

LEGISLACIÓN INFORMÁTICA

Unidad VI: La Legislación y Normatividad Actual Relativa al Hardware



INSTITUTO TECNOLÓGICO
DE MORELIA

Departamento de Sistemas y
Computación

Disponible en: www.benito.org.mx

M.C. Benito Sánchez Raya
sanchezraya@hotmail.com

CONTENIDO

1. Casos de normatividad aplicada al hardware.
 - a) Acceso no autorizado a equipos de cómputo y de telecomunicaciones
 - b) Robo de equipo
2. Debilidades o insuficiencias de la normatividad
 - a) Casos de estudio

1. CASOS DE NORMATIVIDAD APLICADA AL HARDWARE

A) ACCESO NO AUTORIZADO A EQUIPOS DE CÓMPUTO Y DE TELECOMUNICACIONES

- Una recomendación para minimizar riesgos de éste tipo, es la implementación de controles de seguridad proporcionados por los estándares:
 - ISO/IEC 27001:2005
 - Requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI) para ser certificable por una entidad independiente.
 - ISO /IEC 27002:2005
 - Guía de buenas prácticas para la gestión de la seguridad de la información.

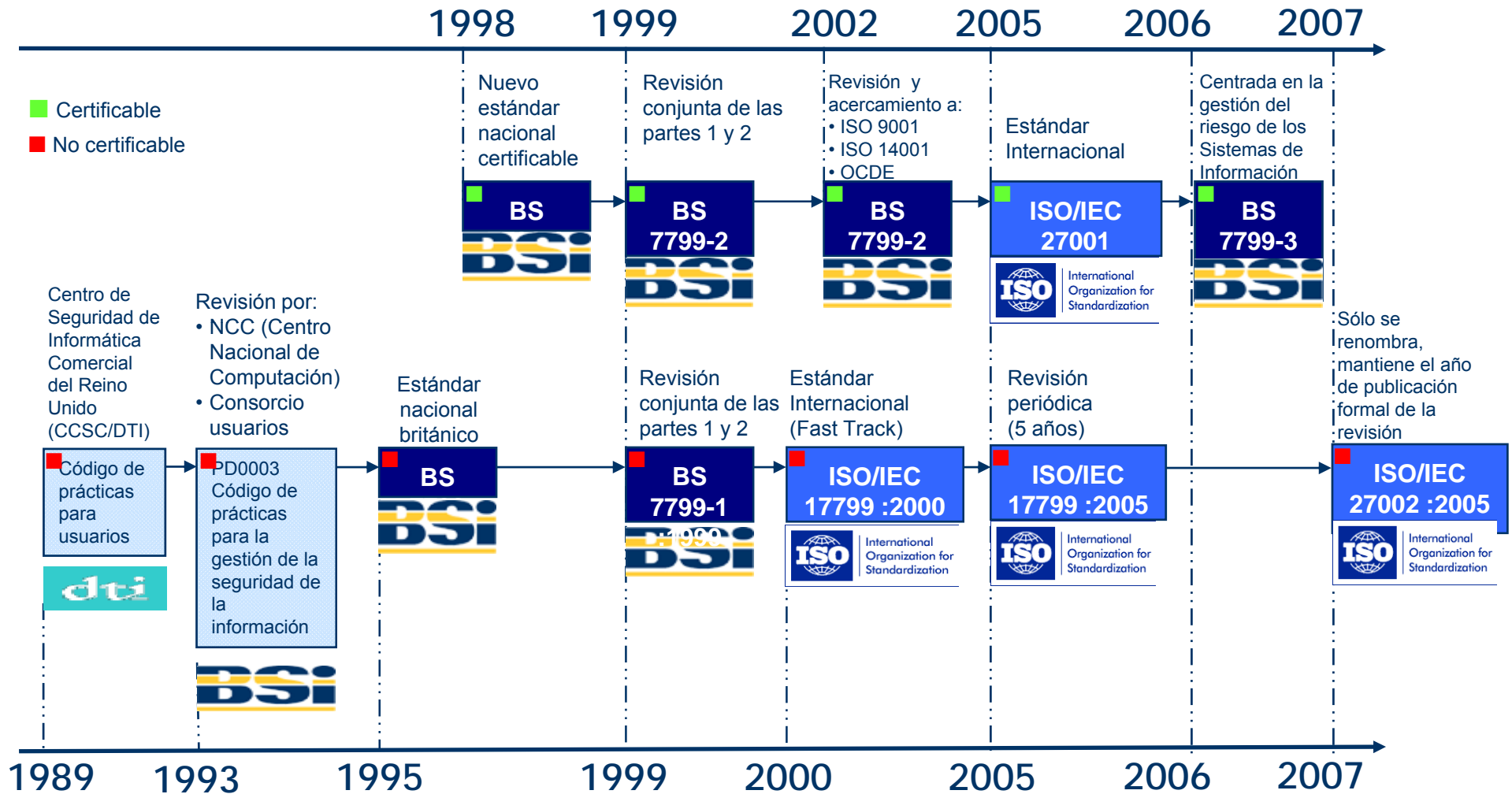
- La información es un activo vital para el éxito de cualquier organización.
- El aseguramiento de dicha información y de los sistemas que la procesan es, un objetivo de primer nivel para la organización.
- ISO/IEC 27000 es un conjunto de estándares de ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission).
- Proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

