso interno

ÌNDICE

1 Objetivo 4
2 Ámbito de aplicación 4
3 Vigencia, revisión y evaluación 4
4 Agentes y responsabilidades 5
5 Normativa 6
5.1 Definición de incidente de seguridad de la información 6
5.2 Clasificación de incidentes de seguridad 7
5.3 Comunicación interna del incidente 12
5.4 Registro 12
5.5 Gestión de los incidentes 13
5.6 Aprendizaje 13
5.7 Recopilación de evidencias 14
5.8 Concienciación, formación y difusión 15
5.9 Denuncias 15
6 Desarrollo de la normativa 15
7 Referencias 16

CONTROL DE VERSIONES

Revisión	Fecha	Motivo del Cambio
0.1	05/02/2026	Borrador

Realizado y revisado Responsable de Seguridad Fecha	Aprobado ComSeg Fecha

1 Objetivo

Conforme a lo dispuesto en el Real Decreto 311/2022, de 3 de mayo (que sustituye a los anteriores: Real Decreto 3/2010, de 8 de enero y Real Decreto 951/2015, de 23 de octubre), por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), este documento contiene las **Normas de gestión de incidencias**, para definir la normativa aplicable a la gestión de incidentes de la Universidad de Extremadura (en adelante UEx).

Se ha implantado la siguiente normativa atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas de la UEx, que resulten de la aplicación de las previsiones contempladas en los Anexos I y II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), en concreto, las establecidas por el apartado "Explotación [op.exp]" y "Monitorización del sistema [op.mon]".

2 Ámbito de aplicación

Esta normativa general se aplica a todo el ámbito de actuación de la UEx, y sus contenidos traen causa de las directrices de carácter más general definidas en la **Política de Seguridad de la Información** de la UEx (aprobada en Consejo de Gobierno el 25 de mayo de 2023, publicada en el DOE de 8 de junio de 2023).

La presente Normativa de gestión de incidentes es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios o trabaje internamente en la UEx, incluyendo el personal de proveedores externos, cuando sean usuarios de los Sistemas de Información de la UEx.

En el ámbito de la presente normativa, se entiende por **usuario** cualquier empleado público perteneciente o ajeno a la UEx así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con la UEx y que utilice o posea acceso a los Sistemas de Información de la UEx.

3 Vigencia, revisión y evaluación

La presente Normativa ha sido aprobada por el Comité de Seguridad de la UEx, estableciendo de esta forma las directrices generales para la gestión de incidentes de seguridad.

Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la UEx. Las versiones anteriores que hayan podido distribuirse constituyen borradores que se han desarrollado temporalmente, por lo que su vigencia queda anulada por la última versión de esta Normativa.

La gestión de esta Normativa corresponde al Comité de Seguridad que es competente para:

- 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 ello.
- Verificar su efectividad.

Anualmente (o con menor periodicidad, si existen circunstancias que así lo aconsejen), el Comité de Seguridad revisará la presente Normativa, que se someterá, de haber modificaciones, a aprobación.

Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

4 Agentes y responsabilidades

Será competencia del Responsable de Seguridad velar por el cumplimiento de la presente normativa, realizando un seguimiento de las incidencias ocurridas.

ROLES	RESPONSABILIDADES
Responsable de Seguridad de la Información	Gestionar esta normativa para: • Interpretar las dudas que puedan surgir en su aplicación. • Verificar su efectividad. • Proceder a su revisión, siempre que sea necesario actualizar sus contenidos o, al menos, anualmente.
Grupo de Respuesta a Incidentes en los Sistemas de Información	Notificar a la autoridad competente en materia de seguridad de las redes y sistemas de información, concretamente a su equipo de respuesta a incidentes de seguridad informática (CSIRT o CERT), los incidentes de seguridad de la información, en los casos y en los términos que determine la normativa aplicable.
Centro de Atención de Usuarios (CAU)	Registrar los potenciales incidentes de seguridad de los que puedan ser notificados. Registrar e l cierre de los tiques cuando el Responsable de la Información o Responsable de Tratamiento de datos personales que pueda verse afectado lo determine. Atender las posibles peticiones que realicen los Responsables de Información y Responsables de Tratamiento de Datos Personales durante los Planes de Actuación. Mantener la debida confidencialidad de cualquier incidente durante todo el proceso y posteriormente.

