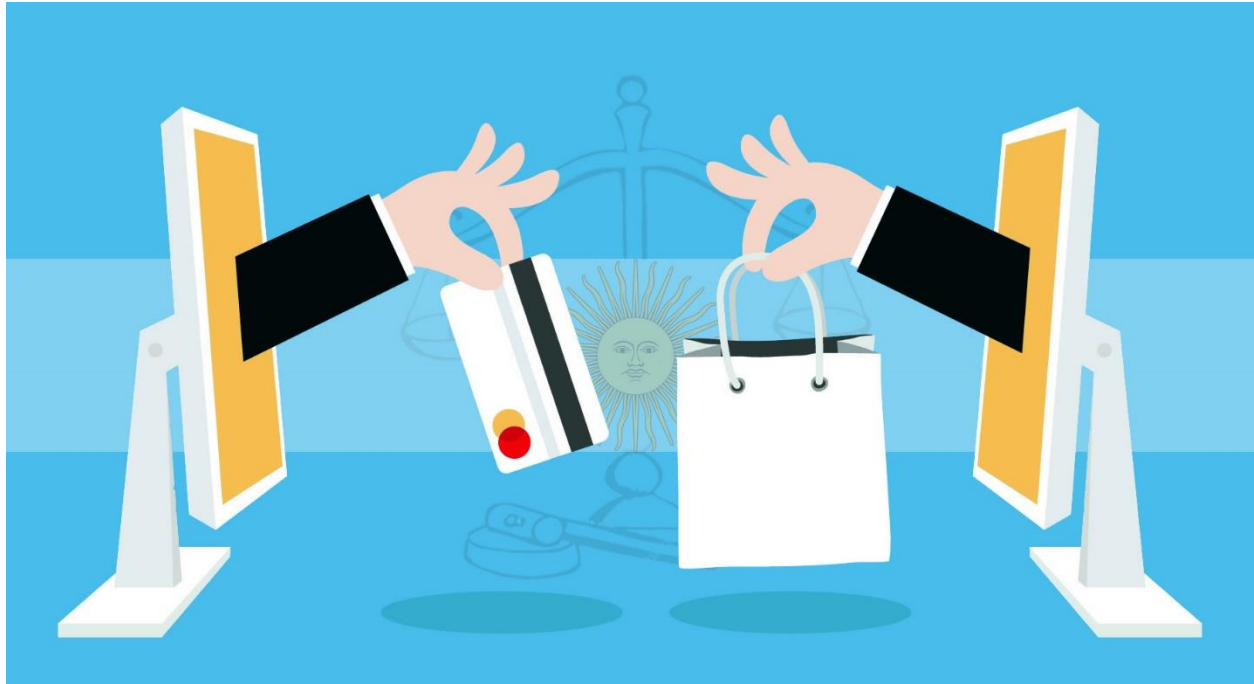


# Trabajo Final

## Desarrollo de Software



Fecha de entrega: **25/06/2019**

### Integrantes:

- |                           |                      |
|---------------------------|----------------------|
| • Contreras Juan          | Legajo: <b>21609</b> |
| • D' Angelo Martín Alexis | Legajo: <b>21998</b> |
| • Marcilio Gastón         | Legajo: <b>21738</b> |
| • Ramírez Ariel           | Legajo: <b>21468</b> |
| • Rivero Cristian         | Legajo: <b>21603</b> |
| • Tidele Alejandro        | Legajo: <b>21841</b> |

## Índice

Introducción .....	2
Características del Software.....	2
Ley de promoción de la industria del software .....	3
Beneficios .....	3
Requisitos para acceder a los beneficios.....	3
Ley de Economía Del Conocimiento .....	5
Financiación.....	5
Beneficios de la Ley de Economía del Conocimiento .....	5
Patentamiento del Software .....	6
¿Por qué registrar un software?.....	6
Propiedad Intelectual .....	6
Ley de Patentes de Invención.....	7
Ley Protección de datos personales .....	8
¿Qué es dato Personal? .....	8
¿Qué tipos de datos personales hay?.....	8
Definiciones .....	9
Categoría de datos.....	10
Datos relativos a la salud .....	10
¿Qué obligaciones debe cumplir el titular de una Base de Datos?.....	10
¿Qué son los derechos ARCO?.....	10
Seguridad de los datos.....	11
¿Quién controla que se cumpla la Ley? .....	12
Ley de Delitos Informáticos.....	13
Cómo afectaría.....	13
Estadísticas.....	13
Casos de Delito Informático .....	14
Ley de Seguridad Informática.....	15
Medidas para el mantenimiento de la seguridad informática y la prevención de intrusiones.....	16
FUENTES:.....	17

