Revista

INTEGRACIÓN

Edición VI 2018, ISSN 2309-4516

UNIVERSIDAD DE SONSONATE
USO
SCIENTIAE ET BONIS ARTIBUS

USO EDITORES

MISIÓN UNIDAD DE INVESTIGACIÓN

Somos la unidad de investigación que promueve y sistematiza la cultura de investigación de manera interactiva, multi e inter disciplinaria y en vínculo con las comunidades académicas y sociales del país, para propiciar la creación, adaptación, generación, y transferencia de conocimientos que se constituyen en alternativas viables e innovadoras ante problemas y expectativas prioritarias para el El Salvador.

Estructura Organizacional del
Comité Técnico Editorial:

Dr. Francisco Carlo Arévalo Herrera
Vice-rector y Director del Sello Editorial

Mauricio Vega
Jefe de Investigación

René Francisco Lara
Jefe de Proyección Social

Karen Escalante
Corrección de Estilo

Diseño: Talleres Gráficos UCA
Impreso en Talleres Gráficos UCA, 2019.
Publicaciones de este ejemplar:300

La producción intelectual de la Universidad de Sonsonate se define como un medio para poner al alcance de la comunidad, la cultura y el conocimiento científico, además fue establecida como una actividad propia del Comité Técnico Editorial de publicaciones impresas, quien recibirá y analizará prospectos de publicaciones para posterior divulgación.

CONTENIDO

CARTA EDITORIAL

Apreciado lector:

La Universidad de Sonsonate se honra en presentar a usted la sexta edición de nuestra revista INTEGRACIÓN; espacio dedicado a exponer temas de investigación científica en distintas áreas del conocimiento. Esta edición es el resultado del esfuerzo que investigadores de la Facultad de Ingeniería y Ciencias Naturales, y de la Facultad de Ciencias Jurídicas han realizado con el fin de aportar conocimiento a la realidad nacional de El Salvador.

En ese sentido, se presenta un artículo relacionado a la teoría general de los medios de impugnación, lo que en la vida jurídica es de relevancia, pues se pretende sentar la base teórica de los principales recursos para la respuesta a resoluciones judiciales, que sean comprendidos, tanto por el sujeto juzgado como por el administrador de derecho y así, facilitar su aplicabilidad. Es un tema jurídico pero de interés social que propende por la ampliación del conocimiento colectivo.

También la revista recoge tres aportes del área de informática que lo que pretende por un lado, es presentar un modelo en que la búsqueda de elementos, en archivos o documentos electrónicos sea más útil y pertinente para el usurario, de tal manera que minimiza el tiempo y eficientiza resultados de búsqueda. Los otros dos temas tienen que ver con la seguridad en el desarrollo de aplicaciones web y la implementación de la firma o certificación digital, que prioriza cibersociedades más seguras, fidedignas y legales.

El objetivo que la revista persigue es contribuir a la socialización del conocimiento generado hacia diferentes sectores de la sociedad, orientado tanto a problemáticas nacionales como a la realidad de países de características similares de la región.

Existe plena seguridad de que los artículos publicados en esta oportunidad muestran formas de trabajo innovadoras que serán de gran utilidad e inspiración para todos los lectores, ya sean académicos o profesionales. Finalmente espero que los aportes entregados en este medio tengan la recepción que se merecen.

Lcda. María de los Ángeles Rodríguez.

Rectora

Apuntes sobre la teoría general de los medios de impugnación

Carlos Manahen Méndez Hernández
carlos.mendez@usonsonate.edu.sv
Facultad de Ciencias Jurídicas-Universidad de Sonsonate

Resumen

Dentro de los medios de impugnación se encuentran los principales recursos (revocatoria, apelación, casación y revisión de la cosa juzgada) que constituyen los mecanismos por medio de los cuales se atacan las diversas resoluciones de los funcionarios judiciales, con el fin de corregir bien la malicia del Juez o bien los errores que en la aplicación del derecho o sustanciación del procedimiento puedan suscitarse en los procesos jurisdiccionales, objetivo del presente trabajo, para cuyos efectos se plasman una serie de aspectos doctrinarios, legales y jurisprudenciales, que en un contexto general aportan los conocimientos esenciales acerca de los medios de impugnación, a partir de los cuales se fija, entre otras cosas, su definición, principios, fundamento constitucional, requisitos, clases, efectos y otros aspectos que deben tenerse en cuenta al momento de la formulación de un medio de impugnación o recurso, y obtener así lo que con estos se pretende.

Palabras claves
recurso, medio de impugnación, apelación, agravio.

Abstract

Whitin the means of impugnation there are the principal sources as - revocation, appeal, cassation and review of the judged thing - which constitute the mechanisms that help to attack the many resolutions given by judicial officers, in order to correct the malice of the Judge or the errors that in the application of the right or substance of the procedure may arise during the jurisdictional processes, the primary objective of the present work, for whose effects are reflected into a serie of doctrinal, legal and jurisprudential aspects, which in a general context contribute to the essential knowledge about the means of impugnation which is based on, among other things, its definition, principles, constitutional basis, requirements, classes, effects and other aspects that must be taken into account at the time of formulation of a means of impugnation or appeal, in order to obtain what we are aiming on.

Keywords:
Resource, means of impugnation, appeal, grievance.

Presentación

Los presentes apuntes tienen por objeto aportar, a la comunidad jurídica y en especial a los estudiantes de la carrera de licenciatura en ciencias jurídicas, una serie de aspectos dogmáticamente coherentes con los conceptos jurídicos referentes a la teoría general de los medios impugnativos, necesarios para la comprensión y posterior estudio de cada uno de los medios de impugnación en particular, es decir, que buscan coadyuvar al posterior análisis y evaluación de estos tomando como fundamento legal los ordenamientos jurídicos en el ámbito civil y mercantil, penal y familia; además de los fundamentos doctrinarios y jurisprudenciales.

De ahí que la presente información pretenda ser un texto tanto práctico como didáctico para cualquier interesado en conocer y aplicar los conceptos básicos acerca de los medios de impugnación.

INTRODUCCIÓN

Partiendo de un general desarrollo conceptual, este documento trata la parte teórica o dogmática que científicamente fundamenta los principales medios de impugnación y, que en ese contexto, orientan el derecho positivo en la configuración de los diferentes mecanismos de impugnación formalmente conocidos como recursos. Como base teórica se delimitan o definen los conceptos tales como: medio de impugnación y recurso; determinando su diferencia, condiciones, formas o modos de incoación, consecuencia o efectos jurídicos dimanados de los mismos. En este contexto dogmático se consignan también fundamentos jurisprudenciales, legales y doctrinarios que positivasen el uso práctico y didáctico de tales mecanismos de ataque, haciéndose una especial referencia a cada uno de los recursos o medios de impugnación que usualmente tienden a regular los distintos ordenamientos jurídicos.

CONCEPTO DE MEDIO DE IMPUGNACIÓN Y DIFERENCIA CON LOS RECURSOS

El proceso para el conocimiento de la pretensión se sujeta a distintos grados de conocimiento; es en ese orden que un proceso se pueda contraer a un procedimiento en primera y segunda instancia, así como a un tercer grado de conocimiento vía casación donde ya no constituye instancia. En este contexto, instancia no es otra cosa que la prosecución del proceso desde la interposición de la demanda hasta que concluye ordinaria o extraordinariamente, decidiendo o no acerca del fondo del asunto, es decir, de la pretensión y de la conducta que adopta el sujeto frente a quien se plantea la tutela jurídica, para algunos cuando tal decisión se encuentra debidamente comunicada. Así mismo, la instancia comprende la prosecución del proceso desde que se introduce un medio de impugnación o recurso ante un tribunal superior hasta que el mismo es decidido o resuelto.

En el primer supuesto estamos frente a la primera instancia. Con el planteamiento de un medio de impugnación consistente en un recurso ordinario (apelación), se abre paso a la segunda instancia y, con la incoación de un recurso extraordinario (casación) se abre paso a un tercer grado de conocimiento, que como se dijo, esta nueva vía cognitiva ya no constituye instancia.

Dicho esto, cabe precisar que el vocablo impugnación proviene del latín *impugnare*, que significa *atacar o asaltar*; consecuentemente, en una acepción amplia los medios de impugnación son todos los mecanismos de que disponen los sujetos procesales o partes, o bien un tercero interesado que haya intervenido o no en el proceso, para atacar las resoluciones o providencias judiciales, comprendiendo cualquier medio de ataque u oposición.

Parte de esos medios de impugnación son los llamados *recursos*, a los que en la mayoría de los casos se refiere nuestro ordenamiento jurí-

dico, utilizando en muchos de los casos, indistintamente los términos medio de impugnación o recurso como si fueran sinónimos, cuando se trata de dos conceptos distintos; ello porque, como ha quedado consignado, medio de impugnación implica cualquier forma o mecanismo de ataque, se trate o no de un recurso, pues éste es simplemente una parte de esa generalidad impugnativa. De ahí que entre medio de impugnación y recurso exista una relación de género a especie, en donde los primeros son el género y los segundos una especie de ese género, pudiéndose afirmar desde esta perspectiva, que todo recurso es un medio de impugnación, pero no todo medio de impugnación es un recurso.

A partir de lo expresado, para ciertos procesalistas, recurso es el medio de impugnación que tienen las partes para obtener que se rectifique mediante revocación, modificación o anulación, los errores cometidos por los Funcionarios Judiciales al tomar cualquier decisión, ya sea que se produzca como consecuencia equivocada de la aplicación de la norma sustancial o material, o bien por inobservancia de las formas procesales. Implica, según lo señalado, un ataque a la eficacia de las decisiones o providencias judiciales.

Couture (1977, p. 339) señala que los recursos generalmente hablando son medios de impugnación de los actos procesales. Explicando que realizado el acto, la parte agraviada por él, tiene dentro de los límites que la ley le confiere antes que haya prelucido su derecho, poderes de impugnación destinados a promover la revisión del acto y su eventual modificación o anulación.

Generalmente, los principales recursos son el ordinario llamado apelación y el extraordinario conocido como casación; sin embargo, en la mayoría de los casos se añaden como recursos la revocatoria y la revisión de la cosa juzgada, a los que en adelante nos referiremos para fundamentar normativa o legalmente los conceptos que aquí se verterán.

FUNDAMENTO CONSTITUCIONAL DE LOS MEDIOS DE IMPUGNACIÓN

Sobre el fundamento constitucional de los medios impugnativos, la jurisprudencia constitucional sostuvo, en un primer momento, que estos no tenían una configuración constitucional propia; ello porque, no dimanan directamente de la constitución pues se encuentran incardinados en el derecho o garantía de audiencia; de ahí que, no toda negativa al acceso a un medio de impugnación deviene en inconstitucional, si el impugnante no cumple con los requisitos establecidos por la respectiva legislación ordinaria.

Actualmente, la nueva postura ha sostenido que, si bien es cierto dicha categoría jurídica se encuentra ligada al derecho de audiencia, posee sustantividad propia, agregándose que tal derecho se conjuga como todo el ordenamiento jurídico con el derecho a un proceso constitucionalmente configurado y el derecho de audiencia, en tal sentido, al consagrarse en la ley un determinado medio impugnativo, la negativa de acceder al mismo sin justificativo constitucional, cuando legalmente procede, deviene en una vulneración de ellos.

De lo expuesto, podemos acotar que no hay duda que el derecho de audiencia se encuentra íntimamente relacionado con el uso de los medios de impugnación, por una parte; por otra, que su ejercicio tiene como limitante las formas y requisitos que las respectivas leyes ordinarias consagran. En este orden, cuando injustificadamente se impide el uso de un medio impugnativo legalmente previsto se violenta el derecho de audiencia y demás derechos que de este se proyectan como el de defensa que ofrece el ser oído y vencido en juicio cuando sea procedente.

Los medios impugnativos o derecho a recurrir son un derecho de naturaleza constitucional procesal, en el sentido que si bien esencialmente dimana de la ley, también se ve constitucio-

nalmente protegido en cuanto constituye una facultad para los gobernados a fin de que tengan la posibilidad de agotar todos los medios para obtener una reconsideración de la impugnación por parte del tribunal superior en grado de conocimiento.

Consecuente con lo anterior, conforme al constitucionalista, cuando se examine el acceso a un determinado medio impugnativo establecido por el legislador contra las resoluciones recaídas en un concreto proceso, debe evitarse la imposición de requisitos e interpretaciones impeditivas u obstaculizadoras que resulten innecesarias, excesivas o carentes de razonabilidad o proporcionalidad respecto de los fines que lícitamente puede perseguir el legislador, o la imposición de condiciones o consecuencias meramente limitativas o disuasorias del ejercicio de tales medios impugnativos legalmente establecidos, pues de lo contrario, la negativa a los mismos, deviene en violatoria de la normativa constitucional.