- La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información.
- La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas.
- La segunda parte (BS 7799-2), publicada por primera vez en 1998, establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

- Las dos partes de la norma BS 7799 se revisaron en 1999.
 - La primera parte se adoptó por ISO, sin cambios, como ISO 17799 en el año 2000.
- En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.
- En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001.
- En 2005 se revisó y actualizó ISO17799.
 - ISO17799 se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

- En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

HISTORIA DE ISO 27001 E ISO 17799



● LA SERIE 27000

- A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares.
- Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.
- **ISO 27000:**
 - En fase de desarrollo.
 - Fecha prevista de publicación: Noviembre de 2008.
 - Contendrá **términos y definiciones que se emplean en toda la serie 27000**.
 - Evitará interpretaciones de conceptos técnicos y de gestión.
 - Se prevé que sea **gratuita**, a diferencia de las demás de la serie.

– ISO 27001:

- Publicada el 15 de Octubre de 2005.
- Es la norma principal de la serie y contiene los **requisitos del SGSI**.
- Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se **certifican por auditores externos** los SGSI de las organizaciones.
- En su Anexo A, sintetiza los objetivos de control y controles que desarrolla la ISO 27002:2005.

– ISO 27002:

- Desde el 1 de Julio de 2007
- Es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición.
- Es una **guía de buenas prácticas** que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.
- No es certificable.

- Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005.
- En España, aún no está traducida (previsiblemente, a lo largo de 2008).
- Desde 2006, está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO 17799; descarga gratuita).
- El original en inglés y su traducción al francés pueden adquirirse en www.iso.org.

– ISO 27003:

- En fase de desarrollo.
- Fecha prevista de publicación: Mayo de 2009.
- Consistirá en una **guía de implementación de SGSI e información acerca del uso del modelo PDCA** (Plan-Do-Check-Act , Planificar-Hacer-Verificar-Actuar) y de los requerimientos de sus diferente fases.
- Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.



– **ISO 27004:**

- En fase de desarrollo.
- Fecha prevista de publicación Noviembre de 2008.
- Especificará las **métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI** y de los controles relacionados.
- Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do”(Implementar y Utilizar) del ciclo PDCA.

– ISO 27005:

- En fase de desarrollo.
- Fecha prevista de publicación es Mayo de 2008.
- Consistirá en una guía de **técnicas para la gestión del riesgo de la seguridad de la información** y servirá, por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI.
- Recogerá partes de ISO/IEC TR 13335.
 - Directrices para el manejo de la seguridad de las TI.

– ISO 27006:

- Publicada el 1 de Marzo de 2007.
- Especifica los **requisitos para la acreditación de entidades de auditoría y certificación de SGSI** .
- Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs.
- Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.