## Introducción

Con el equipo decidimos llevar a cabo un sistema para **Comercios Minoristas**. El marco de análisis comprende el mes de Abril/Mayo en el año 2019 en la provincia de Buenos Aires en Argentina. Detectamos que los comercios minoristas carecen de un sistema eficiente para administrar el contenido de sus locales, y acceder a un sistema de esa envergadura es muy costoso. Por eso, acordamos realizar un sistema Standard, a muy bajo costo, para los comercios que decidan adherirse y poder así, beneficiar a la sociedad.

## Características del Software

- Ingreso y egreso de Stock.
- Módulo de Facturación.
- Fecha de ingreso stock y vencimiento (si lo tiene).
- Stock máximo y mínimo para cada artículo.
- Que cantidad del mismo artículo tienen el mismo vencimiento.
- El sistema descontaría elementos en cada venta.
- Informar cuando el stock sea bajo (vía mail o alguna otra forma)
- Sistema de alerta por fechas de caducidad.
- Importar listas de precios.

## Ley de promoción de la industria del software

### Beneficios

Al dedicarnos al desarrollo de software accedemos a varios beneficios gracias a la ley de promoción de la industria del software, como por ejemplo:

1. Estabilidad fiscal: no te afecta el aumento de impuestos nacionales.
2. Reducción de hasta el 60% del impuesto a las Ganancias.
3. Acceso a un bono para pagar impuestos nacionales (a excepción del impuesto a las Ganancias).  
Este bono se acredita mensualmente y varía según la cantidad de empleados que tengas.

### Requisitos para acceder a los beneficios

Para poder acceder a los beneficios, se deben cumplir **2** de los **3** siguientes ítems:

1. Hacer investigación y desarrollo.
2. Certificar normas de calidad.
3. Exportar.

Además:

- Destinar más del 50% de la actividad de tu empresa al desarrollo de software.
  - Actividades comprendidas: Creación, diseño, desarrollo, producción e implementación y puesta a punto de los sistemas de software desarrollados y su documentación técnica asociada, tanto en su aspecto básico como aplicativo, incluyendo el que se elabore para ser incorporado a procesadores utilizados en bienes de diversa índole, tales como consolas, centrales telefónicas, telefonía celular, máquinas y otros dispositivos.
  - Actividades no comprendidas:
    - La solución de problemas técnicos que se hayan superado en proyectos anteriores sobre los mismos sistemas operativos y arquitecturas informáticas.
    - El mantenimiento, la conversión y/o traducción de lenguajes informáticos, la adición de funciones y/ o preparación de documentación para el usuario, garantía o asesoramiento de calidad de los sistemas no repetibles existentes.
    - Actividades de recolección rutinarias de datos, la elaboración de estudios de mercado para la comercialización de software.
    - Actividades ligadas a la producción de software que no conlleven un progreso funcional o tecnológico en el área del software.
  - Si tuvieran otra actividad paralela, no relacionada con el desarrollo de software se deberá llevar su contabilidad de manera tal que permita la determinación y evaluación en forma separada de la actividad promovida del resto de las desarrolladas.
- Estar constituido como persona física/jurídica en la República Argentina.
- Tener CUIT y clave fiscal nivel 2 en AFIP.
- Contar con Trámites a Distancia (TAD) asociado a AFIP (online y gratuito).
- Estar en curso normal de cumplimiento de sus obligaciones impositivas y previsionales.
- Cumplir con alguna norma de calidad reconocida aplicable a los productos de software (Si en el momento inscripción se encuentra en proceso de certificación para la obtención de alguna norma

de calidad, hay un plazo de tres (3) años para presentar la certificación, contado desde el momento de su inscripción).

El Incumplimiento de normas podría:

- Revocar la Inscripción.
- Inhabilitar para inscribirse nuevamente en el registro.
- Pagar los tributos no ingresados, más los intereses.

## Ley de Economía Del Conocimiento

Como agregado, aprovecho para comentarles sobre esta nueva ley que se aprobó el día 22/5/19.