REQUISITOS GENERALES PARA IMPUGNAR O RECURRIR

Como consecuencia del carácter constitucional procesal de los medios de impugnación, estos deben cumplir con ciertos requisitos o formalidades de orden legal u ordinario que habilitan su admisibilidad como tal; de ahí que todo mecanismo impugnativo, preliminarmente está sujeto a un examen formal de admisibilidad, que tiene por objeto determinar si en el acto de interposición del recurso o medio impugnativo, el impugnante observó o le dio cumplimiento a los requisitos fijados por los diferentes ordenamientos jurídicos secundarios, los que de no configurarse podrían llevar al rechazo in limine del mismo por la vía común de la inadmisibilidad, ante lo cual obviamente, ya no se pasaría al subsiguiente examen de fondo del recurso.

Que, como se ha dicho, tales condiciones formales de admisibilidad son fijados por las diferentes leyes procesales, siendo las comunes o generales, las que a continuación se enuncian:

a. **Taxatividad o especificidad.** Como consecuencia de este requisito, de orden objetivo, un medio impugnativo o recurso únicamente procede o tendrá lugar contra aquellas decisiones que la ley declare expresamente como impugnables o recurribles, tal como se puede desprender de los arts. 503, 508 y 519 del Código Procesal Civil y Mercantil (en adelante CPCM.); 452, 464, 468 y 479 del Código Procesal Penal (en adelante C. Pr. Pn.); 147, 150 y 153 de la Ley Procesal de Familia (en adelante L. Pr. Fam.).
b. **Legitimación activa**. Presupuesto de carácter subjetivo, en virtud del cual solo pueden incoar un medio de impugnación o recurso aquellos que tienen la calidad de partes o tercero interesado en el litigio objeto del proceso y, como tales, obligados a soportar los efectos procesales y materiales de la correspondiente decisión, que en consecuencia, a través de un medio impugnativo buscan la ineficacia de la misma. Arts. 501 Inc. 1°.,527 y 543 CPCM.; 452 Inc. 2°. y 490 C Pr. Pn. y 154 L. Pr. Fam.
c. **Agravio.** También constituye un requisito de orden subjetivo, sobre cuya base únicamente pueden impugnar o recurrir, aquella parte o tercero que recibe un perjuicio por la decisión objeto de impugnación. Este es un requisito que se encuentra estrechamente relacionado con el anterior, – legitimación activa – pues solo quien recibe un perjuicio con la decisión es la única legitimada activamente para recurrir. Arts. 501 In 1°, 527 y 543 CPCM.; 452 Inc. final y 464 Inc. 1° C Pr. Pn. y 154 L Pr Fam.

   Según la doctrina, el agravio o gravamen es aquel que resulta a raíz de las consecuencias negativas que reviste la resolución adoptada en relación con la

pretensión, pretensiones o resistencias planteadas en el proceso. De ahí que, dada la falibilidad de los administradores de justicia, pueda configurarse una compleja o diversidad de consecuencias negativas que causen agravio o perjuicio a los sujetos del proceso, caracterizando así dicho requisito para recurrir. Es por eso que el agravio constituye el principal fundamento de los medios de impugnación, pues lo que se busca es enmendar el daño causado a los injustamente agraviados, corrigiendo la malicia, ignorancia, impericia o negligencia de que pueda adolecer el ejercicio de la función jurisdiccional.

d. **Plazo.** Las leyes como consecuencia del principio de preclusión señala plazos dentro de los cuales se puede interponer o hacer uso del derecho a impugnar; de ahí que, concluido el respectivo plazo precluye tal derecho y la decisión adquiere firmeza y en ciertos casos se produce la calidad o efectos de cosa juzgada. Arts. 504 Inc. 1° , 511 Inc. 1°, 526, 544, 545 y 546 CPCM.; 462 Inc 1°, 465 Inc. 1°, 470 Inc. 1°, y 480 Inc. 1°, C Pr. Pn. y 156 L Pr. Fam.

   Debe señalarse que, siguiendo la regla general del cómputo de los plazos que se cuentan en días hábiles y a partir del día siguiente al de la notificación respectiva de la resolución que se impugna, tal como se prevé en los arts. 142 y 145 CPCM.; 167 y 168 C. Pr. Pn; 24 L. Pr. Fam., sin perjuicio de la forma en particular de como está redactado el art. 480 C. Pr. Pn. la cual deja entrever que en el caso de la casación penal, el plazo de interposición en esta clase de impugnación se computa a partir de la notificación, y no del siguiente a dicho acto de comunicación; situación que ya fue aclarada por la jurisprudencia, en el sentido que debe entenderse que es conforme a la regla general expresada, pues ello es consustancial con el debido y efectivo acceso a los medios impugnativos y, en consecuencia, con la concreción del derecho a la protección jurisdiccional o tutela judicial.

e. **Forma de interposición.** Debe señalarse que por regla general todo medio de impugnación o recurso deberá formularse por escrito, a excepción del recurso conocido como revocatoria que las leyes permiten que pueda formularse en forma oral, principalmente en el acto de las audiencias. Otra circunstancia vinculada a este presupuesto lo constituye la fundamentación del correspondiente medio impugnativo; de ahí que, todo recurrente deberá en el escrito de interposición, exponer con claridad y precisión las razones, motivos o argumentos que lo llevan a incoar un determinado medio de impugnación. Arts. 504, 507, 511 y 525 CPCM.; 462, 465 Inc. 1°, 470, 480 y 491 C. Pr. Pn.; 148, 151, 156 y 158 L. Pr. Fam.

f. **Lugar de interposición.** Sobre este requisito, la regla es que todo medio de impugnación o recurso deberá interponerse ante el tribunal que pronunció la resolución que se impugna; excepcionalmente, existe la llamada revisión de la cosa juzgada, que en el campo civil será planteada ante la Sala de lo Civil de la Corte Suprema de Justicia, es decir, ante el tribunal que conocerá del mismo, tal como lo prevé el art. 540 CPCM.; por otro lado, en el ámbito penal la interposición deberá hacerse ante el juez o tribunal que pronunció la resolución que causó ejecutoria, así lo dispone el art. 491 C Pr. Pn.

FUNDAMENTO DE LOS MEDIOS DE IMPUGNACIÓN

Uno de los fundamentos de los medios de impugnación se encuentra vinculado a la necesidad o interés social de que la actividad jurisdiccional o administración de justicia se cumpla

con el mayor o máximo de aciertos posibles, garantizándose así la seguridad jurídica de los gobernados, es decir, que con los medios de impugnación se persigue el perfeccionamiento de la actividad jurisdiccional; de ahí que ciertos procesalistas sostengan que los medios de impugnación constituyan mecanismos de perfección procesal, lo cual tiene sentido pues su objeto es corregir vicios que puedan contener las decisiones de los jueces y magistrados en el ejercicio de su función. Existe entonces con el uso de los medios de impugnación un concreto interés por la justicia.

Un segundo fundamento de los medios impugnativos o recursos lo constituye la falibilidad humana; como sabemos la actividad jurisdiccional o administración de justicia está en poder de personas, quienes por su naturaleza son falibles, es decir, la raza humana carece de perfección y como tal toda persona tiende a cometer errores o equivocaciones, las que como se dijo se buscan sanear o subsanar a través de los diferentes medios de impugnación o recursos, que implican diferentes grados de conocimiento por distintos órganos de la jurisdicción.

La falibilidad humana expresada, lleva entonces a un tercer fundamento de carácter jurídico de los medios de impugnación, cual es la necesidad de que se presenten las condiciones para que el acto impugnativo sea viable o procedente, estas se encuentran en los posibles vicios o errores cometidos por los funcionarios judiciales en el ejercicio de su función jurisdiccional, y que a través de los medios de impugnación es necesario reparar. En este orden, la doctrina señala dos tipos de errores que jurídicamente fundamente un medio de impugnación o recurso, siendo estos*: error in iudicando* o *error de derecho*, el cual versa sobre la incorrección en el juicio de fondo contenido en el respectivo pronunciamiento emitido dentro del proceso, es decir, en el derecho sustancial o relación jurídica material objeto de la relación jurídica procesal; consecuentemente, dicho error entre otros supuestos, podría configurarse cuando se interpreta erróneamente o se aplica indebidamente la ley. La segunda clase o tipo de error es el *error improcedendo* o *error en el procedimiento*, este recae sobre irregularidades en la actividad procesal donde se emitió la decisión, es decir, este error está relacionado con la forma o modo de realizarse los respectivos actos que componen el proceso, constituyendo por ello un vicio de forma y no de fondo.

EXTREMOS QUE DEMARCAN LA COMPETENCIA DEL TRIBUNAL QUE CONOCE ACERCA DE UN MEDIO DE IMPUGNACIÓN O RECURSO

De acuerdo con la naturaleza del medio de impugnación que fuere planteado, estos pueden ser del conocimiento del mismo tribunal que pronunció la resolución que se impugna (revocatoria), o bien de un tribunal distinto y superior a aquel que dictó la decisión (apelación); en este contexto, al funcionario judicial que le competa decidir acerca de un medio de impugnación o recurso, deberá tomar en cuenta o ceñirse a los limites siguientes:

1. Que la decisión que se adopte este circunscrita a los puntos fijados por el recurrente como motivos de agravio; de ahí que, el tribunal conocedor del medio de impugnación incoado, no puede ir más allá de los puntos o cuestiones planteados en el escrito contentivo del recurso o medio impugnativo fijados por el impugnante, constituyendo éstos un límite al respectivo pronunciamiento; dicho en otros términos, y retomando los elementos conceptuales de la congruencia, el Juez no puede ir más allá del petitorio, ni fundar su decisión en hechos diversos de los que han sido citados por las partes, en este caso del recurrente; de ahí la obligación de todo juzgador o sentenciador de pronunciarse sobre los puntos controvertidos (*tamtum devolutum cuantum apellatum)*. Arts.

515 Inc. 2°, 534 y 535 CPCM.; 467 Inc. 1°, 475 y 484 C. Pr. Pn.

2. La prohibición de la reforma en perjuicio o prohibición de la *reformatio in pejus o in peius*, que implica una prohibición al Juez que conoce de un medio de impugnación o recurso, de empeorar la situación del impugnante o recurrente, en los casos en los que no haya mediado recurso por su adversario, o sea, cuando la decisión ha sido impugnada solo en su interés. Arts. 502 CPCM. y 460 In 1° C. Pr. Pn. Es preciso señalar que en el expresado art. 460 en su Inc. 2°. C. Pr. Pn., se prevé la posibilidad de que los recursos interpuestos por el fiscal, el querellante o el acusador, permiten modificar o revocar la resolución aún a favor de su contraparte, que en este caso sería el imputado, que es lo que en doctrina se conoce como la imperatividad de la *reformatio in melius*.

CLASIFICACIÓN DE LOS MEDIOS DE IMPUGNACIÓN

Una de las clasificaciones acerca de los medios de impugnación que resulta congruente con nuestro ordenamiento jurídico es el siguiente:

1. Aquellos que según su naturaleza pueden ser ordinarios y extraordinarios. Los primeros son los que presentan mayor amplitud de conocimiento, por cuanto pueden proponerse tanto en primera como en segunda instancia, contra una diversidad de decisiones y por cualquier causa que los determine, con el objeto de subsanar errores en el derecho como en la actividad procesal o procedimiento. Entre estos se encuentran la revocatoria, y como principal medio de impugnación ordinario generador de instancia: el recurso de apelación. Arts. 503 ss. y 508 ss. CPCM.; 150 ss. y 153 ss., L Pr.Fam.; 461 ss. y 464 ss. C. Pr. Pn. Los extraordinarios son aquellos que solo proceden contra determinadas resoluciones judiciales y con base a los motivos o causas expresa o taxativamente previstas en la ley; como principal medio de impugnación extraordinario se encuentra el recurso de casación, arts. 478 ss. PC. Pr. Pn. y 519 ss. CPCM. Dentro de esta clase también se ubica al recurso de revisión, arts. 489 ss. C. Pr. Pn., y 540 ss. CPCM.

2. Otra clasificación que se hace acerca de los medios de impugnación es en atención al orden en que son decididos o resueltos, así se tienen principales y subsidiarios. Son principales aquellos que se interponen para ser considerados en primer lugar; y, subsidiario aquel cuya consideración dependerá del evento que no prospere el principal. En nuestro medio, dicha forma de interposición opera en el ámbito penal, en el supuesto de la revocatoria con apelación subsidiaria, tal como se prevé en el art. 463 C. Pr. Pn., y en materia de familia, según lo prescrito en el art. 150 Inc. 2°. L Pr. Fam. Que de acuerdo con la jurisprudencia, esta forma de interposición es un reflejo de la operatividad del principio de preclusión o con mayor precisión del principio de eventualidad; así como también una manifestación del principio de concentración, el cual pugna por la aproximación de los actos procesales y que las partes hagan uso de todos los medios de defensa que la ley en tal caso les franquea para que lo haga en forma simultánea a fin de impedir una acumulación suspensiva de impugnaciones que degeneren en la paralización innecesaria del proceso, de tal modo que el Juez, en forma concentrada, pueda resolver ambos recursos, según proceda. Debe precisarse que este modo de impugnación no opera en el ámbito civil y mercantil, pues el Código Procesal Civil y Mercantil se ha decantado por un único recurso.