Delegado de protección de datos	Gestionar aquellos incidentes de seguridad que afecten a datos personales responsabilidad de la Organización. Notificar a la autoridad de control y partes afectadas, en función del alcance de la brecha de datos personales. Asesorar al Responsable del Tratamiento sobre la oportunidad y modo de notificar los incidentes de seguridad sobre datos de carácter personal. Asesorar al Responsable del Tratamiento sobre la oportunidad y modo de informar a las personas interesadas y afectadas por violaciones de la seguridad de sus datos personales.
Usuarios	Cumplir con su obligación de notificar los incidentes de seguridad que detecten en el entorno de trabajo, o cualquier situación que pueda provocarlas.

5 Normativa

5.1 Definición de incidente de seguridad de la información

Se considera incidente de seguridad de la información o ciberincidente aquel evento o serie de eventos de seguridad de la información, inesperados o no deseados por UEx que tengan una probabilidad significativa de comprometer las operaciones de la organización y amenazar la seguridad de la información en cualquiera de las siguientes seis dimensiones: Disponibilidad, Autenticidad, Integridad, Confidencialidad, Trazabilidad y Privacidad.

Dimensión	Descripción
Disponibilidad	Un incidente de seguridad TIC afecta a la disponibilidad si una persona usuaria autorizada no puede acceder a la información cuando la necesita.
Autenticidad	Un incidente de seguridad afecta a la autenticidad si una entidad no es quien dice ser, o bien las fuentes de la que proceden los datos no son auténticas.
Integridad	Un incidente de seguridad de la información afecta a la integridad si la información ha sido alterada de manera no autorizada.
Confidencialidad	Un incidente de seguridad de la información afecta a la confidencialidad si la información es revelada a personas no autorizadas o a personas que no necesitan conocer la información.
Trazabilidad	Un incidente de seguridad de la información afecta a la trazabilidad si no se puede imputar las actuaciones de una entidad exclusivamente a dicha entidad.
Privacidad	Un incidente de Seguridad de la información afecta a la privacidad si vulnera el derecho a la intimidad, al honor o a la propia imagen o a la protección de dato s de carácter personal de las personas interesadas.

5.2 Clasificación de incidentes de seguridad

La clasificación de incidentes aplicada por la UEx se hará conforme a la taxonomía detallada en la siguiente tabla (siguiendo las guías de referencia del CCN):

Clase de incidente	Tipo de incidente	Descripción y Ejemplos
Contenido abusivo	Spam	Correo electrónico masivo no solicitado. El receptor del contenido no ha otorgado autorización válida para recibir un mensaje colectivo.
	Delito de odio	Contenido difamatorio o discriminatorio. Ej: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
	Pornografía infantil, contenido sexual o violento inadecuado	Material que represente de manera visual contenido relacionado con pornografía infantil, apología de la violencia, etc.
Contenido dañino	Sistema infectado	Sistema infectado con malware. Ej: Sistema, computadora o teléfono móvil infectado con un rootkit.
	Servidor C&C (Mando y Control)	Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Distribución de malware	Recurso usado para distribución de malware. Ej: recurso de una organización empleado para distribuir malware.
	Configuración de malware	Recurso que aloje ficheros de configuración de malware Ej: ataque de webinjects para troyano.
Obtención de información	Escaneo de redes (scanning)	Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos, servicios y cuentas. Ej: peticiones DNS, ICMP, SMTP, escaneo de puertos.