Esta Ley, que es continuación de la de Software que vencía este año, otorga un marco tributario a las **11.000 empresas** que brindan servicios basados en el conocimiento incluyendo software, electrónica, producción audiovisual, industria satelital y biotecnología, permitiéndonos competir globalmente, duplicar el empleo en el sector y multiplicar las exportaciones para que lleguen a **US\$ 15 mil millones** en 2030.

Estas actividades son las más dinámicas de nuestra economía: el empleo entre 2007-2017 creció **65%** más que en el resto de la economía y las ventas también crecieron en el mismo periodo un **70%** frente a un crecimiento general del 12%. Además, los salarios son un **35%** más elevados que en el resto.

### Financiación

Podremos solicitar “Subsidios a Emprendedores” a FONSOFT y así poder financiar nuestro proyecto con todo lo que necesitemos, como por ejemplo:

- Equipamiento
- Licencias
- Capacitación
- Insumos
- Consultorías

### Beneficios de la Ley de Economía del Conocimiento

La nueva normativa reduce los costos laborales para el sector, ya que adelanta el Mínimo no Imponible que la reforma tributaria prevé para el 2022. Además, otorga un bono de crédito fiscal transferible equivalente a 1.6 veces las contribuciones que debieran abonarse sobre ese mínimo no imponible. Este beneficio, puede utilizarse para cancelar impuestos nacionales, como IVA o Ganancias. Además, contempla una alícuota reducida del Impuesto a las Ganancias del 15%.

Por otro lado, la ley estipula que los exportadores que hayan abonado o se le hayan retenido impuestos similares al Impuesto a las Ganancias en el país destino de la exportación, podrán deducir lo pagado contra el impuesto a las Ganancias, obteniendo un alivio fiscal.

También, fomenta la creación de nuevas empresas. A partir de ahora, aquellas empresas con una antigüedad menor a 3 años, y categorizadas como MICRO en el Registro Pyme, pueden ser una actividad elegible acreditando solamente el 70% de su facturación sin necesidad de cumplimentar otros requisitos.

Por último, entre otros beneficios, la normativa implica una mayor estabilidad fiscal para sus beneficiarios ya que no podrán ver aumentada su carga tributaria total nacional a partir la inscripción en el Registro y durante toda la vigencia del mismo, incluyendo los derechos de exportación.

## Patentamiento del Software

### ¿Por qué registrar un software?

Quien registra su obra de software accede a determinados beneficios. Quien registra su obra de software accede a determinados beneficios:

- **Seguridad:** lo que ingresa en el Registro de Derecho de Autor adquiere, mediante el acto administrativo que significa su admisión, luego de un examen, certeza de su existencia en determinada fecha, en lo que hace a su autor y contenido. Si se trata de un contrato, certeza de la fecha, contenido y partes contratantes.
- **Prueba de Auditoría:** es una presunción de autoría que otorga el Estado, con una fecha cierta de inscripción.
- **Elemento de comparación:** el registro en la Dirección Nacional de Derechos de Autor sirve de elemento de comparación en supuestos de plagio y piratería. En esos supuestos, la obra es remitida al Poder Judicial para su valoración.
- **Protección del Usuario de buena fe:** se presume autor de la Obra el que figura como tal en el certificado de registro, salvo prueba en contrario. El autor que publicara la obra conforme a las constancias que obran en la Dirección Nacional de Derechos de Autor, quedaría eximido de responsabilidad penal, en el supuesto de que se presente el verdadero autor reclamando sus derechos.
- **Publicidad de las obras y contratos registrados:** función primordial de un registro es dar a conocer su contenido. La información beneficia a todo aquel que tiene interés en oponer su derecho frente a terceros y a quienes buscan cerciorarse sobre la viabilidad y legitimidad en una contratación.
- Tratándose de una obra inédita publicada, ante cualquier duda, extravío o conflicto, siempre existe la posibilidad de requerir la apertura de sobre y obtener el contenido certificado por la Dirección Nacional del Derecho de Autor.

### Propiedad Intelectual

Los mecanismos de Propiedad Intelectual (PI) son una importante herramienta para el desarrollo y la transferencia de tecnología. Sirven para proteger los resultados de investigación y para obtener tecnologías resguardadas, susceptibles de ser transferidas.

¿Cómo proteger una invención o un resultado de investigación?