3. También se tiende a clasificar a los medios de impugnación en atención al tribunal que los decide o resuelve, así se tienen medios de impugnación que resuelve el mismo tribunal que pronunció la resolución, como en el caso del expresado recurso de revocato-

ria, otros como la aclaración, adición o rectificación, arts. 146 Pr. Pn. y 225 y 226 CPCM.; y, por otro lado que resuelve o decide un tribunal distinto y superior de aquel que pronunció la resolución objeto de impugnación, como en los supuestos de la apelación, casación y revisión ya relacionados.

4. En otro orden, atendiendo a su forma de interposición encontramos medios de impugnación que se interponen de forma oral y de forma escrita; en este contexto, uno de los principales medios de impugnación que puede interponerse de forma oral y en el acto de las audiencias es el recurso de revocatoria, el resto de recursos se interponen por escrito. No obstante según lo prescrito en el art. 156 de la L. Pr. Fam., se prevé la posibilidad de proponer en forma verbal u oral una apelación contra una interlocutoria dictada en una audiencia o diligencia, ello a pesar del inconveniente que puede presentarse por la dificultad de esgrimir una adecuada fundamentación de hecho y de derecho del recurso en cuestión por la trascendencia de lo resuelto.

5. Finalmente, debe señalarse que en materia de familia se regula un típico medio de impugnación que es la apelación diferida, recurso que de acuerdo con lo prescrito en el art. 155 L. Pr. Fam., las apelaciones interpuestas durante el desarrollo o curso del proceso se acumularán para ser conocidas y decididas en la sentencias o resolución interlocutoria que le ponga fin al proceso haciendo imposible su continuación, es decir, que su decisión se difiere hasta la resolución que le da término al proceso, esto es beneficio para evitar dilaciones en el proceso a consecuencia de un medio de impugnación.

EFECTOS DE LOS MEDIOS DE IMPUGNACIÓN

Legal y doctrinariamente se identifican los siguientes efectos de los medios de impugnación:

a. Efecto devolutivo y no devolutivo.
b. Efecto suspensivo.
c. Efecto extensivo o comunicante.

a) Efecto devolutivo y no devolutivo

Cuando ante la interposición de un medio de impugnación o recurso, el conocimiento del mismo pasa ante un tribunal distinto y superior de aquel que pronunció la resolución objeto de impugnación, dejando éste de tener intervención en el proceso, estamos frente al efecto devolutivo, dando así mayores garantías al nuevo conocimiento y decisión del asunto, siendo este su principal fundamento. Figuran en estos medios de impugnación: la apelación, casación, entre otros.

Lo anterior implica que, cuando el tribunal que dictó la resolución impugnada es el competente para conocer del medio de impugnación, el efecto sería no devolutivo, como acontece en el caso del recurso de revocatoria.

Es de esta manera que, conforme al efecto devolutivo, una vez interpuesto el medio de impugnación o recurso, el juez que pronunció la resolución impugnada (*Juez a quo*), se desprende momentáneamente del proceso, asumiendo la competencia para conocer del mismo, el respectivo Tribunal Superior (*Juez Ad quem*); consecuentemente, presentado el medio de impugnación o recurso, la competencia del juez se circunscribe a notificar o bien a emplazar a la parte contraria en relación a dicha interposición, limitándose en lo consiguiente a remitir el escrito contentivo del mismo y demás actuaciones procesales al tribunal superior, tal como acontece en el ámbito patrimonial según lo dispuesto en los arts. 512 y 529 CPCM; en materia penal según los arts. 466, 471 y 483 del C. Pr. Pn., y art.

160 L Pr. Fam., lo cual no acontece cuando el efecto es no devolutivo.

En estos supuestos, corresponderá al tribunal superior no solo el conocimiento acerca del fondo o asunto planteado por el medio de impugnación correspondiente, sino también sobre el análisis o examen preliminar de las condiciones de admisibilidad del mismo, lo que técnicamente suprimió la interposición de hecho en el caso de la apelación, no obstante, aparece regulado en el ámbito de familia, lo cual estimo fue un error de técnica legislativa.

b) Efecto suspensivo

En cuando al efecto suspensivo, debe señalarse que este constituye la regla general de todo medio de impugnación, en el sentido que lo declarado en la resolución que se impugna se deja sin efecto hasta que el mismo se resuelve; dicho, en otros términos, la resolución recurrida o impugnada no puede ejecutarse mientras esté pendiente de resolución el correspondiente medio de impugnación o recurso, esto es, mientras esté abierto el trámite impugnativo. Art. 509 CPCM., 457 C. Pr. Pn.

En este caso, el efecto suspensivo cesara cuando la providencia judicial correspondiente alcance firmeza, por haberse resuelto la respectiva impugnación y no sea ya susceptible de ulterior recurso.

Consecuente con lo anterior, se afirma que el efecto suspensivo se fundamenta en el hecho de que una resolución mientras está sujeta a un medio de impugnación o recurso, no es inamovible o inmutable y, por consiguiente, puede ser modificada en su contenido principal; de ahí que, de ejecutarse, o no suspenderse su ejecución podría producir perjuicios irreparables a la respectiva parte.

Ahora bien, hay resoluciones que, por su naturaleza, contrario a lo expresado, los perjuicios pueden devenir por no ejecutarlas, de ahí que se prevén diversas excepciones al expresado efecto suspensivo, como lo es en el caso de las resoluciones por medio de las cuales se imponen o decretan medidas cautelares, en las que no obstante, su impugnación, deberán llevarse a efecto. Arts. 453 CPCM, 341 y 398 C. Pr. Pn.

c) Efecto extensivo o comunicante.

Este efecto se encuentra específicamente prescrito en el art. 456 C.Pr. Pn., constituyendo una excepción al principio general de la personalidad de la impugnación, en el sentido que el efecto es para quien lo interpone; ello porque, como reza la expresada disposición legal, en caso que existan coimputados o acumulación de causas el recurso interpuesto respecto de uno de ellos favorecerá también a los demás, a menos que se base en motivos exclusivamente personales.

Lo anterior implica que por razones de orden público y a fin de evitar diversidad de criterios ante circunstancias similares, un imputado inactivo puede salir favorecido por la impugnación incoada por un coimputado, extendiéndose así sus efectos al que no hizo uso de su derecho a recurrir; debiendo precisarse que lo será en todo aquello que le favorezca, mas no que le perjudique, por aplicación del principio de la prohibición de la *reformatio in pejus*. Un límite a este efecto es que los motivos que fundamenta la impugnación sean exclusivamente personales del impugnante.

Por la determinación expresa que de dicho efecto hace el Código Procesal Penal, pareciera que el mismo es exclusivo para este ámbito de conocimiento, mas estimo que también tiene aplicabilidad en otras materias, pues carecería de sentido que en caso de pluralidad de sujetos procesales vinculados por una relación jurídica material indivisible, la impugnación interpuesta por uno de éstos no beneficie a los demás si la impugnación no se fundamenta en motivos exclusivamente personales del impugnante; que tal situación puede desprenderse de lo prescrito en el art. 76 inciso final del Código Procesal Civil y Mercantil y, partiendo de lo que prescribe

el art. 20 del mismo cuerpo legal su aplicación se extiende a todo el ordenamiento jurídico.

PRINCIPALES MEDIOS DE IMPUGNACIÓN PREVISTOS POR NUESTRO ORDENAMIENTO JURÍDICO

Los principales medios de impugnación que unánimemente se prevén en los diferentes cuerpos normativos instituidos como recursos por nuestro ordenamiento jurídico son la Revocatoria, Apelación, Casación y Revisión de Sentencias firmes o de la cosa juzgada; que por no ser el objeto de los presentes apuntes el análisis pormenorizado de cada uno de los medios de impugnación en particular, únicamente haré una general, limitada y básica referencia acerca de cada uno de ellos.

Recurso de revocatoria

Este medio de impugnación también es conocido como mutación, reposición o reforma, y es sobre cuya base se busca la reconsideración de lo decidido, por el mismo tribunal que pronunció la resolución que por esta vía se impugna, con el objeto de que se deje sin efecto, adoptándose un criterio u opinión nueva; de ahí su carácter de un medio de impugnación con efecto no devolutivo.

Al respecto de este medio de impugnación (Couture, 1977) afirma: que la revocatoria es un incidente impugnativo nominado e instituido como recurso por los códigos procesales, por el cual se pretende que el mismo tribunal que dictó la resolución impugnada la elimine, modifique o revoque.

La revocatoria puede interponerse de forma oral en audiencia y de forma escrita. En cualquier grado de conocimiento del proceso y, por regla general, procede contra dos tipos de resoluciones, los decretos y los autos simples, excepcionalmente contra ciertos autos definitivos. Arts. 461 C.Pr. Pn., 150 L.Pr.Fam. y 503, 139, 278, 513 y 530 CPCM, entre otros; no cabe la revocatoria contra las sentencias, excepto en lo accesorio tal como lo prevé el art. 150 de la L.Pr. Fam.

Recurso de apelación

La apelación es un recurso devolutivo y ordinario por excelencia, que la ley franquea o concede a toda parte o litigante u otro interesado, cuando crea haber sufrido un agravio por la sentencia o decisión del Juez inferior para reclamar de la misma ante el Tribunal superior en grado, generalmente colegiado, para que este la revoque, anule, reforme o modifique.

El efecto devolutivo concedido a la apelación, produce lo que se conoce como segunda instancia; ello porque como consecuencia de la apelación se genera un segundo examen y decisión sobre la cuestión de fondo planteado en el proceso, por un órgano jurisdiccional distinto y superior de aquel que pronuncio la resolución apelada (Cámaras de Segunda Instancia o Sala de lo Civil de la Corte Suprema de Justicia cuando el demandado sea el Estado), prevaleciendo este segundo pronunciamiento sobre el primero. Esto implica que como consecuencia de estos dos grados de conocimiento o instancias, se producen dos pronunciamientos sobre el objeto del proceso, en donde, como se dijo, el segundo prevalece sobre el primero.

La apelación cabe contra sentencias, autos definitivos y contra las resoluciones que las leyes señalen expresamente, indistintamente de su clase o tipo y, por regla general, su forma de interposición es por escrito debidamente fundamentado. Arts. 176, 341, 464, 468 C.Pr. Pn., 508, CPCM. y 153 L.Pr. Fam., entre otros. Es preciso señalar que en el ámbito de familia se prevé la interposición de la apelación de forma oral en el acto de una audiencia contra una sentencia interlocutoria o auto, tal como se dispone en el art. 156 L. Pr. Fam.

De lo apuntado, se destacan en relación al expresado medio de impugnación ciertas carac-

terísticas que lo identifican y distinguen, siendo estas: que es un recurso que se interpone ante el mismo tribunal que pronuncio la resolución que se impugna, es decidido por un tribunal distinto y superior en grado al que pronuncio la resolución recurrida (Cámaras de Segunda Instancia y la Sala de lo Civil cuando el demandado sea el Estado), es el principal recurso ordinario por excelencia, es de carácter devolutivo y, por ello, un recurso que genera instancia.

Recurso de casación.

En un contexto histórico, es preciso señalar que en El Salvador fue la Constitución de 1883 la que estableció por primera vez el recurso de casación; que al mismo tiempo se creó el órgano jurisdiccional encargado de dicho medio de impugnación que se denominó CORTE DE CASACIÓN, siendo una ley secundaria la que regulo su funcionamiento, instaurándose su conocimiento como una tercera instancia. En este primer contexto histórico, dicho recurso tuvo una vida efímera o limitada, pues fue suprimido por la Constitución de 1886. Fue con la Constitución de 1950 que por segunda vez se estableció el expresado recurso y, con ello, se le dio una nueva estructura a la Corte Suprema de Justicia, en el sentido que se suprime la hasta entonces conocida tercera instancia en el procedimiento judicial, decretándose en 1953 la Ley de Casación que conforme al principio de ultractividad aún tiene aplicación para ciertos casos; Ley que sufrió reformas en 1989, siendo este el dato más reciente en torno a la regulación y tratamiento del recurso de casación, que como se dijo, vino a sustituir a la antes llamada tercera instancia.

