EL PUESTO DE TRABAJO

Medidas de protección II

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

UNIVERSIDAD DE SEVILLA

crue Universidades Españolas

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
www.incibe.es

ÍNDICE

1. BUENAS PRÁCTICAS

En el seno de toda institución es común que haya una serie de protocolos sobre cómo el personal debe utilizar los recursos de la universidad para realizar su trabajo. Con la información, los soportes y los dispositivos electrónicos, no es diferente. Todos tenemos que conocer estas buenas prácticas y aplicarlas para cuidar de los recursos y proteger los intereses de la universidad.

1.1. Documentación sensible

Debido a la actividad de la universidad es común que en ciertas situaciones el personal haga uso de **información sensible**, por ejemplo, datos de estudiantes, docentes, nóminas, etc.

Por ello, gestionar esta información, de manera adecuada, es imprescindible, ya que un acceso no autorizado a la misma puede suponer un grave perjuicio para la universidad.

Como ya se indicó en el recurso formativo anterior, cuando este tipo de documentación se encuentra en formato físico, debe quedar **guardada en un lugar seguro** al finalizar la jornada laboral. Pero, ya se encuentre en formato digital o en formatos tradicionales, **únicamente** debe estar **accesible para el personal autorizado**, bien sea por medio de permisos de usuario o por cualquier otro método que evite miradas indiscretas.

En ciertas ocasiones, bien sea por descuido o por olvido esta documentación sensible puede quedar abandonada en las impresoras y escáneres de la universidad. El personal ha de prestar especial atención cuando se utiliza este tipo de dispositivos.

El almacenamiento de documentación también puede estar externalizado en un proveedor dedicado a la custodia documental. En el caso de que exista este servicio se ha de establecer un acuerdo de confidencialidad y se comprobará que la información está correctamente custodiada.

La destrucción de la información al terminar su ciclo de vida también es un proceso crítico, que si no se realiza correctamente puede derivar en una fuga de información. Cuando se destruye información que contiene datos sensibles o confidenciales, debe hacerse de forma segura utilizando destructoras de papel o por medio de empresas especializadas que ofrezcan garantías.

1.2. Contrato de confidencialidad

En muchas ocasiones, bien sea por la necesidad de externalizar servicios o por proteger la información de la universidad, se deben establecer acuerdos de confidencialidad, es decir que se deberán firmar acuerdos si se trata con información confidencial. **Este tipo de acuerdos sentarán las bases de la relación que se establecerá entre ambas partes fijando los compromisos que se adquieren mutuamente, en el caso de externalizar los servicios.**

Si en la universidad se trata información cuya confidencialidad debe estar garantizada, se han de incluir varias cláusulas en los contratos como:

- indicar qué información se considera confidencial y por lo tanto está protegida por el acuerdo;
- fijar la duración de la relación de confidencialidad, que generalmente será superior al tiempo de prestación del servicio;
- en caso de ser necesario, se indicará la jurisdicción legal a la que se acoge cada una de las partes.

1.3. Uso adecuado de Internet y sistemas corporativos

Los dispositivos y recursos que la universidad ofrece están pensados para que sean utilizados para los fines de la institución. Por tanto, no deben ser usados para cuestiones personales o en circunstancias que puedan afectar a la seguridad de la universidad.

Internet ofrece multitud de recursos que pueden ser aprovechados por los usuarios para usos no profesionales en su tiempo o lugar de trabajo o desde sus dispositivos profesionales, pero estos usos también esconden riesgos. **Acceder a sitios de dudosa legitimidad como webs de descargas, juego, adultos, etc., no es un uso lícito de los recursos institucionales,** pues no solo disminuye la eficiencia de estos recursos y puede ocasionar gastos innecesarios, sino que puede acarrear daños irreparables para la universidad. Muchos de esos sitios pueden no ser seguros o contar con publicidad que puede llevar a situaciones de confusión, resultando en un incidente de seguridad, como una infección por malware del dispositivo o de toda la red.

Al igual que sucede con Internet, los recursos de la universidad como impresoras, escáneres, ordenadores, teléfonos, etc., deben ser tratados solamente para tareas institucionales y no ser alterados si no estamos autorizados para ello.

1.4. Software legítimo

Las normas de protección de la propiedad intelectual obligan a las universidades a usar en todo momento software legal. El uso de **«programas piratas» o adquiridos de forma fraudulenta podría conllevar sanciones económicas y penales**, nunca se debe instalar software sin licencia en ningún dispositivo de la universidad.

Además, por norma general, instalar **software ilegal puede terminar en una infección por malware del equipo,** bien sea por los anuncios de las webs de descargas, porque el programa ha sido modificado añadiendo código malicioso; o porque se requiere de un crack para que funcione, que también podrá estar infectado.