A través de una Patente de Invención, derecho exclusivo que concede el Estado al creador de una invención, por el cual se impide a terceros no autorizados realizar actos de fabricación, uso, oferta para la venta, venta o importación del producto objeto de la patente o producto obtenido directamente por medio del procedimiento objeto de la patente.

## Ley de Patentes de Invención

Una Patente de Invención es un derecho exclusivo que concede el Estado al creador de una invención, por el cual se impide a terceros no autorizados realizar actos de fabricación, uso, oferta para la venta, venta o importación del producto objeto de la patente o producto obtenido directamente por medio del procedimiento objeto de la patente.

Este derecho es territorial, es decir que la protección sólo alcanza el territorio del Estado que ha concedido la patente, y temporal por un período de 20 años desde la solicitud de la patente.

Para que una invención sea susceptible de ser protegida por patente, la misma debe cumplir tres criterios básicos establecidos por la Ley:

- Novedad.
- Actividad inventiva.
- Aplicación Industrial.

Tener en cuenta que:

- **Titularidad de la patente:** El titular de la Propiedad Intelectual resultante de la actividad de los científicos del CONICET es el propio Consejo y la institución contraparte (en casos de doble dependencia).
- **Patentar no es contrario a publicar.** Son acciones complementarias, aunque es necesario presentar la solicitud de patente y luego divulgar la información en revistas científicas, congresos, tesinas, tesis, etc.
- **Beneficios económicos:** Quienes participen en la invención y desarrollo del conocimiento (inventores) podrán percibir los frutos económicos que provengan de la explotación comercial de la propiedad intelectual licenciada a terceros.
- **Inventor no es sinónimo de autor de una publicación.** Inventor es toda aquella persona que realiza un aporte intelectual a la invención.



## Ley Protección de datos personales

(Ley 25.326)

Sancionada en el año 2000, durante el gobierno de Fernando de la Rúa y reglamentada en el año 2001 con el decreto 1558/01 en cumplimiento de la Ley N° 25.326 para la efectiva protección de los datos personales.

La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal. En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas.

### ¿Qué es dato Personal?

Dato personal es información que nos identifica o nos puede hacer identificables. La protección de datos no se refiere solo a datos íntimos, sino a cualquier tipo de dato que identifique o permita la identificación de una persona, y esté en conocimiento o tratamiento de terceros. Dato personal es el nombre, DNI, una fotografía o una grabación de voz, la IP, un pin de teléfono, un avatar, la dirección de email, el CV, la orientación sexual, la condición de consumidor de un producto o de cliente de una empresa, la situación crediticia, un diagnóstico, el historial médico, los hábitos de consumo, la cuenta de banco, la afiliación a un club o red social, etc.

### ¿Qué tipos de datos personales hay?

#### Datos de Identificación

Nombre, apellido, domicilio, teléfono, PIN, correo electrónico, firma, DNI, CUIT/L, fecha de nacimiento, edad, nacionalidad, estado civil, sexo, imagen, dirección de IP, etc.

#### Datos Laborales

Puesto, empleador, domicilio, correo electrónico institucional, teléfono del trabajo, legajo, nómina, sanciones, licencias, seguridad social, aportes, historial en la empresa

#### Datos Patrimoniales

Información fiscal, historial crediticio, cuentas bancarias, ingresos y egresos, información de consumos, situación de solvencia, etc.

#### Datos Académicos

Curriculum vitae, trayectoria educativa, títulos, matriculas habilitantes, certificados, condición de alumno, calificaciones, etc.

#### Datos Ideológicos

Creencias religiosas, afiliación política, sindical, pertenencia a organizaciones de la sociedad civil, asociaciones religiosas.

## **Datos de Salud**

Estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico, psiquiátrico, régimen de licencias, etc.

## **Características Personales y Físicas**

Tipo de sangre, ADN, huella digital, altura, peso, discapacidades, color de piel, iris y cabellos, señales particulares, etc.

## **Vida y Hábitos Sexuales**

Origen étnico y racial, orientación sexual, análisis de perfiles, etc.

## **Definiciones**

A los fines de la presente ley se entiende por:

- **Datos personales:** Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.
- **Datos sensibles:** Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.
- **Archivo, registro, base o banco de datos:** Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.
- **Tratamiento de datos:** Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos 2 personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.
- **Responsable de archivo, registro, base o banco de datos:** Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos.
- **Datos informatizados:** Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado.
- **Titular de los datos:** Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley.
- **Usuario de datos:** Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos.
- **Disociación de datos:** Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable.