Con la entrada en vigencia del Código Procesal Civil y Mercantil quedo derogada la expresada Ley de Casación de 1953, tal como como se prevé en el art. 705 CPCM., quedando ahora regulado por dicha normativa, a excepción de la casación en el ámbito penal cuyo contenido, tratamiento y regulación siempre ha estado plasmado en el Código Procesal Penal, ahora a partir del art. 478 C. Pr. Pn.

La casación es el proceso de impugnación de una resolución judicial, ante el grado supremo de la jerarquía judicial, por razones inmanentes al proceso en que dicha resolución fue dictada; es decir, que las partes no pueden acudir a ella a base de su simple interés, sino que tienen que contar con una causa legalmente determinada, o sea, con un motivo, el cual recae sobre circunstancias determinadas y taxativas coincidentes precisamente con las circunstancias que funcionan con dichos motivos de casación.

De lo definido deviene el carácter extraordinario por antonomasia de dicho medio impugnativo, en el sentido que la casación procede contra determinadas resoluciones judiciales y en atención a motivos tasados, limitando así sus poderes de conocimiento a temas determinados y taxativos coincidentes, como se consignó, con las circunstancias que funcionan como motivos de casación; de ahí que, este recurso no constituya instancia, explicándose así su naturaleza jurídica.

Es de esta forma que, además de ser un control de la legalidad de las resoluciones judiciales, una de las principales y esenciales finalidades de la casación es velar por una correcta y uniforme aplicación del ordenamiento jurídico por los tribunales de instancia, es decir uniformar la jurisprudencia.

Consecuente con lo expresado, la casación procede contra resoluciones pronunciadas en segunda instancia, es decir, en apelación y que le pongan fin a un proceso, esto es, contra sentencias y autos definitivos, situación que tiene sus propias particularidades según la materia de que se trate. Arts. 478 y 479 C. Pr. P., 519, 520, 521, 522 y 523 CPCM.

Cabe señalar en el presente trabajo, que la casación tiene por objeto exclusivo examinar o determinar si en la sentencia objeto de dicho medio de impugnación ha existido infracción

a la ley (aplicación indebida de la norma, aplicación o interpretación errónea de la norma e inaplicación o violación de la norma) o a la doctrina legal o un quebrantamiento en las formas esenciales del proceso, es decir, infracciones de fondo o de forma.

Recurso de revisión de la cosa juzgada o de sentencias firmes

La revisión de la cosa juzgada, más que un recurso es un medio de impugnación o bien un proceso que procede contra sentencias firmes, es decir, que tiene por objeto impugnar la cosa juzgada; de ahí que se trate de una excepcional modalidad de impugnación, pues tal facultad impugnativa, en el afán de anteponer el valor justicia, constituye un desconocimiento a la inimpugnabilidad o irrevocabilidad de las resoluciones judiciales que materialmente han adquirido la calidad de cosa juzgada y, con ello, a la seguridad jurídica misma.

Dado el carácter excepcional expresado, la revisión de la cosa juzgada únicamente procede si se configuran algunas de las circunstancias o motivos taxativamente previstos por la ley, es decir, que el ordenamiento jurídico respectivo prevé las circunstancias que van a funcionar como causas o motivos para promover la revisión de la cosa juzgada. Arts. 541 y 542 CPCM. y 489 C.Pr.PN.

Cabe precisar que según la materia que se trate, la revisión de la cosa juzgada presenta ciertas diferencias en cuanto a condiciones o formas de interposición, legitimación, competencia funcional y tratamiento procesal; en este orden, en el ámbito penal legítimamente procederá la interposición de dicho medio impugnativo en todo tiempo, únicamente a favor del imputado, ante el tribunal que pronunció la sentencia que causó ejecutoria y bajo el procedimiento que se fija por el Código Procesal Penal en los arts. 489 al 497; contrario a lo expresado, en el campo civil, la revisión de sentencias firmes podrá interponerla cualquiera de las partes (actor, demandado e inclusive un tercero) específicamente ante la Sala de lo Civil de la Corte Suprema de Justicia, dentro de los plazos tanto generales como especiales al efecto fijados y conforme a su propio procedimiento determinado por la ley de la materia, según los arts. 540 al 550 CPCM.

JURISPRUDENCIA CONSTITUCIONAL ACERCA DE PRINCIPIOS Y GARANTÍAS FUNDAMENTALES VINCULADOS CON LOS MEDIOS DE IMPUGNACIÓN

Actos procesales de comunicación

Acceso a los medios impugnativos

Según la Sala de lo Constitucional (2010, p. 9):

Los llamados actos de comunicación, (…) son las herramientas de que se vale el juzgador para hacer saber a las partes las actuaciones que resulten dentro de un proceso o procedimiento. Por medio de ellos, se pretende que los distintos sujetos puedan no sólo conocer las resultas de la sustanciación, sino que, eventualmente, puedan recurrir de ellas cuando lo estimen pertinente.

Es importante señalar que la realización de los actos procesales de comunicación está regida en su ejercicio concreto, al cumplimiento de los presupuestos y requisitos contemplados en las respectivas leyes.

Sobre el acceso a los medios impugnativos o derecho a recurrir se ha expresado que el mismo es un derecho de naturaleza constitucional procesal, que si bien esencialmente es un derecho de configuración legal, también se ve constitucionalmente protegido en cuanto constituye una facultad de los gobernados de poder acceder a los medios impugnativos que les franquea la ley de una forma efectiva, posibilitando con ello alcanzar una real protección jurisdiccional.

En el presente caso, el demandante afirmó que en el juicio ejecutivo civil 1-EC-2007, que se instauró en su contra en el Juzgado de lo Laboral de Santa Tecla, no se le notificó personalmente la sentencia definitiva mediante la que se le

condenó al pago de la deuda reclamada, ya que dicha providencia se notificó por medio del tablero judicial, no obstante tener conocimiento el tribunal de la dirección de su lugar de residencia pues, tal como consta en el proceso, fue allí donde le emplazaron; que por tal razón se vio imposibilitado de recurrir contra la mencionada providencia condenatoria, por lo que considera se han vulnerado sus derechos.

Posibilidad de notificar providencias judiciales por medio de edicto o tablero judicial

Por su parte, la autoridad demandada negó las violaciones constitucionales atribuidas y argumentó que la sentencia definitiva fue notificada al apoderado general judicial del demandante por tablero judicial, debido a que éste no cumplió con la prevención que le hizo el tribunal a su cargo, en la que se le ordenó señalar lugar para oír notificaciones en la ciudad de Santa Tecla; en vista de lo cual, se aplicó el art. 220 en relación con el art. 1276 del Código de Procedimientos Civiles vigente en ese momento, aplicado a este caso.

Al respecto, esta Sala (Sala de lo Constitucional, 2010, pág. 10) considera pertinente hacer las siguientes consideraciones:

1. De acuerdo al artículo 1276 del Código de Procedimientos Civiles, las partes en los escritos de demanda y contestación tenían la obligación de indicar un lugar para oír notificaciones en el lugar del juicio, de tal manera que, si la parte no cumplía con dicha disposición, el juzgador podría notificar la providencia judicial por medio de edicto fijado en el tablero del tribunal, según lo regulaba el artículo 220 inciso tercero parte final.

   En efecto, esta última disposición establecía que: "Si la parte no tiene casa o no la hubiere designado conforme se previene en el artículo 1276, las notificaciones y citaciones se harán por edicto en la forma prescrita en los incisos primero y segundo de este artículo". En ese sentido, si bien, el mencionado precepto posibilitaba que la notificación fuera efectuada por edicto o tablero judicial, condicionaba ese supuesto al caso en que no se hubiese señalado lugar para recibir notificaciones dentro de la circunscripción territorial del tribunal.

2. Aplicando lo antes expuesto al caso en estudio, de la certificación del expediente remitido por el Juez de lo Laboral de Santa Tecla, se advierte que la resolución de las nueve horas con cincuenta minutos del día 15-III-2007, mediante la cual se emplazó al [actor] fue materializada por el Juzgado Segundo de Paz de Colón, departamento de La Libertad, de manera que el emplazamiento del referido señor *…+ fue realizado en su casa de habitación por medio de la señora *…+, quien manifestó ser su esposa.

   Consta además, que él [actor] contestó la demanda incoada en su contra por medio del escrito presentado por su apoderado general judicial abogado *…+, señalando para oír notificaciones una dirección en la jurisdicción de Lourdes Colón, La Libertad. En vista de dicha situación se le previno para que señalara lugar dentro de la circunscripción territorial de Santa Tecla, lo cual no hizo, por lo que se procedió a notificar la sentencia pronunciada a las diez horas y treinta minutos del día 12-VII-2007, a través del tablero judicial.

Notificación de sentencia definitiva en tablero judicial no afecta el derecho de defensa

Las líneas y criterios jurisprudenciales en materia de Amparo y Sentencias definitivas <530-2008> (Sala de lo Constitucional, 2010, p. 10-11) señalan que:

> En ese orden de ideas, y habiéndose establecido ya que el artículo 1276 Pr.C. aplicable en ese momento, obligaba a las partes procesales a señalar una dirección para recibir notificaciones dentro del lugar del juicio y que el referido profesional no cumplió a

cabalidad con lo ordenado en dicho precepto legal, no le era exigible al juez una actuación distinta a la llevada a cabo, pues el artículo 220 de la norma citada establecía el modo de proceder en casos como el que se estudia, habilitándolo para realizar las notificaciones por medio del tablero judicial.

Examinada la esquela de notificación de las once horas y diez minutos del día 24-VII 2007, se establece que las condiciones prescritas por el legislador para realizar la notificación conforme el artículo 220 Pr.C. derogado, fueron cumplidas, lo que permite colegir que al notificar el juez por medio del tablero judicial la sentencia definitiva pronunciada en el juicio ejecutivo civil con referencia 1-EC-2007, lo hizo en virtud de la actuación de la parte actora que no señaló lugar para oír notificaciones tal y como lo prescribía el artículo 1276 Pr.C., y no por una irregularidad judicial, por lo que se concluye que el Juez de lo Laboral de Santa Tecla siguió el procedimiento establecido en la normativa aplicable en ese momento para realizar la comunicación procesal relacionada, en consecuencia no ha imposibilitado la oportunidad de defensa al demandante, por lo que habrá que declarar no ha lugar el amparo solicitado.

Derecho a los medios impugnativos: permite un control posterior de las resoluciones judiciales o administrativas

A este respecto la (Sala de lo Constitucional, 2010, p. 142) detalla:

1. En esencia, el acceso a los medios impugnativos o "derecho a recurrir" es un derecho de naturaleza constitucional procesal, que si bien esencialmente dimana de la ley, también se ve constitucionalmente protegido en cuanto constituye una facultad de los gobernados, que ofrece la posibilidad de alcanzar efectivamente una real protección jurisdiccional.
2. Cuando el legislador establece un medio impugnativo, es porque mediante un control posterior de las resoluciones a través de diferentes grados de conocimiento, se logra subsanar las posibles irregularidades incurridas y por tanto restablecer los derechos violados que resultaren de un primer grado de conocimiento. De ahí que al conocerse del asunto controvertido en una instancia o grado superior, ello implica la posibilidad de un nuevo examen de la situación planteada y consecuentemente, el de obtener una correcta aplicación de la ley.

Ausencia de prueba sobre la interposición adecuada del recurso de apelación

Las líneas y criterios jurisprudenciales en materia de Amparo y Sentencias definitivas <357-2008> (Sala de lo Constitucional, 2010, p. 143) señalan que:

> El artículo 69 de la Ordenanza aplicada en este caso, dispone: "En cuanto a procedimiento y recursos se aplicará lo establecido en el Título X del Código Municipal vigente."
>
> En dicho Código en el Art. 137 del título indicado, el legislador establece el recurso de apelación para ante el Concejo Municipal, de las resoluciones del alcalde o del funcionario delegado y a su vez el procedimiento que debe seguirse.
>
> Al respecto, en el presente caso el Concejo Municipal demandado, no ha negado ni aceptado el acto que se le imputa, pues no presentó ningún informe ni contestó los traslados, pero tampoco el demandante ha probado haber interpuesto algún recurso con relación a la multa impuesta por el Síndico Municipal.
>
> Esta Sala concluye que el demandante no ha interpuesto ningún recurso ante el Concejo Municipal respecto a la actuación del Síndico Municipal, por lo que habrá que so-

breseerse en el proceso en relación a este punto, por falta de agravio constitucional.

