Universidad Veracruzana

LA INFORMACIÓN

Un activo esencial de tu universidad

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

metared

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

www.incibe.es

ÍNDICE

1. LA IMPORTANCIA DE LA INFORMACIÓN

La información en las universidades es esencial para llevar a cabo los distintos procesos que se producen en ella: gestión académica, investigaciones, procesos administrativos, información sobre campus, etc. El almacenamiento, tratamiento y gestión de la información, en formato digital o en otros formatos son las actividades que conforman los llamados **sistemas de información** que soportan estos procesos. Estos sistemas incluyen también los datos, los recursos materiales (tradicionales, como el bolígrafo y el papel, o tecnológicos) y las personas necesarias para realizar esas actividades.

ACADÉMICAS

ADMINISTRATIVAS

INVESTIGACIÓN

DIFUSIÓN

Actividades de los sistemas de información

ALMACENAMIENTO

TRATAMIENTO

GESTIÓN

1. LA IMPORTANCIA DE LA INFORMACIÓN

La información también es un activo de la universidad: tangible e intangible

TANGIBLE	INTANGIBLE
Ordenadores	Know-How
Dispositivos de almacenamiento	Reputación
Teléfonos móviles	Propiedad Intelectual

Si hablamos de los activos que componen estos sistemas de información, es fácil identificar, en primer lugar, aquellos más tangibles como ordenadores, dispositivos de almacenamiento, teléfonos móviles, etc. Sin embargo, no se debe olvidar que existen otros **activos de información, también esenciales para la universidad, que son intangibles** como el know-how de los docentes, estudiantes y personal administrativo, la reputación, el software, o la propiedad intelectual.

Es lógico pensar que la información es un recurso esencial para cualquier organización, más aún en aquellas que proveen servicios basados en el conocimiento, como las universidades.

Por ello, es un aspecto fundamental incidir en que **las universidades deben preocuparse por su información,** pues de no estar disponible, alterarse o difundirse sin consentimiento podría afectar la continuidad de la institución. Si la información sobre nuestros procesos como institución, los datos personales y académicos de nuestros estudiantes, docentes y personal de administración, o detalles sobre proyectos de investigación cayeran en manos ajenas las consecuencias podrían ser muy negativas para nuestra actividad y nuestra reputación.

Las universidades deben preocuparse por su información

1. LA IMPORTANCIA DE LA INFORMACIÓN

A la protección de los activos de información frente a las amenazas que puedan afectar a su disponibilidad, integridad o confidencialidad la denominamos **seguridad de la información**. Los incidentes de seguridad que afectan a la información de la universidad pueden ser:

Accidentales

Los sucesos no intencionados son la causa de muchos incidentes. Algunos ejemplos son: borrado de un archivo que pensabas que ya no servía, enviar un correo a un destinatario erróneo o sencillamente una avería en el disco duro.

Intencionados por parte de miembros de la comunidad universitaria o insiders

En ocasiones son los propios miembros de la comunidad universitaria los que deciden llevarse o modificar información de la universidad, causar infecciones o facilitar el acceso a terceros. Lo hacen por motivos propios, es paradigmático el cambio de notas o sustracción de exámenes, o bajo la influencia o el soborno de ciberdelincuentes. Un insider puede causar muchos incidentes pues tiene fácil acceso a la información de la universidad. En particular, los robos o fugas de información son fáciles de realizar dado el reducido tamaño de los dispositivos de almacenamiento extraíble y su creciente capacidad, la accesibilidad a los servicios de almacenamiento en la nube o debido al acceso generalizado al correo electrónico.

Causados por ciberdelincuentes

Utilizando códigos maliciosos o malware que introducen aprovechando debilidades de nuestros sistemas y en ocasiones nuestra ingenuidad o falta de preparación, como cuando utilizan ingeniería social para conseguir el acceso. El malware puede robar información como es el caso de los troyanos o hacerla inaccesible para su propietario al que extorsionan pidiendo un rescate como hacen los llamados ransomware **[Ref. - 1]**, o hacer que nuestro equipo esté a las órdenes de una botnet que realiza cualquier actividad delictiva.

Por tanto, es muy importante que se adopten las decisiones y medidas necesarias antes de que se produzca un incidente de seguridad que afecte a la información de tu universidad.

3. REFERENCIAS

1. INCIBE - Protege tu empresa – Herramientas - Servicio AntiRansomware - https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware

2. INCIBE - Protege tu Empresa - ¿Qué te interesa? - Protección de la información - https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

3. Agencia Española de Protección de Datos - https://www.aepd.es/index.html

4. INCIBE - Protege tu Empresa – Blog – Artículos filtro: Protección de la información - https://www.incibe.es/protege-tu-empresa/blog/filtro/proteccion-informacion

5. INCIBE - Protege tu Empresa – Guías - Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario - https://www.incibe.es/protege-tu-empresa/guias/ganar-competitividad-cumpliendo-el-rgpd-guia-aproximacion-el-empresario

6. INCIBE - Protege tu Empresa – Blog - Historias reales: mi trabajo robaron y mi proyecto plagiaron - https://www.incibe.es/protege-tu-empresa/blog/historias-reales-mi-trabajo-robaron-y-mi-proyecto-plagiaron