



Tecnológico Nacional de
México

Instituto Tecnológico de
Reynosa

Materia: Modelos de negocio y
outsourcing

Maestro: Ileana Deyanira Trejo García

Título: Portafolio Unidad #4 Legislación de
la información y propiedad intelectual

Fecha de entrega: 17/11/22

Alumno: Castillo Jr. Gregorio

Numero de control: 19580589

Índice

Índice	1
Investigación (Leyes de seguridad en la información)	2
Examen (Elaborar examen con 10 preguntas).....	4
Resumen (Artículos de la LFDA para los programas de computación y bases de datos)	6
Investigación (Convenio de Berna)	9
Conclusiones.....	11
Fuentes de información	12

Investigación (Leyes de seguridad en la información)

Las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías.

La seguridad de la información, según la ISO 27001, se basa en la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas aplicados para su tratamiento.

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos o procesos autorizados cuando lo requieran.

Dentro de este conjunto están:

Norma	Descripción
ISO/IEC 27000	Vocabulario estándar para el SGSI para todas las normas de la familia.. Se encuentra en desarrollo actualmente.
ISO/IEC 27001	Certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.
ISO/IEC 27002	<i>Information technology - Security techniques - Code of practice for information security management.</i> Previamente BS 7799 Parte 1 y la norma ISO/IEC 17799. Es un código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.
ISO/IEC 27003	Directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010, No está certificada actualmente.

ISO/IEC 27004	Métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.
ISO/IEC 27005	Normativa dedicada exclusivamente a la gestión de riesgos en seguridad de la información. Proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma ISO/IEC 27001. Es la más relacionada a la actual British Standar BS 7799 parte 3. Publicada en junio de 2008.
ISO/IEC 27006	Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma especifica requisitos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación.
ISO/IEC 27007	Guía para auditar al SGSI. Se encuentra en preparación.
ISO/IEC 27799:2008	Guía para implementar ISO/IEC 27002 en la industria de la salud.

Artículo 6.- Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley.

Artículo 7.- Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta Ley y demás normatividad aplicable.

Artículo 8.- Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley.

Artículo 9.- Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.

Examen (Elaborar examen con 10 preguntas)

1.- ¿Porque es importante conocer las leyes?

- a) Nos permite asegurarnos a nosotros y al cliente
- b) Nos permite aprovechar los márgenes legales
- c) Nos permite tener claro el estatuto legal de la empresa

2.- Es quien regula las normas:

- a) DDFA
- b) NSA
- c) ISO

3.- Son los estándares principales para la legislación de información y propiedad intelectual

- a) ISO 27000 y 27001
- b) ISO 37000 y 37001
- c) ISO 17000 y 17001

4.- Son consecuencias de no cumplir con las normas de protección de datos

- a) Problemas legales con dueños y empleados de la empresa con la que se trabaja
- b) Problemas legales con dueños y clientes de la empresa con la que se trabaja
- c) Problemas legales con clientes y empleados de la empresa con la que se trabaja

5.- Es el encargado de regular los derechos de autor en Mexico

- a) LFDA
- b) IDPDD
- c) CMDD

Relaciona con lo correspondiente

A.- ISO 27000

B.- ISO 27001

C.- Son el objetivo de las normas de la seguridad de la información

D.- Son los principios básicos de Berna

E.- LFDA

(**D**) Las obras originarias deberán ser objeto, la protección no deberá estar subordinada, la protección es independiente de la existencia de protección

(**B**) Es el estándar internacional para la gestión de la seguridad de la información en las organizaciones

(**E**) Es la Ley Federal Del Derecho Autor

(**A**) Es el estándar internacional para la seguridad de la información

(**C**) Confidencialidad, Integridad y Disponibilidad

Resumen (Artículos de la LFDA para los programas de computación y bases de datos)

Artículo 101.- Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código

Artículo 102.- Los programas de computación se protegen en los mismos términos que las obras literarias

Artículo 103.- Salvo pacto en contrario, los derechos patrimoniales sobre un programa de computación y su documentación

Artículo 104.- Como excepción a lo previsto en el artículo 27 fracción IV, el titular de los derechos de autor sobre un programa de computación o sobre una base de datos conservará, aún después de la venta de ejemplares de los mismos

Artículo 105.- El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:

- I. Sea indispensable para la utilización del programa, o
- II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación

Artículo 106.- El derecho patrimonial sobre un programa de computación comprende la facultad de autorizar o prohibir:

- I. La reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma;
- II. La traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante;
- III. Cualquier forma de distribución del programa o de una copia del mismo, incluido el alquiler;

- IV. La decompilación, los procesos para revertir la ingeniería de un programa de computación y el desensamblaje
- V. La comunicación pública del programa, incluida la puesta a disposición pública del mismo.