Derecho a recurrir para obtener la reconsideración de una resolución

De acuerdo con (Sala de lo Constitucional, 2010, p. 162-163):

> Se ha señalado –Sentencia de Amparo Ref. 1112-2008 del 04-VI-2010, Considerando II 2 C– que el derecho a los medios impugnativos o derecho a recurrir es un derecho de naturaleza constitucional procesal, que si bien esencialmente dimana de la ley, también se ve constitucionalmente protegido en cuanto constituye una facultad para las partes a fin de que tengan la posibilidad de agotar todos los medios para obtener una reconsideración de la resolución impugnada por parte del tribunal o ente administrativo superior en grado de conocimiento. Y es que, si bien la interpretación y aplicación de las disposiciones que regulan los presupuestos y requisitos establecidos por el legislador para la válida promoción de los medios impugnativos corresponde a la jurisdicción ordinaria, ello no obsta para que dicha concreción se realice de conformidad a la ley y a la Constitución, esto es, en la forma más favorable a la efectividad de los derechos fundamentales.
>
> Por ello, el derecho a recurrir, no obstante ser un derecho de configuración legal, tiene sustantividad propia, pues el mismo se conjuga –como todo el ordenamiento – con el derecho a un proceso constitucionalmente configurado y con el de audiencia, en tanto que al consagrarse en la ley un determinado medio impugnativo, la negativa de acceder al mismo sin justificativo constitucional, cuando legalmente procede, deviene en una vulneración de ellos, ya que, en caso de estar legalmente consagrada la posibilidad de otro grado de conocimiento, negar la misma sin basamento constitucional supondría no observar los derechos de rango constitucional.
>
> Una vez que el legislador ha establecido un medio para la impugnación de las resoluciones recaídas en un concreto proceso o procedimiento, o para una específica clase de resoluciones, el derecho de acceso al medio impugnativo adquiere connotación constitucional, y una denegativa del mismo, basada en causa inconstitucional o por la imposición de requisitos e interpretaciones impeditivas u obstaculizadoras que resulten innecesarias, excesivas o carezcan de razonabilidad o proporcionalidad respecto de los fines que lícitamente puede perseguir el legislador, por la imposición de condiciones o consecuencias meramente limitativas o disuasorias del ejercicio de los medios impugnativos legalmente establecidos, deviene en violatoria de la normativa constitucional.

Inexistencia de vulneración al derecho de recurrir cuando se ha notificado en debida forma la resolución de destitución

Así mismo en la (Sala de lo Constitucional, 2010, p. 166) también se advierte que:

> Según lo manifiesta la parte actora, la resolución de destitución le fue notificada, por lo que pudo hacer uso efectivo de los medios impugnativos pertinentes; aunado a ello, la resolución en comento también le fue notificada al defensor del peticionario durante la realización de la audiencia, quien pudo interponer el recurso correspondiente, en caso de considerarlo procedente. Ello implica que al haberse notificado la resolución de destitución, se garantizó la posibilidad de interposición de los recursos que correspondieran, no existiendo vulneración al derecho de recurrir por la falta de interposición de los mismos.

Derecho a los medios impugnativos

Derecho de audiencia y actos procesales de comunicación

Respecto a ello, la (Sala de lo Constitucional, 2010, p. 176-177) advierten que:

> El derecho de audiencia, de acuerdo a la jurisprudencia de esta Sala – Sentencias de Amparo Ref. 782-2008 Considerando III 1, Ref. 265-2007 Considerando III 1, Ref. 98-2006 Considerando II 1, Ref. 226-2004 Considerando IV, entre otras-, es un concepto amplio en cuya virtud se exige que, antes de proceder a limitar la esfera jurídica de una persona o a privársele por completo de un derecho, debe ser oída y vencida con arreglo a las leyes.
>
> El derecho de audiencia posibilita la intervención del gobernado, a fin que conozca los hechos que se le imputan y tenga la oportunidad, si lo estima pertinente, de comparecer para intentar desvirtuarlos.
>
> En tal sentido, los procesos jurisdiccionales y los procedimientos administrativos, deben estar diseñados para respetar el derecho de audiencia, no quedando ninguna duda de su contenido estrictamente procesal, vinculado con el resto de derechos que son tutelados por el proceso de amparo.
>
> Por lo anterior, puede señalarse que existe violación del derecho de audiencia, cuando el afectado no ha tenido la oportunidad real de pronunciarse en un caso concreto, privándosele de un derecho sin el correspondiente juicio o procedimiento, o cuando en el mismo no se cumplen las formalidades procesales esenciales, vale decir, la oportunidad de defensa y oposición y la oportunidad probatoria.
>
> El derecho de audiencia se encuentra íntimamente relacionado con los actos procesales de comunicación, dichos actos, podemos decir que son las herramientas que utiliza el juzgador para hacer saber a las partes lo que está ocurriendo al interior de un proceso o procedimiento.
>
> Por la notificación que es uno de los actos referidos, se pretende que los distintos sujetos puedan no sólo conocer las resultas de la sustanciación del proceso, sino que, eventualmente puedan recurrir de una actuación cuando lo estimen pertinente.
>
> También es de hacer notar, que la realización de los actos procesales de comunicación está regida en su ejercicio concreto, al cumplimiento de los presupuestos y requisitos contemplados en las respectivas leyes.

Derecho a recurrir

Con relación al derecho a recurrir, esta Sala (Sala de lo Constitucional, 2010, p. 177) ha sostenido reiteradamente que dentro del "debido proceso", existen derechos que expresamente lo viabilizan, potencian, componen o concretan. Así también, hay otros derechos que aunque no se encuentren de forma expresa en el texto constitucional, esta Sala ha reconocido su existencia como integrantes de aquel proceso constitucionalmente configurado – debido proceso, por ejemplo, el derecho de acceso a los medios impugnativos, que suele denominarse "derecho a recurrir".

El anterior derecho, es por su propia naturaleza de configuración legal, lo que implica que al consagrarse en la ley un determinado medio impugnativo para atacar alguna resolución de trámite o definitiva, debe permitirse a la parte agraviada el acceso efectivo al mismo, con lo cual se estaría también accediendo, eventualmente, a un segundo o tercer examen de la cuestión – otro grado de conocimiento-, potenciándose el derecho de acceso a la jurisdicción.

En resumen, el acceso a los medios impugnativos o "derecho a recurrir", es un derecho de naturaleza constitucional procesal, que si

bien esencialmente dimana de la ley, también se ve constitucionalmente protegido en cuanto constituye una facultad de los gobernados, para alcanzar efectivamente una real protección jurisdiccional.

Se cumple el presupuesto cuando el demandado ha sido legalmente notificado de la sentencia impugnable

A este respecto, las lineas y criterios jurisprudenciales (Sala de lo Constitucional, 2010, p. 178) dictan:

> De acuerdo al procedimiento reseñado, en el presente caso, la sociedad demandante, no obstante haber sido emplazada para que, de conformidad a lo que establecía el inciso primero del Art.595 Pr.C, contestara la demanda y en aplicación del Art.57 de la Ley de Procedimientos Mercantiles, alegara todas las excepciones de cualquier clase que tuviera, dejó pasar el plazo correspondiente sin hacer lo que la ley le permitía.
>
> En vista de lo anterior, la Jueza Cuarto de lo Mercantil no declaró la rebeldía, lo cual no lo establecía el legislador en el juicio ejecutivo en esa materia y omitió el plazo del encargado o de pruebas en aplicación del inciso segundo del artículo 57 citado en el párrafo anterior, por lo que, al no haber manifestado oposición la demandante en el plazo legal correspondiente, se presume el allanamiento al juicio.
>
> Por tanto, cuando la parte demandada al ser emplazada no comparece, o, en términos amplios, no contesta la demanda, lo que está haciendo voluntariamente, es no ejercer su derecho a ser escuchada y a defenderse.
>
> El ordenamiento jurídico, regula la oportunidad en que las partes procesales deben ejercer sus derechos y cuando estos derechos son además cargas procesales, la falta de ejercicio oportuno, de ninguna manera equivale a indefensión o violación al derecho de defensa.
>
> En este caso, el curso del juicio ejecutivo siguió el orden legalmente establecido, por lo tanto no contiene actuaciones que puedan impugnarse como inconstitucionales, pues la demandante tuvo la oportunidad para ejercer sus derechos, ya que al ser emplazada, pudo contestar la demanda y alegar excepciones, y al no hacerlo, voluntariamente dejó de ejercer su derecho de defensa; asimismo al habérsele notificado la sentencia de remate y no interponer recurso de apelación, se deduce que no pretendió hacer uso del derecho a recurrir.
>
> En síntesis, ha quedado establecido en autos, que el emplazamiento y las notificaciones se hicieron en la dirección señalada en la demanda; que tales diligencias se efectuaron por vía permitida por el legislador y que la llevó a cabo la persona idónea para efectuar tal actividad.

Recurso de casación

Efectos suspensivo y extensivo

Las líneas y criterios jurisprudenciales (Sala de lo Constitucional, 2013, p. 656-657) establecen que:

> Es de señalar que en la certificación de los pasajes remitidos a esta sala, no consta que la favorecida haya recurrido en casación de su sentencia condenatoria, sin embargo se tiene que otros procesados sí impugnaron tal decisión; no obstante ello, el expediente del proceso penal respectivo fue remitido íntegra – mente a la Sala de lo Penal, con todos los imputados para que conociera de los recursos interpuestos; ello, según se extrae del oficio de remisión número 3268 del Juzgado Especializado de Sentencia de San Miguel que data del 25/6/2012. Ante la situación descrita y en virtud de que la peticionaria manifiesta que la favorecida al mo-

mento de requerir la tutela ante esta sede constitucional se encontraba en detención provisional a pesar de advertirse, a partir de lo agregado al proceso, que no recurrió de la sentencia condenatoria, es preciso iniciar por hacer referencia a algunos aspectos del diseño de los recursos regulado en el Código Procesal Penal derogado, pertinentes y de ineludible consideración para dirimir el asunto en análisis. Dentro del capítulo relativo a las disposiciones generales de los recursos, el legislador ha determinado, en el artículo 411, que estos generan un efecto suspensivo, es decir, por regla general, una resolución que admite impugnación no debe ser ejecutada durante el plazo para recurrir ni mientras se tramita el recurso. Excepcionalmente esta deberá serlo, cuando exista una disposición estableciéndolo así. Por otro parte, el legislador también ha regulado que los recursos tienen efecto extensivo, artículo 410, cuando estos sean interpuestos por coimputados, el cual permite que los imputados que por cualquier causa no ejerciten, por sí o a través de su defensa técnica, el derecho a recurrir, se beneficien aún así de los efectos positivos que puede generar la interposición de un medio de impugnación dirigido a dejar sin efecto resoluciones que les causen agravio; así, las consecuencias favorables que, de la interposición de un recurso se derivan para el recurrente, por disposición legal se extienden a quien no tenga dicha calidad. Esto a su vez impide el surgimiento, en un mismo proceso, de pronunciamientos diferentes respecto a situaciones que deben ser resueltas de forma idéntica, por estar basadas esencialmente en las mismas circunstancias. En razón de esto último, el efecto extensivo no puede aplicarse cuando la impugnación se fundamente exclusivamente en motivos personales del imputado a cuyo favor se recurre, pues en ese caso las argumentaciones se construyen en torno a tales especificaciones, las cuales no podrían trasladarse de igual manera a otro incoado que se encontraría en una situación diferente. Los efectos suspensivo y extensivo imposibilitan, de acuerdo con la ley, que una resolución judicial impugnable adquiera firmeza automáticamente cuando el imputado no ha recurrido: el primero, pues aquella no puede ejecutarse durante el trámite del recurso, aunque este no haya sido interpuesto por el imputado, por ejemplo en casos en los cuales quien impugna la decisión es la parte acusadora; el segundo, en virtud de que no obstante un específico acusado haya decidido no cuestionar la resolución emitida en su contra, por disposición legal, puede aprovecharse de los resultados favorables de la impugnación planteada por un coimputado. Las anteriores consideraciones están referidas a cualquier recurso y, por ende, también al de casación, de esta forma al interponerse por un imputado, puede aprovechar a los otros que no lo hayan incoado. Si este tiene por objeto cuestionar la sentencia condenatoria, por lo tanto, la misma no adquirirá firmeza hasta una vez resuelta la casación, independientemente de que inicialmente haya sido promovido en relación con alguna de las personas condenadas, siempre y cuando –se insiste– no verse sobre motivos personales del procesado que lo ha impulsado; esto en aplicación del efecto suspensivo y extensivo que suponen que la resolución recurrida no puede ejecutarse tanto en relación con los imputados recurrentes como respecto de aquellos a quienes puede favorecer el recurso.