– **ISO 27007:**

- En fase de desarrollo.
- Fecha prevista de publicación Mayo de 2010.
- Consistirá en una **guía de auditoría de un SGSI.**

– **ISO 27011:**

- Recién liberada (2008).
- Consistirá en una **guía de SGSI específica para telecomunicaciones**, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).



– **ISO 27031:**

- En fase de desarrollo.
- Fecha prevista de publicación Mayo de 2010.
- Consistirá en una **guía de continuidad de negocio en TICs.**

– **ISO 27032:**

- En fase de desarrollo.
- Fecha prevista de publicación Febrero de 2009.
- Consistirá en una **guía relativa a la ciberseguridad.**

– ISO 27033:

- En fase de desarrollo.
- Fecha prevista de publicación es entre 2010 y 2011.
- Provenirá de la revisión de ISO 18028.
- Norma que consiste en 7 partes:
 1. **Gestión de seguridad de redes**
 2. **Arquitectura de seguridad de redes**
 3. **Escenarios de redes de referencia**
 4. **Aseguramiento de las comunicaciones entre redes mediante *gateways***
 5. **Acceso remoto**
 6. **Aseguramiento de comunicaciones en redes VPNs**
 7. **Diseño e implementación de seguridad en redes.**



– **ISO 27034:**

- En fase de desarrollo; su fecha prevista de publicación es Febrero de 2009.
- Consistirá en una **guía de seguridad en aplicaciones.**

– **ISO 27799:**

- En fase de desarrollo.
- Fecha prevista de publicación es 2008.
- Es un **estándar SGSI en el sector sanitario** aplicando ISO 17799 (actual ISO 27002).

● **Contenido de la Norma ISO 27002:2005**

- Sólo se incluye esta norma, por ser la que está más apegada a la seguridad del Hardware.
 - a) **Introducción:** conceptos generales de seguridad de la información y SGSI.
 - b) **Campo de aplicación:** se especifica el objetivo de la norma.
 - c) **Términos y definiciones:** breve descripción de los términos más usados en la norma.
 - d) **Estructura del estándar:** descripción de la estructura de la norma.

- e) **Evaluación y tratamiento del riesgo:** indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.
- f) **Política de seguridad:** documento de política de seguridad y su gestión.
- g) **Aspectos organizativos de la seguridad de la información:** organización interna; terceros.
- h) **Gestión de activos:** responsabilidad sobre los activos; clasificación de la información.
- i) **Seguridad ligada a los recursos humanos:** antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.

- j) **Seguridad física y ambiental:** áreas seguras; seguridad de los equipos.
- k) **Gestión de comunicaciones y operaciones:** responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.
- l) **Control de acceso:** requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; ordenadores portátiles y teletrabajo.

- m) **Adquisición, desarrollo y mantenimiento de los sistemas de información:** requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptográficos; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.
- n) **Gestión de incidentes de seguridad de la información:** notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras.
- o) **Gestión de la continuidad del negocio:** aspectos de la seguridad de la información en la gestión de la continuidad del negocio.

- p) **Cumplimiento:** cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorías de los sistemas de información.
- q) **Bibliografía:** normas y publicaciones de referencia.

– Puede descargarse una lista de todos los controles que contiene esta norma aquí:


<http://www.iso27000.es/download/ControlesISO27002-2005.pdf>

● **Beneficios del ISO 27000**

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.

- Posibilidad de integrarse con otros sistemas de gestión.
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costos y mejora de los procesos y servicio.

- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de la compra sistemática de productos y tecnologías.