## Categoría de datos

1. Ninguna persona puede ser obligada a proporcionar datos sensibles.
2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.
3. Prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros
4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas

## Datos relativos a la salud

Los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional.

## ¿Qué obligaciones debe cumplir el titular de una Base de Datos?

Las principales obligaciones a cargo del Responsable son:

- Cumplir el deber de informar.
- Recabar el consentimiento.
- Registrar sus bases de datos
- Disponer de un Documento de Seguridad o Manual de Protección de Datos.
- Contar con el Flujo o Arquitectura de Datos Personales.
- Capacitar a su personal.
- Definir un procedimiento para la tutela de derechos ARCO.
- Regularizar movimientos y accesos de datos de terceros.
- Regularizar movimiento y tratamiento de datos dentro de la empresa

## ¿Qué son los derechos ARCO?

ARCO es la sigla para identificar los derechos que tiene el titular de los datos personales respecto de quienes tratan sus datos: acceso, rectificación/ actualización, cancelación, supresión, y oposición. Las empresas deben habilitar un procedimiento de tutela de derechos mediante el que se garantice a sus clientes la efectiva respuesta a sus derechos ARCO.

## Seguridad de los datos

El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

Un sistema informático puede ser protegido desde un punto de vista lógico o físico.

Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota.

En el caso de los virus hay que subrayar que en la actualidad es amplísima la lista de ellos que existen y que pueden vulnerar de manera palpable cualquier equipo o sistema informático. Así, por ejemplo, nos encontramos con los llamados virus residentes que son aquellos que se caracterizan por el hecho de que se hallan ocultos en lo que es la memoria RAM y eso les da la oportunidad de interceptar y de controlar las distintas operaciones que se realizan en el ordenador en cuestión llevando a cabo la infección de programas o carpetas que formen parte fundamental de aquellas.

De la misma forma también están los conocidos virus de acción directa que son aquellos que lo que hacen es ejecutarse rápidamente y extenderse por todo el equipo trayendo consigo el contagio de todo lo que encuentren a su paso.

Los virus cifrados, los de arranque, los del fichero o los sobre escritura son igualmente otros de los peligros contagiosos más importantes que pueden afectar a nuestro ordenador.

Entre las herramientas más usuales de la seguridad informática, se encuentran los programas antivirus, los cortafuegos o firewalls, la encriptación de la información y el uso de contraseñas (passwords).

Un sistema seguro debe ser íntegro (con información modificable sólo por las personas autorizadas), confidencial (los datos tienen que ser legibles únicamente para los usuarios autorizados), irrefutable (el usuario no debe poder negar las acciones que realizó) y tener buena disponibilidad (debe ser estable).

De esta forma, y teniendo en cuenta la ley de protección de datos personales, es importante que un sistema informático cuente con una buena seguridad de datos, ya que una empresa al contratar un software, por lo general brinda sus datos personales a los desarrolladores, confiando que los mismos no van a ser divulgados ni estafados por terceros (a menos que como el artículo 5 de dicha ley dice, el cliente/empresa dé su consentimiento a la viralización de sus datos).

## ¿Quién controla que se cumpla la Ley?

La Dirección Nacional de Protección de Datos Personales (DNPDP) es el órgano del gobierno de la República Argentina encargado del control de la Ley de Protección de datos personales (ley 25.326)

Su sede se encuentra en la Ciudad Autónoma de Buenos Aires. Es un organismo que tiene a su cargo el Registro Nacional de las Bases de Datos, instrumento organizado a fin de conocer y controlar las bases de datos que circulan en el país y que pertenece a la órbita del Ministerio de Justicia, Seguridad y Derechos Humanos.

Además, es asesora y asiste a los titulares de datos personales recibiendo las denuncias y reclamos efectuados contra los responsables de los registros, archivos, bancos o bases de datos por violar los derechos de información, acceso, rectificación, actualización, supresión y confidencialidad en el tratamiento de los datos. Las denuncias que se hagan ante la DNPDP, son al exclusivo efecto de revelar deficiencias o incumplimientos a las normas aplicables en el tratamiento de los datos personales que hagan los archivos, registros bancos o bases de datos.