Artículo 107.- Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones

Artículo 108.- Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado

Artículo 109.- El acceso a información de carácter privado relativa a las personas contenida en las bases de datos a que se refiere el artículo anterior

Artículo 110.- El titular del derecho patrimonial sobre una base de datos tendrá el derecho exclusivo, respecto de la forma de expresión de la estructura de dicha base, de autorizar o prohibir:

- I. Su reproducción permanente o temporal, total o parcial, por cualquier medio y de cualquier forma;
- II. Su traducción, adaptación, reordenación y cualquier otra modificación;
- III. La distribución del original o copias de la base de datos;
- IV. La comunicación al público,
- V. La reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

Artículo 111.- Los programas efectuados electrónicamente que contengan elementos visuales, sonoros, tridimensionales o animados quedan protegidos por esta Ley en los elementos primigenios que contengan.

Artículo 112.- Queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo

Artículo 113.- Las obras e interpretaciones o ejecuciones transmitidas por medios electrónicos a través del espectro electromagnético y de redes de telecomunicaciones y el resultado que se obtenga de esta transmisión estarán protegidas por esta Ley.

Artículo 114.- La transmisión de obras protegidas por esta Ley mediante cable, ondas radioeléctricas, satélite u otras similares, deberán adecuarse, en lo conducente, a la legislación mexicana

Investigación (Convenio de Berna)

El Convenio de Berna, que fue adoptado en 1886, trata de la protección de las obras y los derechos de los autores. Ofrece a los creadores como los autores, músicos, poetas, pintores, etc., los medios para controlar quién usa sus obras, cómo y en qué condiciones.

Los **tres principios básicos** son los siguientes:

- a) Las obras originarias de uno de los Estados Contratantes deberán ser objeto, en todos y cada uno de los demás Estados Contratantes, de la misma protección que conceden a las obras de sus propios nacionales
- b) La protección no deberá estar subordinada al cumplimiento de formalidad alguna
- c) La protección es independiente de la existencia de protección en el país de origen de la obra. Empero, si en un Estado Contratante se prevé un plazo más largo de protección que el mínimo prescrito por el Convenio, y cesa la protección de la obra en el país de origen, la protección podrá negarse en cuanto haya cesado en el país de origen

Las condiciones mínimas de protección se refieren a las obras y los derechos que han de protegerse, y a la duración de la protección:

- **el derecho a traducir.**
- **el derecho de realizar adaptaciones y arreglos** de la obra,
- **el derecho de representar y ejecutar en público** las obras dramáticas, dramático–musicales y musicales,
- **el derecho de recitar en público** las obras literarias,
- **el derecho de transmitir al público** la representación o ejecución de dichas obras,
- **el derecho de radiodifundir** (los Estados Contratantes cuentan con la posibilidad de prever un simple derecho a una remuneración equitativa, en lugar de un derecho de autorización),
- **el derecho de realizar una reproducción** por cualquier procedimiento y bajo cualquier forma

El Convenio de Berna permite ciertas limitaciones y excepciones en materia de derechos económicos, es decir, los casos en que las obras protegidas podrán

utilizarse sin autorización del propietario del derecho de autor y sin abonar una compensación. Generalmente se utiliza el término "libre utilización" de obras protegidas para referirse a esas limitaciones, y figuran en el párrafo 2) del artículo 9 (reproducción en determinados casos especiales), el artículo 10 (citas y uso de obras a título de ilustración de la enseñanza), el artículo 10*bis* (reproducción de artículos de periódicos o artículos similares y el uso de obras con fines de información sobre acontecimientos actuales) y el párrafo 3) del artículo 11*bis* (grabaciones efímeras con fines de radiodifusión).

Conclusiones

Dentro de esta unidad nos encargamos de revisar cuales son las leyes con las cuales nos podemos apoyar a la hora de tener que trabajar en el área de tecnologías, todo esto debido a rozamiento de carácter legal ya sea por incumplimiento o cualquier otro aspecto que nos pueda perjudicar, nos sirven para protegernos a nosotros y poder proteger a los clientes, haciendo que todo sea realice dentro del aspecto legal de nuestro país, estas leyes con las que se supone trabajaríamos dentro de nuestro marco legal, están mas enfocadas a la protección de datos y contenido propio, con lo cual podemos organizarnos mejor y saber que tipos de acciones hay que evitar para no tener problemas legales ya sea dentro o fuera de nuestra empresa, dicho esto, es importante no solamente conocer el contenido que manejamos si no también el contenido que ofrecemos, esto para poder brindar mas control y estar consciente de que es lo que vamos a realizar a determinado cliente.

Fuentes de información

Normas ISO sobre gestión de seguridad de la información / Seguridad Informática. (s. f.).

http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

Convenio de Berna para la Protección de las Obras Literarias y Artísticas. (s. f.).

<https://www.wipo.int/treaties/es/ip/berne/index.html>

Ley Federal del Derecho Autor. (s. f.).

https://www.diputados.gob.mx/LeyesBiblio/pdf/122_010720.pdf

ISO 27000 y el conjunto de estándares de Seguridad de la Información. (s. f.).

<https://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-informacion.html>