- 
- Una vez implementado los controles de seguridad físicos recomendados, se puede crear una buena política apoyándose en:
 - El Código Penal Federal
 - Código Federal de Procedimientos Civiles

CODIGO PENAL FEDERAL

TITULO NOVENO

Revelación de secretos y acceso ilícito a sistemas y equipos de informática

CAPITULO II

Acceso ilícito a sistemas y equipos de informática

Artículos: 211 bis 1 al 211 bis 7

– Código Penal Federal:

- **Artículo 211 bis 1.-** Al que sin autorización **modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad**, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización **conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad**, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

- **Artículo 211 bis 2.-** Al que sin autorización **modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad**, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

Al que sin autorización **conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad**, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

- **Artículo 211 bis 3.-** Al que **estando autorizado** para acceder a sistemas y equipos de informática del **Estado**, indebidamente **modifique, destruya o provoque pérdida de información** que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.
- Al que **estando autorizado** para acceder a sistemas y equipos de informática del **Estado**, indebidamente **copie información que contengan**, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

- **Artículo 211 bis 4.-** Al que sin autorización **modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero**, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.

Al que sin autorización **conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero**, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.

- **Artículo 211 bis 5.-** Al que **estando autorizado** para acceder a sistemas y equipos de informática de las instituciones que integran el **sistema financiero**, indebidamente **modifique, destruya o provoque pérdida de información** que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa.
- Al que **estando autorizado** para acceder a sistemas y equipos de informática de las instituciones que integran el **sistema financiero**, indebidamente **copie información que contengan**, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa.
- Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

- **Artículo 211 bis 6.-** Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código.
- **Artículo 211 bis 7.-** Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

CODIGO PENAL FEDERAL

TITULO QUINTO

Delitos en Materia de Vías de Comunicación y Correspondencia

CAPITULO I

Ataques a las vías de comunicación y violación de correspondencia

Artículos: 165 a 172

- **Artículo 165.-**
- **Artículo 166.-**
- **Artículo 167.-** Se impondrán de uno a cinco años de prisión y de cien a diez mil días multa:
 - **I.-**
 - **II.-** Al que **destruya o separe** uno o más postes, aisladores, alambres, máquinas o aparatos, empleados en el servicio de telégrafos; **cualquiera de los componentes de la red pública de telecomunicaciones**, empleada en el **servicio telefónico, de conmutación o de radiocomunicación, o cualquier componente de una instalación de producción de energía magnética o electromagnética** o sus medios de transmisión.

- III.-
- IV.-
- V.-
- VI.- Al que dolosamente o con fines de lucro, **interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica**, sean telegráficas, telefónicas o satelitales, **por medio de las cuales se transfieran señales de audio, de video o de datos;**
- VII.
- VIII.
- IX.

- **Artículo 168.-**
- **Artículo 168 bis.-** Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa, a quien sin derecho:
 - **I. Descifre o decodifique señales de telecomunicaciones** distintas a las de satélite portadoras de programas, o
 - **II. Transmita la propiedad, uso o goce de aparatos, instrumentos o información que permitan descifrar o decodificar señales de telecomunicaciones** distintas a las de satélite portadoras de programas.

- 
- 
- **Artículo 169.-**
 - **Artículo 170.-**
 - **Artículo 171.-**
 - **Artículo 172.-**

CÓDIGO FEDERAL DE PROCEDIMIENTOS CIVILES

TITULO CUARTO Pruebas

CAPITULO IX Valuación de la prueba Artículos: 197 a 218

- **ARTICULO 197.-**
- **ARTICULO 198.-**
- **ARTICULO 199.- La confesión expresa hará prueba plena cuando concurren, en ella, las circunstancias siguientes:**
 - **I.-** Que sea hecha por persona capacitada para obligarse;
 - **II.-** Que sea hecha con pleno conocimiento, y sin coacción ni violencia, y
 - **III.-** Que sea de hecho propio o, en su caso, del representado o del cedente, y concerniente al negocio.

- **ARTICULO 200.-** Los hechos propios de las partes, aseverados en la demanda, en la contestación o en cualquier otro acto del juicio, **harán prueba plena en contra de quien los asevere, sin necesidad de ofrecerlos como prueba.**
- **ARTICULO 201.-** La confesión ficta(ficticia) produce el efecto de una presunción, cuando no haya pruebas que la contradigan.
- **ARTICULO 202.-**

- **ARTICULO 203.- El documento privado forma prueba** de los hechos mencionados en él, sólo en cuanto sean contrarios a los intereses de su autor, cuando la ley no disponga otra cosa. El documento proveniente de un tercero sólo prueba en favor de la parte que quiere beneficiarse con él **y contra su colitigante, cuando éste no lo objeta**. En caso contrario, la verdad de su contenido debe demostrarse por otras pruebas.
- **ARTICULO 204.-**
- **ARTICULO 205.-**
- **ARTÍCULO 206.-**
- **ARTICULO 207.- Las copias hacen fe de la existencia de los originales**, conformes a las reglas precedentes; pero **si se pone en duda su exactitud, deberá ordenarse su cotejo con los originales** de que se tomaron.