Mediante el Decreto 746/2017 en su artículo 19 indica que la Agencia de Acceso a la Información Pública actuará como Autoridad de Aplicación de la Ley de Protección De Datos Personales N° 25.326.

## Ley de Delitos Informáticos

El 4 de Junio de 2008 se sancionó la ley de Delitos Informáticos. Dicha ley pena los siguientes delitos informáticos:

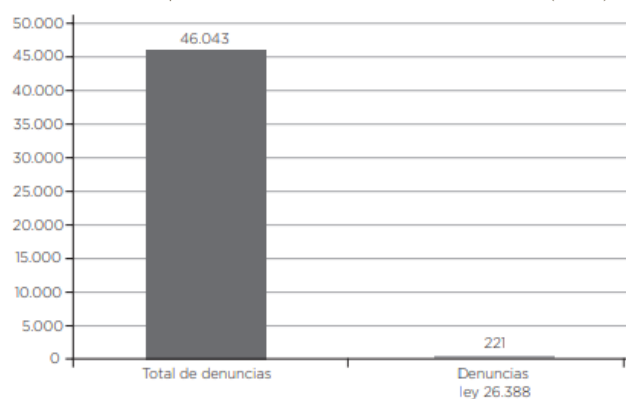
- Pornografía infantil por Internet u otros medios electrónicos.
- Violación, apoderamiento y desvío de comunicación electrónica.
- Intercepción o captación de comunicaciones electrónicas o telecomunicaciones.
- Acceso a un sistema o dato informático.
- Publicación de una comunicación electrónica.
- Acceso a un banco de datos personales.
- Revelación de información registrada en un banco de datos personales.
- Inserción de datos falsos en un archivo de datos personales.
- Fraude informático.
- Daño o sabotaje informático.

### Cómo afectaría

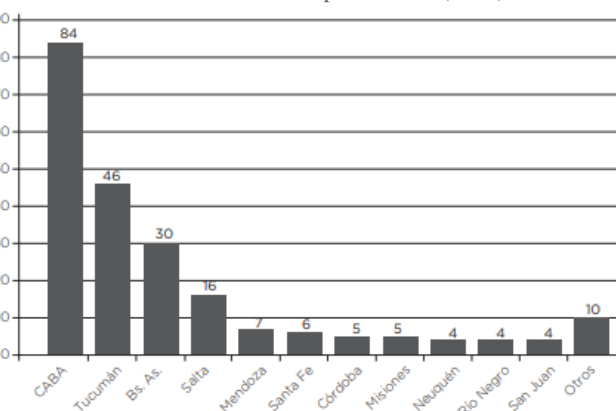
En un principio, nuestra aplicación se limitaría al consumo interno de un comercio, es decir, no estaría abierto al público, por lo tanto, no se vería afectada por ninguno de los delitos informáticos mencionados. Pero si la aplicación se expandiera, y tuviera un módulo de **E-Commerce**, abierto al público, podrían existir litigios con los usuarios por intentos de penetración al sistema (Xploits), explotación de posibles fallas en los canales de comunicación (Hacking) o simple ingeniería social (Phishing).

### Estadísticas

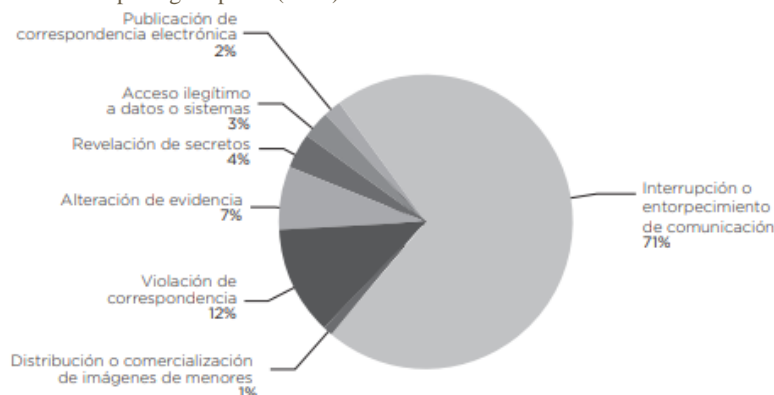
Total Denuncias | Total Denuncias Delitos Informáticos (2013)



Denuncias Delitos Informáticos por Distrito (2013)



Total Denuncias Delitos Informáticos por figura penal (2013)



## Casos de Delito Informático

Desde que existen las transacciones virtuales, los sistemas han sido atacados para utilizar dichas transacciones y beneficiarse de su fin, sin invertir dinero. Otros ataques son para hallar vulnerabilidades y así informar al desarrollador para prevenir el mismo, ¿pero qué pasa cuando no se informa?