Efectos extensivo y suspensivo implican que el coimputado que no re – currió mantenga su condición de procesado durante la tramitación del medio de impugnación

Sin embargo, en la práctica, si el plazo de decisión de la casación se supera sin justificación, podría generar una distorsión de lo pretendido con el reconocimiento del efecto extensivo, pues la dilación en la emisión de la sentencia

afectaría no solo derechos de quienes lo han promovido, sino además de aquellos – "Ahora bien, en cuanto al recurso de casación, es de citar que de conformidad con la normativa aplicable al caso en estudio, tiene como plazo Máximo para su resolución 15 días, el cual, excepcionalmente, si se ordena audiencia especial para la fundamentación y discusión del mismo, podrá extenderse hasta 35 días –artículos 427 y 428 del Código Procesal Penal derogado–involucrados por la decisión debido a dicho efecto. De esa manera, una figura prevista para favorecer a los imputados y evitar la disparidad en la decisión de casos que deben resolverse de forma idéntica, se desnaturalizaría ante la tardanza del tribunal y en lugar de implicar un beneficio para quien no ha recurrido se transformaría en una medida que, además de generar incertidumbre jurídica por prolongar el resultado del ejercicio de la acción penal, puede impedir al indiciado, por ejemplo, acceder a beneficios penitenciarios aplicables, de acuerdo a la pena que se le hubiere impuesto, si ya se estuviera ejecutando esta, así como de cualquier otra oportunidad legal dispuesta a favor de quien cumple pena (ver en similar sentido resolución HC 116-2009/126-2009 Ac, de fecha 25/11/2011). De ahí la relevancia de que los recursos de casación sean resueltos dentro de los plazos establecidos en la ley, con el objeto de contestar las solicitudes planteadas ante el tribunal encargado de decidir el mismo y para que, entre otros aspectos, pueda determinar si el recurso puede serle vinculante, de conformidad con los parámetros del artículo 410 de la normativa procesal penal, a quien no ha impugnado la sentencia condenatoria. En conclusión, en el supuesto de que un coimputado haya recurrido en casación, mientras no exista un pronunciamiento expreso del tribunal competente considerando que en el caso no es aplicable el efecto extensivo regulado por la ley, ya sea porque la persona ha renunciado a dicho beneficio legal o porque el recurso se encuentra basado en motivos personales de otro imputado que no pueden trasladársele al no recurrente, este último continuaría en calidad de procesado. Con fundamento en todo lo anterior, para efectos de esta decisión, debe considerarse que la favorecida con el hábeas corpus se encontraba en detención provisional pues, no obstante la señora […] no recurrió de la sentencia condenatoria dictada en su contra, su calidad de procesada no se modificó a la de persona condenada, sino que mantuvo dicho estatus durante el trámite del aludido medio impugnativo, en virtud de los efectos suspensivo y extensivo del recurso de casación. Desde esa perspectiva, y al haberse verificado las razones por las que de acuerdo a la normativa procesal penal aplicable, la sentencia de la favorecida no adquirió firmeza, y siendo que en este proceso el pretensor objeta, como se dijo, de inconstitucional el cumplimiento de la medida cautelar de la detención provisional en virtud de haberse excedido el límite máximo dispuesto en la ley para su mantenimiento; esta sala entrará a analizar lo propuesto". Sala de lo Constitucional, *Hábeas Corpus*, número de referencia: 34-2013, fecha de la resolución: 10/04/2013 Relaciones: Sala de lo Constitucional, *Hábeas Corpus*, número de referencia: 219-2012, fecha de la resolución: 05/04/2013 Sala de lo Constitucional, *Hábeas Corpus,* número de referencia: 227-2012, fecha de la resolución: 19/04/2013 Sala de lo Constitucional, *Hábeas Corpus*, número de referencia: 255-2012, fecha de resolución: 10/04/2013. (Líneas y Criterios Jurisprudenciales de la Sala de lo Constitucional 2013 Tomo II, Pag.657 y 658)

Conclusiones.

El primordial objetivo de un medio de impugnación es que se entre al conocimiento del fondo del mismo, esto es de los agravios, que constituyen su asunto principal; que previo a ello, todo medio de impugnación está sujeto a un examen preliminar, cuyo objetivo es determinar si en el acto de su interposición, formulación o estructuración se han cumplido con todas las condiciones que llevan a su admisibilidad como tal, lo que significa que de no cumplirse con tales condiciones será rechazado, inhibiéndose el tri-

bunal de conocer sobre su fondo o asunto principal. En este contexto, son innumerables los recursos que tras su examen preliminar devienen en inadmisibles por no haber hecho un uso adecuado de los mismos, consecuentemente, ya no son revisados en su fondo; de ahí que es importante saber cómo debe formularse o estructurarse un medio de impugnación, para lo cual se torna necesario conocer la base dogmática o teórica que los fundamentan; es de esta forma que los presentes apuntes tienen como base primordial aportar los conocimientos esenciales en esa parte dogmática que, como se dijo, fundamentan los medios de impugnación y los principales recursos que se regulan por los diferentes ordenamientos jurídicos, como son la revocatoria, apelación, casación y revisión de sentencias firmes.

Referencias

Asamblea Legislativa de la República de El Salvador. (1994). Ley Procesal de Familia. San Salvador, El Salvador: s/ed. Recuperado el 02 de julio de 2018, de https://www.oas.org/dil/esp/Ley_Procesal_de_Familia_El_Salvador.pdf

Couture, E. (1977). Fundamentos Procesal Civil (Segunda reimpresión inalterada ed.). (D. Palma, Ed.) Buenos Aires.

Luna, R. A. (1998). De la iniciación del proceso. San Salvador, El Salvador: Universidad de El Salvador. Obtenido de http://www.csj.gob.sv/BVirtual.nsf/f8d2a0b5ee4651a-386256d44006c123c/678f5743bb1c81e-906256b3e00747b78?OpenDocument

Sala de lo Constitucional. (2010). Líneas y criterios jurisprudenciales. Recuperado el 11 de agosto de 2018, de http://www.jurisprudencia.gob.sv/VisorMLX/weblj/Constitucional/Incons2010.pdf

Sala de lo Constitucional. (2013). Líneas y criterios jurisprudenciales. (Vol. II). El Salvador: Asamblea Legislativa.

Aplicación para firma digital y generación de certificados utilizando la API Bouncy Castle considerando la Ley de Firma Digital de El Salvador*

Álvaro Hernán Zavala Ruballo
alvarohz@usonsonate.edu.sv
Facultad de Ingeniería y Ciencias Naturales – Universidad de Sonsonate

*Este artículo ya ha sido publicado anteriormente en: Á. Hernán Zavala Ruballo, "Application for digital signature and generation of certificates using the Bouncy Castle API considering digital signature law in El Salvador," 2018 IEEE 38th Central America and Panama Convention (CONCAPAN XXXVIII), San Salvador, 2018, pp. 1-6.
doi: 10.1109/CONCAPAN.2018.8596612

Resumen

Considerando que en El Salvador la Ley de Firma Digital fue aprobada hace poco más de dos años, con el objetivo de otorgarle el mismo poder legal que la firma autógrafa, la aplicación propuesta construida con la API Bouncy Castle para llevar acabo la firma y verificación de documentos, así como la generación de certificados, y con el objetivo de ofrecer servicios de autenticación, integridad de los datos y no repudio, se divide en dos partes, la primera, un software de escritorio construido en Java Swing para generación del par de llaves privada-publica con la cual se firman documentos utilizando el algoritmo de firma digital de curvas elípticas (ECDSA), debido a la necesidad de llaves pequeñas, y la función resumen SHA3 para huellas digitales; la segunda, una aplicación web en JSP para generación de certificados digitales que simula las tareas de una Autoridad Certificadora (CA) como proveedor de certificados, donde los usuarios pueden solicitarlos y estos son enviados por correo, el certificado raíz auto firmado como parte de una infraestructura de llave pública (PKI) es utilizado para firmar los certificados generados a otros usuarios. Una CA presta sus servicios de certificación que garantiza ante terceros, que confían en sus certificados, la relación entre la identidad de un usuario y su llave pública.

Palabras clave

Autoridad de certificación, Certificado digital, Firma digital, Criptografía de curva elíptica, SHA

Abstract

Considering that in El Salvador the digital signature law was approved just over two years ago in order to grant it the same legal power as the handwritten signature, the application developed with the Bouncy Castle API was created to help and facilitate the process of sign and verify documents, and generate certificates to provide services of authentication, data integrity and non-repudiation. The application is divided in two parts, the first, a desktop software built in Java Swing to generate the private-public key pair and uses the Elliptic Curve Digital Signature Algorithm (ECDSA), due to smaller keys needed, and the hash function SHA3 for digital fingerprint, the second is, a web application in JSP for generating digital certificates that simulates the tasks of a Certification Authority (CA) as a certificate provider, where users can request them and these are sent to the applicant's mail, the root certificate auto-signed as part of a Public Key Infrastructure (PKI) is used to sign the certificates generated to other users. A CA pro-

vides its certification services that guarantees to third parties, which trust their certificates, the relationship between a user's identity and his public key.

Keywords

Certificate authority, Digital certificate, Digital signature, Elliptic curve cryptography, SHA

INTRODUCCIÓN

La firma digital certificada son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos, así como autenticar que la persona firmante es quien dice ser (Ley de Firma Electrónica, 2015). No confundir el término firma digital con el simple escaneo de una firma autógrafa y su inserción en un documento como imagen.

La firma digital se basa en criptografía de llave pública como RSA y Curvas Elípticas. Un esquema de firma digital consiste en 3 algoritmos: a) un algoritmo de generación de llaves, la salida es una llave privada con su correspondiente llave pública; b) un algoritmo de firma digital, que, dado un mensaje y la llave privada produce la firma como salida; y c) un algoritmo de verificación, que, dada la llave pública, el mensaje y la firma acepta o rechaza la autenticidad e integridad del mensaje. Como parte del proceso de firma, el documento o mensaje a firmar se transforma en huella digital de longitud fija, la cual se obtiene de aplicar una función resumen, cuya salida se le conoce como digesto.

Un certificado digital o certificado de llave pública, como se le conoce en criptografía, es un documento electrónico usado para probar la propiedad de una llave pública, este incluye de acuerdo con el estándar X.509 ((IETF)) ciertas partes, entre ellas: la llave pública e identidad del propietario, firma digital de la CA y período de validez. La CA es la entidad de confianza responsable de emitir y revocar certificados firmándolos con su llave privada, normalmente estas tienen un certificado raíz auto firmado o firmado por la CA raíz que la identifica como la autoridad de certificación, a la CA raíz también se le conoce como ancla de confianza.

Para llevar a cabo la tarea de firmar un documento como remitente o de verificar una firma como destinatario de un documento es necesaria una herramienta que facilite ambas tareas, pues típicamente los usuarios no entienden la seguridad con que se deben manejar cosas como llaves secretas o llaves privadas, o tienen muy básica formación en uso de tecnologías de la información, por ello, el presente documento es una propuesta técnica de una aplicación informática para firmar, verificar, generar el par de llaves privada-pública, gestionar estas llaves y brindar seguridad sobre la llave privada a través de almacenamiento seguro mediante cifrado simétrico. Existen librerías criptográficas, entre ellas OpenSSL y Bouncy Castle como dos de las más documentadas y usadas, la primera en C y la segunda en versiones para Java y C# de .NET, en este caso se utiliza a Bouncy Castle que ofrece las características necesarias en cuanto a funciones y algoritmos necesarios involucrados en la firma digital.

El sistema emisor de certificados está representado por una aplicación web construida en JSP, que cumple con elementos de un esquema PKI del estándar RFC 3820 , donde los usuarios del software de firma-verificación pueden solicitar los certificados y de esta forma garantizar la relación entre la identidad de un usuario y su llave pública, esta aplicación es quien simula ser una CA, luego un correo electrónico es enviado al usuario solicitante con el certificado generado con el estándar X.509 V3 ((IETF)), al igual que la aplicación de escritorio, la aplicación web también utiliza la API Bouncy Castle para la implementación de los algoritmos criptográficos.