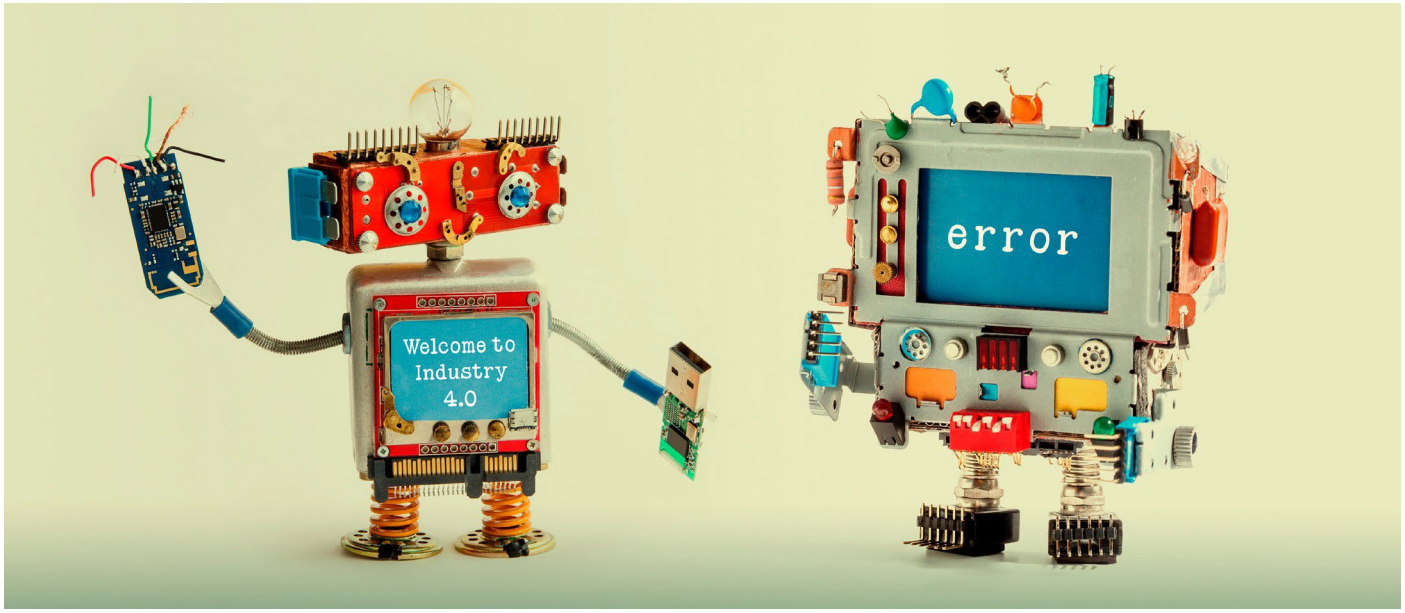
1.5. Cómo y cuándo reportar un incidente de seguridad

Si sufrimos un incidente que pudiera afectar a la seguridad de la universidad, el primer paso que tenemos que dar es **analizar qué ha pasado.** De esta manera, conociendo el tipo de incidente se podrá medir más eficazmente la repercusión en la institución y cómo actuar. Una clasificación posible de los incidentes es la siguiente:

- **acceso no autorizado** a sistemas o información, como en el caso de robo de un dispositivo o de las credenciales de acceso
- **denegaciones de servicio,** en las cuales el incidente impide el correcto funcionamiento de un recurso, como por ejemplo la página web de la universidad
- **infección por malware**
- **robo de información de la universidad**

Una vez conozcamos qué ha pasado, lo siguiente que tenemos que hacer es avisar al personal de la universidad, encargados del tema de seguridad de la información para que estén informados de lo sucedido. Por ejemplo si hay fuga de información de carácter personal, lo pondremos en conocimiento del responsable que deba comunicarlo a los afectados y **a los organismos oficiales dedicados a la seguridad de la información.**

En caso de que el incidente suponga un delito (falsificación, injurias y calumnias, daños de propiedad intelectual, sabotaje, piratería, estafa, robo de identidad, etc.) es recomendable **interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado** aportando toda la información que se pueda de lo sucedido.



1.6. Uso seguro de dispositivos de almacenamiento extraíble

Los dispositivos de almacenamiento extraíbles como memorias USB, discos duros portátiles, tarjetas de memoria, CD, etc., permiten una transferencia rápida y directa de información. Hoy en día son muy utilizados, por ello **tenemos que minimizar las situaciones de riesgo** como robo, manipulación, extravío e infección por virus.

En primer lugar, **si su uso está permitido en la universidad,** en caso de que así sea, debemos saber en qué **situaciones se pueden utilizar** y qué **información se puede llevar en estos dispositivos.** Una buena práctica cuando se necesita almacenar en estos dispositivos información sensible o confidencial consiste en **cifrar la información.** También tendremos que estar atentos ante cualquier incidente como robo o pérdida de dispositivos con este tipo de información para informar de forma inmediata al responsable.

Otro aspecto importante es asegurarse de que la información que contienen los dispositivos que vamos a desechar o reutilizar, una vez es borrada, no vuelva a ser accesible, para ello se utilizarán **métodos seguros de borrado y destrucción de soportes.**