Desde 1985 en EEUU se condenan a los cibercriminales, y 9 años más tarde se condenó el primer delito informático “Famoso”:

- **1994:** *Kevin Poulsen* fue condenado a 51 meses al ser encontrado culpable de lavado de dinero y obstrucción de la justicia valiéndose de medios tecnológicos.
- **1995:** *Chris Pile* fue condenado en el Reino Unido a 18 meses de cárcel al ser encontrado culpable de crear y distribuir códigos maliciosos. Dentro de los códigos maliciosos se encuentran los virus *Pathogen* y *Queeg* que se cargaban en memoria para afectar los programas que estuvieran en ejecución.
- **1999:** *Kevin Mitnick* debió permanecer 68 meses en la cárcel después de ser encontrado culpable de interceptar comunicaciones y estar relacionado con otros delitos de fraude.
- **2002:** *David L. Smith* fue condenado a 20 meses de prisión, después de que se declarara culpable de crear y propagar códigos maliciosos. Específicamente fue el creador de *Melissa* uno de los virus que más daño a causado en Internet al afectar miles de cuentas de correo electrónico.
- **2004:** *Adam Botbyl* fue condenado con 26 meses de cárcel después de que fuera encontrado culpable de robar números de tarjetas de crédito de una conocida cadena de almacenes después de que logró acceder a los sistemas de la empresa conectándose a través de una red WiFi. Al lograr el acceso lo utilizó para modificar porciones de código de los programas utilizados por los empleados.
- **2004:** *Max Ray Vision* fue condenado a 108 meses, una de las condenas más largas que se ha visto hasta el momento por un delito informático. En este caso el delito también estaba relacionado con el robo de información financiera: alrededor de dos millones de tarjetas de crédito.
- **2006:** *Jeanson James Ancheta* fue condenado a 57 meses por llevar a cabo ataques de denegación de servicios (**DoS**) utilizando cientos de *computadoras zombies*.
- **2012:** *James Jeffery* fue condenado a 32 meses por llevar a cabo un acceso indebido al sitio web de una entidad que facilitaba servicios de aborto en Reino Unido, para robar información de usuarios y hacer un defacement de la página.
- **2012:** *Albert Gonzalez* fue condenado a 240 meses la pena más larga impuesta hasta el momento a un cibercriminal. Albert fue el responsable de uno de los fraudes más grandes de la historia, utilizando técnicas de **SQL injection** logró robar alrededor de 170 millones de números de tarjetas de crédito y claves de cajeros automáticos.
- **2013:** *Lewys Martin* fue condenado a 24 meses luego de que fuera encontrado culpable de accesos no autorizados a diversos sistemas. Dentro de los sistemas vulnerados se encuentran prestigiosas *universidades inglesas*, *sitios de policía* y *gubernamentales del Reino Unido* y otros sitios de *departamentos oficiales del gobierno de Estados Unidos*.
- **2017:** *Emanuel Vélez Cheratto* (“**Líbero**”), nacido en Córdoba, fue condenado a 3 años y 2 meses de prisión efectiva por ser el autor de reiteradas estafas vinculadas a las tarjetas de crédito.

## Ley de Seguridad Informática

Se entiende a la seguridad informática como el proceso de prevenir y detectar el uso no autorizado de un sistema informático. La seguridad informática es en realidad una rama de un término más genérico que es la seguridad de la información, aunque en la práctica se suelen utilizar de forma indistinta ambos términos.

Los primeros pasos se dieron con la resolución 669/2004 el 20 de diciembre de 2004, la cual establecía que el Sector Público Nacional debe adecuar y actualizar sus políticas de seguridad informática; conformar comités y darles sus responsabilidades relacionadas.