	Análisis de paquetes (sniffing)	Observación y grabación del tráfico de redes.
	Ingeniería social	Recopilación de información personal sin el uso de la tecnología. Ej: mentiras, trucos, sobornos, amenazas.
Intento de intrusión	Explotación de vulnerabilidades conocidas	Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).
	Intento de acceso con vulneración de credenciales	Múltiples intentos de vulnerar credenciales. Ej: intentos de ruptura de contraseñas, ataque por fuerza bruta.
	Ataque desconocido	Ataque empleando exploit desconocido.
Intrusión	Compromiso de cuenta con privilegios	Compromiso de un sistema en el que el atacante ha adquirido privilegios.
	Compromiso de cuenta sin privilegios	Compromiso de un sistema empleando cuentas sin privilegios.
	Compromiso de aplicaciones	Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ej: inyección SQL.
	Robo	Intrusión física. Ej: acceso no autorizado a Centro de Proceso de Datos.
Disponibilidad	DoS (Denegación de servicio)	Ataque de denegación de servicio. Ej: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
	DDoS (Denegación distribuida de servicio)	Ataque de denegación distribuida de servicio. Ej: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.

	Mala configuración	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.
	Sabotaje	Sabotaje físico. Ej: cortes de cableados de equipos o incendios provocados.
	Interrupciones	Interrupciones por causas ajenas. Ej: desastre natural
Compromiso de la información	Acceso no autorizado a información	Acceso no autorizado a información. Ej: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
	Modificación no autorizada de información	Modificación no autorizada de información. Ej: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.
	Pérdida de datos	Pérdida de información Ej: pérdida por fallo de disco duro o robo físico.
Fraude	Uso no autorizado de recursos	Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej: uso de correo electrónico para participar en estafas piramidales.
	Derechos de autor	Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej: Warez.
	Suplantación	Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.

	Phishing	Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.
Vulnerable	Criptografía débil	Servicios accesibles públicamente que puedan presentar criptografía débil. Ej: servidores web susceptibles de ataques POODLE/FREAK.
	Amplificador DDoS	Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej: DNS open resolvers o Servidores NTP con monitorización monlist.
	Servicios con acceso potencial no deseado	Ej: Telnet, RDP o VNC
	Revelación de información	Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej: SNMP o Redis.
	Sistema vulnerable	Sistema vulnerable. Ej: mala configuración de proxy en Universidad de Extremadura (WPAD), versiones desfasadas de sistema.
Otros	Otros	Todo aquel incidente que no tenga cabida en ninguna categoría anterior.
	APT	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

5.3 Comunicación interna del incidente

Cuando se produzca una incidencia de seguridad de la información, habrá que tener en cuenta las siguientes consideraciones:

- Todos los usuarios (tanto internos como externos a la UEx) deben ser informados y concienciados sobre la responsabilidad de notificar las incidencias de seguridad de forma inmediata, así como sobre los procedimientos y canales de comunicación disponibles para ello. Cualquier usuario que tenga conocimiento de una incidencia o debilidad de seguridad deberá notificarla de forma inmediata a través de los canales y destinatarios establecidos por la UEx.
- El canal de notificación para usuarios es el Centro de Atención al Usuario (CAU) de la UEx (https://cau.unex.es). Si no fuese posible acceder a dicho servicio, se notificará en el teléfono de atención del propio servicio 924 28 93 18 (extensión 89318), o bien a través de correo electrónico a cau@unex.es. En el caso de notificación telefónica o por correo, será el propio Técnico del CAU que recibe la notificación quien la registrará en la aplicación.
- Adicionalmente a la notificación de incidencias y debilidades de seguridad por parte de los usuarios, existen otras fuentes para la detección de incidencias de seguridad, como puede ser la monitorización de los sistemas de información, las alertas del sistema y otras vulnerabilidades que puedan ser detectadas dentro de los sistemas de información de la UEx.
- Los canales establecidos y el sistema de notificación de incidencias deben presentar el formato adecuado para incluir toda la información necesaria para facilitar la gestión y trazabilidad de la incidencia, sirviendo de herramienta de apoyo para el desarrollo de las actividades de reporte y resolución de incidencias.