ANÁLISIS DEL PROBLEMA

Actualmente en El Salvador a través del Ministerio de Economía se realizan esfuerzos para la implementación de la firma digital por medio de la creada Unidad de Firma Electrónica, por lo tanto, es necesario anticipar los retos y recomendaciones a los que esta unidad se va a enfrentar. El proceso de obtención de una firma electrónica deberá incluir el software y la capacitación en el uso, el cual será regulado en el Reglamento de la Ley de Firma Electrónica. La ley también establece la equivalencia jurídica a aquellas autoridades certificadoras que cumplan con los requisitos técnicos emanados por la Unidad de Firma Electrónica y que se sometan a la evaluación para respaldar la competencia técnica y credibilidad de los entes acreditados, (Reglamento de la Ley de Firma Electrónica, 2015) por lo que será posible tener una o varias CA's. En la actual ley no se contemplan decisiones técnicas referentes a la criptografía, y considerando que podrá existir más de una CA, esto debe ser estandarizado utilizando algoritmos que provean las garantías de seguridad mínimas con respecto a la calidad y al tamaño de las llaves, además las funciones de resumen para el cálculo de las huellas digitales de los archivos no deben estar "rotas". Debe mencionarse que la vulnerabilidad de la criptografía empleada dependerá en gran medida de estas decisiones de seguridad, donde los algoritmos como SHA-1 para cálculo de digestos o el RSA de 1024 bits son altamente frágiles. Además, el uso de contraseñas ideadas por seres humanos es otro punto importante, esto porque la Unidad de Firma Electrónica debe implementar almacenamiento seguro en llaves privadas de los usuarios y que estas estén protegidas contra lecturas no autorizadas, para ello nuevamente el tamaño de llave y la entropía de las contraseñas juegan un papel relevante, y dar las garantías de seguridad necesarias. También se debe diseñar el software para la firma electrónica considerando criterios de usabilidad y una interfaz amistosa para su fácil uso, pues normalmente el eslabón más débil en la seguridad de la información es la llamada "capa 8" y una aplicación compleja con funcionamiento poco intuitivo y en adición a malas decisiones técnicas de diseño dará como resultado que la llave privada del firmante se vea comprometida y dar lugar a ataques de *usurpación de identidad*. Mencionar que actualmente no se conoce ninguna herramienta desarrollada o esfuerzo por parte de la Unidad de Firma Electrónica en El Salvador para desarrollar un software como el propuesto en el presente artículo.

METODOLOGÍA

Para el desarrollo de la aplicación y la determinación de requerimientos se utiliza como referencia la metodología ágil SCRUM, y basándose en algunos de sus artefactos como: Pila del Producto, Pila del Sprint y Sprint (Scrum Manager Body of Knowledge, 2018).

Visión del Producto

La aplicación debe permitir a los usuarios de firma electrónica:

- Generar el par de llaves privada-pública y permitir exportar estas llaves a un formato estándar de codificación Base64 como Privacy Enhaced Mail (PEM)
- Seguridad basada en usuario y contraseña para el propietario del par de llaves, codificando la contraseña con una función de resumen, se debe aplicar reglas para fortalecer la entropía de la contraseña
- Protección de la llave privada, por medio de cifrado, usando un algoritmo de llave secreta (cifrado por bloques)
- Firma de documentos con algoritmo de llave publica, y permitir exportar esta firma a archivo en formato Abstract Syntax Notation One (ASN.1)
- Verificar documentos firmados utilizando la llave pública o certificado del signatario, archivo de firma y archivo firmado

- Verificar firma de certificados emitidos por CAs acreditadas
- Importar claves respaldadas por la misma aplicación

Para la plataforma web

- Generar los certificados en el formato X.509 V3 que contienen la llave pública generada por el usuario.
- Firmar como CA los certificados generados, en el entendido que, se comprueba de forma inequívoca la identidad de las personas a quienes se les genera los certificados digitales.
- Servir de repositorio al público de todos los certificados con llaves públicas generados para que puedan los usuarios de forma independiente comprobar a través de la aplicación de escritorio la firma de los documentos.
- Descarga de la aplicación de firma-verificación publicando su huella digital para comprobar su integridad

Pila del Producto

En líneas generales la Pila del Producto es una lista ordenada o priorizada de las tareas que componen el proyecto de aplicación.

Pila del Producto

ID	Nombre	Descripción	Estimación (Horas)
1	Codificación de Clases app desktop	Codificar las Clases a utilizar en la aplicación de firma, verificación y generación del par de llaves	20
2	Creación de Interfaces de usuario app desktop	Diseñar y probar las Interfaces de usuario para la aplicación de firma, verificación y generación del par de llaves	10
3	Integración Clases e Interfaces app desktop	Programación de eventos y flujos del programa	25
4	Codificación de las Clases app web	Codificación de las Clases que guardan la información de los usuarios y de la Autoridad Certificadora.	5
5	Codificación de los controladores app web	Codificación de los controladores que permiten la generación de los certificados auto firmados de la CA y los certificados de los usuarios.	10
6	Diseño gráfico app web	Diseño gráfico de la página principal y de los formularios de proceso.	20
7	Realización de pruebas y ajustes app web y desktop	Realización de pruebas entre los datos generados por la aplicación web y la aplicación de escritorio.	25

Pila de Sprint

La Pila del Sprint es una lista de tareas que se van a realizar en una iteración, para construir un incremento o componente de la aplicación. Para cada una registra la información: descripción breve, persona que la tiene asignada, esfuerzo para terminarla.

Un Sprint es un bloque temporal, y en cada iteración se proporciona un resultado completo llamado entregable, el cual es un producto disponible para ser utilizado (Scrum Manager Body of Knowledge, 2018).

Pila del Sprint

ID	Elemento de la Pila de Producto	Tarea del Sprint	Sprint asignado
1	Codificación de Clases app desktop	Codificar Clase de manejo de usuarios y base de datos	1
		Codificar Clase del cifrado por bloques AES parametrizando el tamaño de llave	1
		Escribir Clase para firma y verificación usando ECDSA, el formato de salida de la firma será ASN.1 y la curva utilizada de 256 bits	1
		Escribir Clase para funciones Hash desde SHA1 hasta SHA3-512	1
		Codificar utilerías para manejo de archivos y lanzador de programa	1
2	Creación de Interfaces de usuario app desktop	Diseñar interfaz de Inicio de sesión y registro de usuario	1
		Creación de ventana para importar llaves	1
		Creación de ventana principal de 4 opciones: Firmar, Verificar, Perfil y Exportar llaves	1
		Diseñar ventana para validar contraseña en el proceso de firma y descifrar llave privada	1
3	Integración Clases e Interfaces de usuario app desktop	Programar eventos que dirigen la ventana principal	2
		Realizar la codificación de eventos y flujo de ventana de inicio de sesión y registro de usuario	2
		Programar eventos de importación de llaves	2
		Codificar la entrada y validación de contraseña para extraer la llave privada	2
4	Codificación de las Clases app web	Análisis de las necesidades de almacenamiento de datos.	3
		Codificación de las Clases y su abstracción usando la metodología Code First.	3
		Generación de las Clases en la base de datos y configurar las actualizaciones por migraciones.	3
5	Codificación de los controladores app web	Codificación de los controladores y las vistas bajo el esquema Modelo-Vista-Controlador.	3
6	Diseño gráfico app web	Diseñar interfaces de registro, solicitud, búsqueda y descarga de certificados	3
		Generación de las imágenes y sus retoques.	3
		Programación en JavaScript para dinámica de la página principal.	3
7	Realización de pruebas y ajustes app web	Verificación de la interoperabilidad entre la app de escritorio y la app web.	4
		Corrección de los errores encontrados.	5

Cada Sprint como bloque temporal e iterativo incluye pruebas a cada entregable como tarea adicional

Funcionamiento del software

La aplicación se divide en dos partes: A) aplicación de escritorio para firma-verificación y B) aplicación web para emisión de certificados, ambas programadas con el API Bouncy Castle, la funcionalidad de cada una se describe a continuación.

A) Aplicación de escritorio para firma y verificación

1. Descripción técnica

La aplicación permite cuatro opciones principales: perfil, firmar, verificar y exportar llaves. La opción *perfil* permite manejar los datos del usuario, su par de llaves generado de acuerdo a Fig. 3, y llave secreta. La opción *firmar* solicita el documento a firmar, realiza el proceso de firma que se describe en Fig. 1 y se obtiene como salida un archivo separado de firma con formato ASN.1. La opción *verificar* solicita el documento firmado, el archivo separado de la firma, y la llave pública o certificado del firmante, luego sigue el proceso descrito en Fig. 2 y se obtiene como salida si la firma es correcta o no, adicional a esto la firma en el certificado se verifica para saber que la procedencia es la CA de confianza (aplicación web). La opción *exportar llaves* permite obtener archivos en formato PEM de cada una de las llaves (privada y pública).

Otras opciones ofrecidas por la aplicación son: importar llaves (privada-pública) respaldadas por la misma aplicación, cambiar la llave secreta con la que se cifra la llave privada según Fig. 1. Todo lo anterior precedido de una autenticación de usuario y clave secreta del usuario para poder acceder a las opciones ya mencionadas.

Especificaciones técnicas para firma

Algoritmo de firma	Elliptic Curve Digital Signature Algorithm (ECDSA)
Curva utilizada	Secp256k1
Función Hash para Huella Digital	SHA3-256withECDSA
Cifrador por bloques	AES
Tamaño de llave para AES	256 bits (32 bytes)
Función Hash para cifrado de llave privada	SHA3-256
Formato de salida de firma	Abstract Syntax Notation One (ASN.1)
Formato de exportación de llaves y certificados	Privacy Enhaced Mail (PEM)
Entropía de contraseña	10 caracteres (4 palabras aleatorias)

De acuerdo a los tamaños de llaves y algoritmos sugeridos por el NIST (National Institute of Standards and Technology) las especificaciones anteriores superan la seguridad mínima requerida en cada uno de ellos siendo como objetivo mínimo una seguridad de 128 bits.

2. Diagramas de Bloques

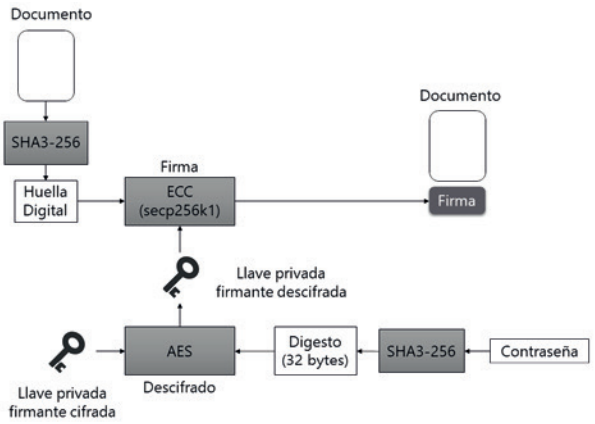

Fig. 1. Firma usando ECC (secp256k1) y SHA3-256.

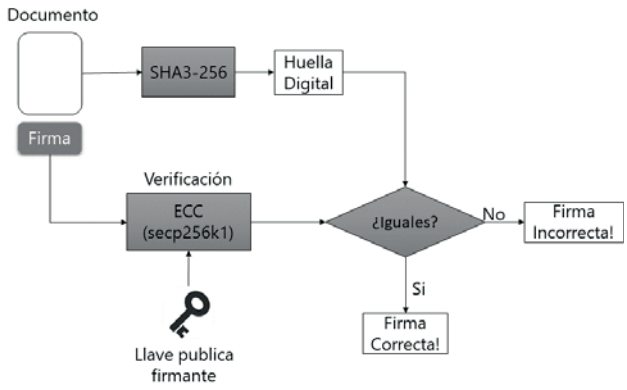

Fig. 2. Verificación de la firma.

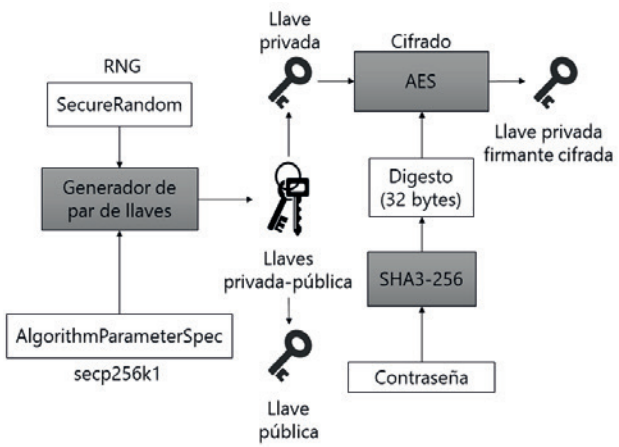

Fig. 3. Generación de par de llaves y cifrado de llave privada

3. Diagrama de Clases

A continuación, se presenta el diagrama de Clases, con las clases creadas para dar soporte a lógica de la aplicación, así como sus algoritmos criptográficos empleados, manejo de base de datos y utilerías adicionales.