- **ARTICULO 208.-**
- **ARTICULO 209.-**
- **ARTICULO 210.-**
- **ARTICULO 210-A.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.**
- Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta.

- **Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.**

– Artículo adicionado DOF 29-05-2000

- **ARTICULO 211.-**
- **ARTICULO 212.-**
- **ARTICULO 213.-**
- **ARTICULO 214.-**

● **ARTICULO 215.- El valor de la prueba testimonial quedará al prudente arbitrio del tribunal, quien, para apreciarla, tendrá en consideración:**

- **I.-** Que los testigos convengan en lo esencial del acto que refieran, aun cuando difieran en los accidentes;
- **II.-** Que declaren haber oído pronunciar las palabras, presenciado el acto o visto el hecho material sobre que depongan;
- **III.-** Que, por su edad, capacidad o instrucción, tengan el criterio necesario para juzgar el acto.
- **IV.-** Que, por su probidad, por la independencia de su posición o por sus antecedentes personales, tengan completa imparcialidad;
- **V.-** Que por sí mismos conozcan los hechos sobre que declaren, y no por inducciones ni referencias de otras personas;
- **VI.-** Que la declaración sea clara, precisa, sin dudas ni reticencias, sobre la substancia del hecho y sus circunstancias esenciales.
- **VII.-** Que no hayan sido obligados por fuerza o miedo, ni impulsados por engaño, error o soborno, y
- **VIII.-** Que den fundada razón de su dicho.

- **ARTICULO 216.-**
- **ARTICULO 217.-** El valor de las pruebas fotográficas, taquigráficas y de otras cualesquiera aportadas por los descubrimientos de la ciencia, quedará al prudente arbitrio judicial.
- **Las fotografías de personas, lugares, edificios, construcciones, papeles, documentos y objetos de cualquier especie, deberán contener la certificación correspondiente que acredite el lugar, tiempo y circunstancias en que fueron tomadas, así como que corresponden a lo representado en ellas, para que constituyan prueba plena. En cualquier otro caso, su valor probatorio queda al prudente arbitrio judicial.**
- **ARTICULO 218.-**

● Panorama Mundial

– Italia:

- En su artículo 615-ter del Código Penal prevé un delito denominado “*Acceso abusivo ad un sistema informático o telemático*”, que **tipifica la intrusión a un sistema informático o telemático** protegido con medidas de seguridad o contra la voluntad expresa de quien tiene derecho a excluirlo.

– Estados Unidos:

- La “Counterfeit Access Device and Computer Fraud and Abuse” (18 U.S.C. Sec.1030) **tipifica penalmente el acceso no autorizado a sistemas informáticos** operados por el gobierno, y en particular a los asociados a la defensa nacional, los archivos externos y la energía atómica, así como instituciones financieras.

– **Suecia:**

- Castiga únicamente el acceso a un sistema de procesamiento de datos.

– **Francia:**

- Sanciona, por la ley 88/19, art. 462-4, tanto al que accede al sistema como al que se mantiene en él.

– **Chile:**

- No penaliza el acceso, sólo la difusión o revelación de los datos.

– **Venezuela:**

- Existe la “**Ley Especial Contra los Delitos Informáticos**”. Ley especializada sobre el tema.

B) ROBO DE EQUIPO

- En el país el robo de computadoras, equipos de cómputo, sistemas de cómputo, sistemas informáticos, refiriéndonos al hardware concretamente, no se estipula ni se tipifica.
- Se trata como un mueble, es decir que en el país el robo de un equipo de cómputo no significaría más que equiparlo con una silla o una lámpara.