5.4 Registro

En el registro de las incidencias de seguridad, habrá que tener en cuenta las siguientes consideraciones:

- Todas las incidencias de seguridad deben tener un número único que permita su identificación y trazabilidad a lo largo del proceso de gestión. Este número facilitará tanto el almacenamiento y registro de la incidencia como la búsqueda de incidencias.
- Toda la información relacionada con las causas, tratamiento y resolución de incidencias de seguridad debe registrarse junto con las evidencias, logs y trazas obtenidas sobre esta.
- La información registrada debe almacenarse y protegerse de forma que no pueda modificarse (incluso por los administradores del sistema).
- El registro de los logs y trazas, así como otros registros y evidencias adjuntos a la incidencia deben cumplir con los requerimientos legales, contractuales y los relativos la normativa interna de la UEx.

- En caso de que la incidencia afecte a ficheros que contengan datos de carácter personal, se debe evaluar e informar al Responsable de Seguridad y al DPD.

5.5 Gestión de los incidentes

En la gestión de las incidencias de seguridad, habrá que tener en cuenta las siguientes consideraciones:

- Las incidencias deben ser clasificadas de acuerdo con los criterios de clasificación que se consideren más adecuados para la UEx, para permitir ofrecer la respuesta más adecuada en cada caso.
- Los responsables de la gestión de las incidencias deberán recabar de los usuarios toda la información necesaria para gestionar la incidencia.
- En caso de verse afectados datos personales de los tratamientos gestionados por la UEx (tanto donde ostenta la figura de Responsable del Tratamiento como Encargado), el Responsable de Seguridad debe valorar su gravedad e informar al Delegado de Protección de Datos.
- Deben establecerse las responsabilidades y procesos necesarios para garantizar una respuesta rápida, efectiva y ordenada a las incidencias y debilidades de seguridad.
- En determinados casos será necesario adoptar medidas para la contención de la incidencia que eviten daños mayores. Cuando la adopción de estas medidas de contención conlleve una paralización de los sistemas de usuario se debe informar con antelación a los usuarios afectados mediante los canales de comunicación establecidos.
- En los casos de incidencias graves o en las que sea necesario activar el Plan de Contingencias, las incidencias deben ser comunicadas de forma inmediata al Responsable de Seguridad, que debe decidir las acciones a adoptar en cada caso (entre ellas la activación del Plan de Contingencias o la convocatoria del Comité de Seguridad para informar de los hechos).
- La resolución de la incidencia debería ser comunicada a los usuarios que la han reportado o que fueron afectados durante su gestión, para proceder al cierre definitivo de la misma.

5.6 Aprendizaje

En el aprendizaje de las incidencias de seguridad, habrá que tener en cuenta las siguientes consideraciones:

- La gestión y registro de las incidencias de seguridad deben revisarse periódicamente para identificar la causa o problema subyacente de estas y las soluciones adoptadas, identificar posibles deficiencias de seguridad o proponer las soluciones más adecuadas. Se debería

revisar elaborar un informe donde se establezcan las conclusiones de las revisiones realizadas.

- La evaluación de las incidencias de seguridad de la información indica que hay que aumentar o añadir nuevos controles que limiten la frecuencia, daño o coste de futuras incidencias o pueden considerarse como fuente de información dentro de los procesos de revisión de las políticas de seguridad.
- El responsable y los operadores de incidencias, así como en su caso los usuarios afectados deben ser formados y prevenidos sobre la base de conocimiento adquirido, y sobre posibles incidencias que puedan repetirse en el futuro para prevenir que éstas vuelvan a producirse. Así, salvando la confidencialidad de la gestión de incidencias, las incidencias deben utilizarse en los procesos de mejora continua como ejemplo para la concienciación y formación de usuarios y administradores del sistema ante incidencias similares para prevenirse su reaparición en el futuro.

5.7 Recopilación de evidencias

Cuando el seguimiento de una actuación contra una persona u organización, tras un incidente grave o desastre, conlleve la interposición de acciones legales (civiles o penales), disciplinarias o de responsabilidad contractual, las evidencias del incidente deben recolectarse, archivarse y presentarse según la legislación aplicables para la admisibilidad de pruebas dentro del orden jurisdiccional aplicable o de los procesos contractualmente definidos.