Las siguientes resoluciones fueron:

- Resolución 45/2005, de la Subsecretaría de la Gestión Pública, de 24 de junio de 2005. Faculta al Director Nacional de la Oficina Nacional de Tecnologías de Información a aprobar la Política de Seguridad de la Información Modelo y dictar las normas aclaratorias y complementarias que requiera la aplicación de la Decisión.
- Disposición 6/2005, de 3 de agosto de 2005, de la Oficina Nacional de Tecnologías de la Información (ONTI) que aprueba la Política de Seguridad de la Información Modelo.
- Disposición 11/2006, de 19 de septiembre de 2006, de la Dirección Nacional de Protección de Datos Personales, que adopta medidas de Seguridad para el Tratamiento y Conservación de los Datos Personales.
- Disposición 12/2010, de 18 de junio de 2010, de la Dirección Nacional de Protección de Datos Personales, que regula los Datos Sensibles y aplicación del proceso de disociación.
- Disposición 5/2015, de 10 de noviembre de 2015, de la Jefatura de Gabinete, por la que se crea el “Registro de Equipos de Respuesta ante Incidentes de Seguridad Informática”

Actualmente, en nuestro país, la ley 26.388 en su artículo 8, tiene como penas de 1 mes a 2 años de cárcel para quienes *“A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales”*, en caso de ser funcionario público, también cuenta con 1 a 4 años de inhabilitación de ocupar cargos públicos.



## Medidas para el mantenimiento de la seguridad informática y la prevención de intrusiones

Los ataques más utilizados en contra de un sistema informático son los troyanos, los gusanos y la suplantación y espionaje a través de redes sociales. También son populares los ataques DOS/DDoS, que pueden ser usados para interrumpir los servicios (esto viene quedando en desuso ya que los nuevos router y firewalls vienen con protocolos de seguridad que los rechazan). La creación de roles y usuarios definidos dentro de las empresas y organizaciones pueden prevenir que los mismos integrantes de dichas instituciones sean los causantes de este abuso; a nivel gerencial, las llaves “dobles”, es decir, los passwords de seguridad tienen una combinación de palabras de varias personas.

Las medidas de seguridad informática que puedes tomar incluyen:

- **Asegurar la instalación de software legalmente adquirido**: por lo general el software legal está libre de troyanos o virus.
- **Suites antivirus**: con las reglas de configuración y del sistema adecuadamente definido.
- **Hardware y software cortafuegos**: los firewalls ayudan con el bloqueo de usuarios no autorizados que intentan acceder a tu computadora o tu red.
- **Uso de contraseñas complejas y grandes**: las contraseñas deben constar de varios caracteres especiales, números y letras. Esto ayuda en gran medida a que un hacker pueda romperla fácilmente.
- **Cuidado con la ingeniería social**: a través de las redes sociales los ciberdelincuentes pueden intentar obtener datos e información que pueden utilizar para realizar ataques.
- **Criptografía, especialmente la encriptación**: juega un papel importante en mantener nuestra información sensible, segura y secreta.

## FUENTES:

- Portal oficial del Estado argentino, (02/06/19) Acceder a los beneficios de la Ley de Promoción de Software: Argentina.gob.ar ([LINK](#))
- Julián Pérez Porto y María Merino. (2008) Definición de: Seguridad informática ([LINK](#))
- ABOGADOS PORTALEY, (26/06/2008) La incorporación de los delitos informáticos al Código Penal argentino ([LINK](#))
- Dirección Nacional del Sistema Argentino de Información Jurídica, (2013) Una aproximación a la estadística criminal sobre delitos informáticos ([LINK](#))
- Camilo Gutiérrez Amaya, (12/11/2013) Top 10 de condenados por delitos informáticos: ¿quiénes fueron los primeros de la historia? ([LINK](#))
- Seguridad Informática Argentina. (07/12/2016) Legislación Argentina, Seguridad Informática ([LINK](#))
- ¿Qué es la seguridad informática y como puede ayudarme? (21/03/2018) Seguridad informática y prevención ([LINK](#))
- Código Penal Argentino. (04/06/2008) Ley 26.388 de Delitos Informáticos ([LINK](#))
- CESSI Argentina. (2019) Registro De Software ([LINK](#))
- Consejo Nacional de Investigaciones Científicas y Técnicas. Propiedad Intelectual ([LINK](#))
- Clarín (23/05/2019) Ley de Economía del Conocimiento ([LINK](#))
- Portal oficial del Estado argentino, (02/06/19) Acceder a los beneficios de la Ley de Promoción de Software: Argentina.gob.ar ([LINK](#))