Seguros:



- Lo Jack para laptops (<http://www.lojack.com.mx/>)
 - Computrace LoJack for Laptops. Es un sistema de medios de rastreo y localización de laptops robadas.
 - Se instala en el BIOS un software aprobado por el Departamento de Defensa de los EUA
 - En forma “silenciosa” se controla y rastrea por internet.
 - Incluye: data delete
 - Existen convenios con la mayoría de los fabricantes de PCs.
 - \$ 1,199 anuales.

CÓDIGO PENAL FEDERAL

TITULO VIGÉSIMO SEGUNDO **Delitos en Contra de las Personas en su Patrimonio**

CAPITULO I **Robo**

Artículos: 367 a 381

- **Artículo 367.-** Comete el delito de robo: el que se apodera de una cosa ajena mueble, sin derecho y sin consentimiento de la persona que puede disponer de ella con arreglo a la ley.
- **Artículo 368.-** Se equiparan al robo y se castigarán como tal:
 - I.- El apoderamiento o destrucción dolosa de una cosa propia mueble, si ésta se halla por cualquier título legítimo en poder de otra persona y no medie consentimiento; y

- II.- El uso o aprovechamiento de energía eléctrica, **magnética, electromagnética**, de cualquier fluido, o de **cualquier medio de transmisión**, sin derecho y sin consentimiento de la persona que legalmente pueda disponer de los mismos.

- **Artículo 368 Bis.-** Se sancionará con pena de tres a diez años de prisión y hasta mil días multa, al que **después de la ejecución del robo y sin haber participado en éste, posea, enajene o trafique de cualquier manera, adquiera o reciba, los instrumentos, objetos o productos del robo, a sabiendas de esta circunstancia y el valor intrínseco de éstos sea superior a quinientas veces el salario.**

- **Artículo 368 Ter.-** Al que comercialice en forma habitual objetos robados, a sabiendas de esta circunstancia y el valor intrínseco de aquéllos sea superior a quinientas veces el salario, se le sancionará con una pena de prisión de seis a trece años y de cien a mil días multa.
- **Artículo 369.-** Para la aplicación de la sanción, se dará por consumado el robo desde el momento en que el ladrón tiene en su poder la cosa robada; aún cuando la abandone o la desapoderen de ella. En cuanto a la fijación del valor de lo robado, así como la multa impuesta, se tomará en consideración el salario en el momento de la ejecución del delito.

- **Artículo 370.-** Cuando el valor de lo robado no exceda de cien veces el salario, se impondrá hasta dos años de prisión y multa hasta de cien veces el salario.
- Cuando exceda de cien veces el salario, pero no de quinientas, la sanción será de dos a cuatro años de prisión y multa de cien hasta ciento ochenta veces el salario.
- Cuando exceda de quinientas veces el salario, la sanción será de cuatro a diez años de prisión y multa de ciento ochenta hasta quinientas veces el salario.

- **Artículo 371.- Para estimar la cuantía del robo se atenderá únicamente el valor intrínseco del objeto** del apoderamiento, pero si por alguna circunstancia no fuere estimable en dinero o si por su naturaleza no fuere posible fijar su valor, se aplicará prisión de tres días hasta cinco años.
- **Artículo 372.- Si el robo se ejecutare con violencia**, a la pena que corresponda por el robo simple se agregarán de seis meses a cinco años de prisión. **Si la violencia constituye otro delito, se aplicarán las reglas de la acumulación.**

- **Artículo 373.- La violencia a las personas se distingue en física y moral.**
- Se entiende por violencia física en el robo: la fuerza material que para cometerlo se hace a una persona.
- Hay violencia moral: cuando el ladrón amaga o amenaza a una persona, con un mal grave, presente o inmediato, capaz de intimidarlo.