Con el fin de asegurar y preservar la admisibilidad de las evidencias en un proceso judicial se han de tener en cuenta las siguientes consideraciones:

- Se debe desarrollar un **procedimiento interno de recolección de evidencias** que determine los pasos a seguir por la UEx para la recolección y presentación de evidencias que tienen como fin facilitar el desarrollo y defensa de las acciones disciplinarias, judiciales o de reclamación de responsabilidades que puedan emprenderse por la UEx. Este procedimiento debe contener:
    - Las pautas más importantes a seguir en la recogida de evidencias, estableciendo los controles necesarios para la trazabilidad de las actuaciones realizadas en esta etapa y los controles a implementar dentro del proceso posterior de custodia de las evidencias para contrastar su integridad y completitud al aportarlas como prueba en los procesos correspondientes.
    - Las medidas de seguridad a adoptar en el caso de la aparición de actividades ilícitas por parte de personal interno y de cara a prevenir actuaciones de destrucción de pruebas o de represalias del personal investigado contra la UEx.

- Se debe disponer de herramientas de monitorización y gestión y registro de evidencias que cuentan con los requisitos necesarios para monitorizar, registrar y almacenar toda actividad dentro de los sistemas de información de la UEx desde el primer momento en que una evidencia se genera, permitiendo así establecer una cadena de custodia que garantice la integridad y completitud de las evidencias recogidas de cara a posibles procesos que puedan surgir posteriormente. No obstante, lo anterior, la UEx también podrá solicitar los servicios de **consultores de seguridad y asesores legales expertos en la materia**, que le asesoren de cara a poder llevar una investigación del hecho de forma eficaz, así como para facilitar la admisibilidad de las evidencias provistas dentro de las diferentes jurisdicciones aplicables.

5.8 Concienciación, formación y difusión

El Comité de Seguridad de la Información de la UEx, en coordinación con otros órganos realizará acciones de concienciación, formación y difusión de esta normativa y del procedimiento de gestión de incidentes de seguridad, abarcando, al menos, las responsabilidades que la normativa asigna en materia de seguridad, los conceptos básicos sobre incidentes de seguridad y los mecanismos de notificación interna.

5.9 Denuncias

El procedimiento de gestión de incidentes de seguridad contemplará la gestión específica de aquellos incidentes que puedan ser constitutivos de delito, recogiendo aspectos como la interposición de denuncias policiales y siguiendo el protocolo de actuación que se determinen al respecto.

6 Desarrollo de la normativa

Con relación a la gestión de incidencias, la UEx realiza las siguientes actividades:

- Se ha desarrollado un **procedimiento de gestión de los incidentes de seguridad de la información (PS.06 Gestión de incidentes)** en el que se detallen los pasos a seguir para la notificación, valoración y respuesta ante las incidencias y debilidades de seguridad de la información, así como las que afecten a datos de carácter personal.
- Se ha implantado una plataforma o sistema para la gestión de incidencias que permita su recogida, registro y gestión conforme al **procedimiento de Gestión de Incidentes**. Este sistema permite garantizar una respuesta adecuada, organizada y eficaz a las incidencias que se puedan producir, mejorando su control e impidiendo que alguna incidencia pueda quedar sin respuesta.
- Se gestionan las incidencias de seguridad de la información que transcienden los límites de la UEx. En base a ello, se debería incluir, dentro de los Contratos de Prestación de Servicios con

terceros, cláusulas donde se establezcan los medios de comunicación y respuesta de incidentes y debilidades de seguridad, de forma tal forma que se pueda proporcionar una respuesta coordinada y una distribución de información que permita una eficaz gestión y resolución de estas.

7 Referencias

Esta Norma se apoya y se ve complementada por las siguientes referencias:

Internas:

- PO.01 Política de Seguridad de la Información de la Universidad de Extremadura.
- NG.01 Normativa General de Utilización de los Recursos y Sistemas de Información.
- PS.06 Procedimiento de Gestión de incidentes.
- Otras por definir.

Externas:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).
- UNE - ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la información.
- UNE - ISO/IEC 27001:2007 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información.
- ISO/IEC 9001:2000 Sistemas de gestión de la calidad.
- Guías de seguridad de las TIC CCN-STIC Serie 800.