- **Artículo 375.-** Cuando el valor de lo robado no pase de diez veces el salario, sea restituido por el infractor espontáneamente y pague éste todos los daños y perjuicios, antes de que la Autoridad tome conocimiento del delito no se impondrá sanción alguna, si no se ha ejecutado el robo por medio de la violencia.
- **Artículo 379.-** No se castigará al que, sin emplear engaño ni medios violentos, se apodera una sola vez de los objetos estrictamente indispensables para satisfacer sus necesidades personales o familiares del momento.

● Legislación en Venezuela contra robo de equipo:

– Ley Especial Contra los Delitos Informáticos.
Capítulo II.

- **Artículo 13.- Hurto.** El que a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de **bienes o valores tangibles o intangibles** de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

2. Debilidades o insuficiencias de la normatividad

- La acción delictiva en el país no se prevé en un simple acceso no autorizado
 - Al entrar a una oficina o a un edificio federal o alguna área especializada no causa un “allanamiento” y mucho menos de “morada”.
- Difícilmente un delincuente va a entrar a un área protegida por medios de seguridad física sin motivo alguno, la violación de estos medios si será tomado en cuenta como daño en propiedad ajena.

- Las debilidades de la normatividad en éste sentido son la falta de tipificación de los delitos en forma explícita, es decir, las leyes y los procedimientos dejan a consideración de jueces magistrados y tribunales el sentido y orientación o validez de una conducta delictiva.

CÓDIGO PENAL FEDERAL

TITULO VIGÉSIMO SEGUNDO **Delitos en Contra de las Personas en su Patrimonio**

CAPITULO VI **Daño en propiedad ajena**

Artículos: 397-399

– **Artículo 397.-** Se impondrán de cinco a diez años de prisión y multa de cien a cinco mil pesos, a los que **causen incendio, inundación o explosión con daño o peligro** de:

- I.- Un edificio, vivienda o cuarto donde se encuentre alguna persona;
- II.- Ropas, muebles u objetos en tal forma que puedan causar graves daños personales;
- III.- Archivos públicos o notariales;
- IV.- Bibliotecas, museos, templos, escuelas o edificios y monumentos públicos, y
- V.- Montes, bosques, selvas, pastos, mieses o cultivos de cualquier género.

- **Artículo 398.-** Si además de los daños directos resulta consumado algún otro delito, se aplicarán las reglas de acumulación.
- **Artículo 399.-** Cuando por cualquier medio se causen daño, destrucción o deterioro de cosa ajena, o de cosa propia en perjuicio de tercero, se aplicarán las sanciones del robo simple.

● **CASOS DE ESTUDIO:**

1. **Empresa de generación de energía eléctrica a través del uso del calor**
 - Bien distribuida el área
 - Restringen el acceso solo a personas autorizadas
 - Cuentan con una llave que permite la entrada a la oficina en general y por ende queda libre el acceso a quien fuese, si la puerta estuviese abierta o bien que no estuviera el personal.
 - Se tiene un sistema de monitoreo de circuito cerrado, graba las 24 hrs, el acceso al área de cómputo, pero el servidor que almacena dicho video esta ubicado **dentro de la misma área.**
 - **No se cuenta con un reglamento que especifique que esos videos se tomarán como evidencias para un posible proceso penal.**

2. **Cervecería ubicada en la ciudad de Morelia**

- Se tiene una excelente ubicación del site dentro del edificio, lugar poco accesible para la mayoría de los empleados, fuera del alcance de visitantes.
- Cuentan con vigilancia de ingreso y registro al edificio
- Tiene dos “candados”, es decir, una puerta que te permite la entrada al área de sistemas y otra puerta directa al site.
- **Medidas de control de acceso como tal no existen, debido a que no se han presentado casos de accesos no autorizados, ni robo de equipos.**

● **ACTIVIDADES DE APRENDIZAJE**

- Leer y analizar el “convenio sobre la ciberdelincuencia” emanado por el Consejo de Europa.
- Leer y analizar el “protocolo adicional al Convenio sobre la ciberdelincuencia”.
- Investigar y leer los estándares siguientes, en su versión completa:
 - ISO /IEC 27002:2005



- **REFERENCIAS**

Material de Titulación

Arturo García Velázquez. 2006.

Instituto Tecnológico de Morelia.