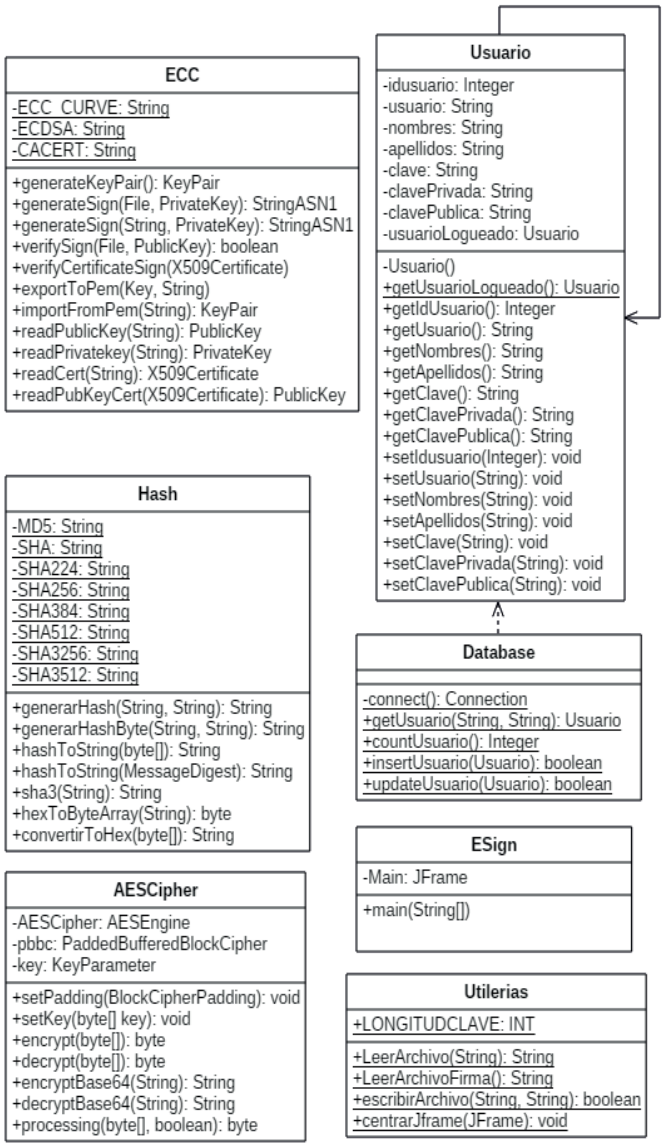

Fig. 4. Diagrama de Clases. Clases creadas para dar soporte a la aplicación

4. Diseño de interfaces de usuario (IU)

A continuación, la interfaz de usuario principal es mostrada y las opciones disponibles son: perfil, firmar, verificar y exportar llaves, estas opciones aparecen en pestañas y en un menú lateral, a continuación de ellas se describen otras auxiliares. Cabe destacar que cada una de las opciones solamente requiere unos 3 a 4 clics y un par de selecciones por parte del usuario tomando como base una forma sencilla y practica de funcionar.

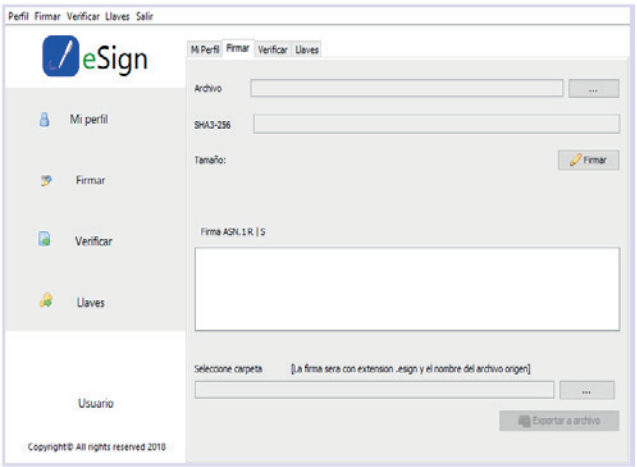

Fig. 5. Interfaces de usuario (IU) ventana principal.

Otras IU adicionales para el funcionamiento se describen a continuación:

- Cambiar Clave: permite el cambio de contraseña de usuario.
- Importar Llaves: ventana usada para importar pares de llaves generadas y respaldadas de la misma aplicación.
- Login: brinda entrada de usuario y contraseña para iniciar sesión en la aplicación.
- Passphrase: ventana diseñada para solicitar la contraseña para descifrar la llave privada.
- Registrarse: utilizada para registrar usuarios cuando la aplicación esta recién instalada, permite generar el par de llaves o importarlas.

B) Aplicación web para emisión de certificados

1. Descripción técnica

La aplicación web es el lugar donde se generan los certificados para cada usuario y donde los usuarios pueden consultar los certificados de otros usuarios, para ser utilizados para la verificación de la firma de los documentos.

La aplicación web tiene como finalidad realizar las siguientes actividades:

- Generar sus propias llaves y su correspondiente certificado auto firmado como Autoridad Certificadora.
- Obtener la llave pública de cada usuario y sus datos personales para generar su certificado de acuerdo a Fig. 6 y ser enviado por correo electrónico.
- Establecer una coincidencia entre cada persona y su correspondiente certificado V3 (IETF) que contiene la llave pública del usuario.
- Poner a disposición del público todos los certificados públicos generados para su descarga.
- Permitir a la autoridad certificadora generar nuevos certificados de usuarios y renovación para los ya existentes cuando estos expiran.
- Deshabilitar los certificados cuando estos expiran.

2. Diagrama de bloques.

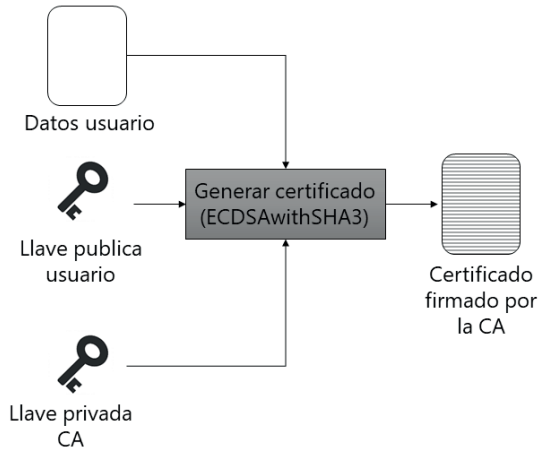

Fig. 6. Generación del certificado.

3. Diagrama de Clases.

En el siguiente diagrama se detallan las clases utilizadas para soportar la aplicación web adicionales a las de Fig. 4.

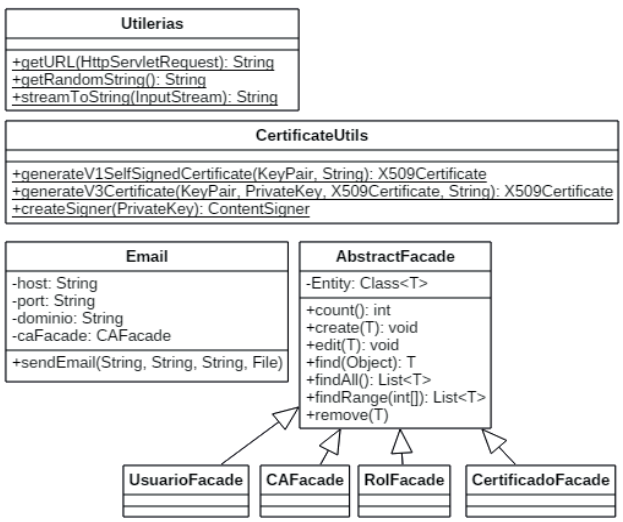

Fig. 7 Clases que soportan la aplicación web.

4. Diseño de interfaces

A continuación, se muestran las interfaces de registro y solicitud de certificados, y mencionar que existen vistas para buscar y descargar certificados de otras personas, así como de un inicio de sesión, perfil y cambios de contraseña.

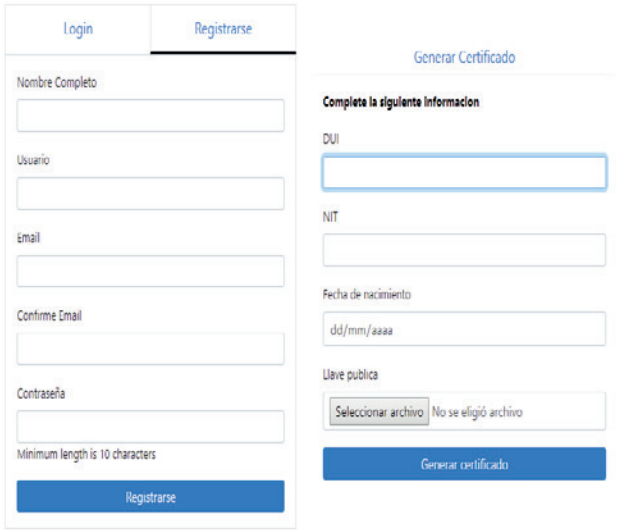

Fig. 8 Interfaces de usuario de la aplicación web.

5. Base de datos

La aplicación web utiliza la siguiente base de datos:

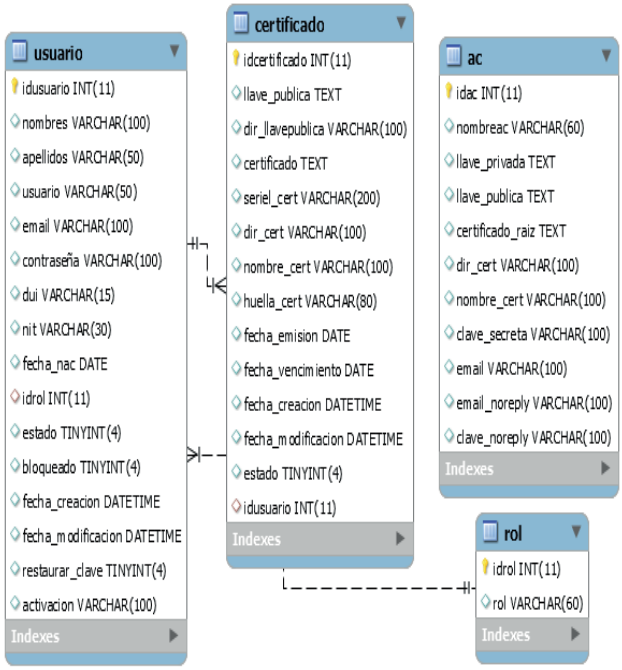

Fig. 9 Diagrama Entidad-Relación de la base de datos

CONCLUSIONES

- El desarrollo de una infraestructura que soporte a una Autoridad Certificadora es un desafío que implica el conocimiento de algoritmos criptográficos y de programación para su implementación.
- Que el algoritmo de curvas elípticas representa una opción para el almacenamiento de llaves en dispositivos con poco almacenamiento o en sistemas donde se requieren almacenar grandes cantidades de llaves públicas, dado que por su tamaño ocupan menos espacio en disco.
- Representa una decisión importante de diseño establecer los algoritmos criptográficos, con la suficiente seguridad como para resistir a los criptoanálisis y avances tecnológicos y matemáticos que podrían vulnerarlos.
- En el presente documento no se emplearon procedimientos como por ejemplo los señalados por WebTrust o ETSI como mecanismos de control a las autoridades certificadoras (ETSI) (WebTrust).
- Los algoritmos utilizados, tanto simétricos, asimétricos o Hash, responden a un tamaño mínimo de llave seguro contra ataques de fuerza bruta (128 bits), arma preferida de un hacker, y aún se desconocen vulnerabilidades en ellos.
- La firma o verificación son procesos complejos en su interior, pero que, a través de la aplicación propuesta, con interfaz amigable y las consideraciones de usabilidad tomadas en cuenta se hace un proceso más sencillo y práctico para cualquier usuario.
- La aplicación de firma electrónica propuesta brinda los servicios de autenticación, integridad de los datos y no repudio, que son el propósito principal buscado y puede servir como base, pues actualmente no se conoce ninguna herramienta o esfuerzo por parte de la Unidad de Firma Electrónica en El Salvador para desarrollar una como la propuesta en el presente artículo.
- La aplicación de escritorio puede ser fácilmente adaptable para personas jurídicas o para distintos algoritmos de cifrado o hashes.
- Por estar escrita en Java es multiplataforma y puede llegar a una cantidad más grande de usuarios

RECOMENDACIONES

- La aplicación de firma requiere atención especial en el manejo de la clave secreta, pues no hay forma de recuperarla si esta es olvidada, si se emplearan mecanismos de recuperación de clave en línea se puede comprometer la llave privada, se deja para análisis posteriores la recuperación de la clave secreta
- Añadir un llavero para manejo de los certificados o llaves públicas, con el objetivo de poder ubicarlos desde la misma aplicación
- Agregar intentos y tiempo entre intentos al formulario de inicio de sesión para evitar ataques de fuerza bruta y de diccionario
- Publicar un manual explicando cómo comprobar la integridad de la aplicación de firma-verificación a través de su huella digital para evitar alteraciones maliciosas del software.
- Implementar una CRL (Certificate Revocation List) o mecanismo para verificar los certificados válidos y no válidos de forma automática por la aplicación de escritorio para firma y que el usuario pueda estar seguro que el certificado es confiable.
- Crear una política de contraseñas fáciles de recordar, para las personas, pero con una entropía muy alta.

REFERENCIAS

Asamblea Legislativa de El Salvador (2015). Ley de Firma Electrónica. *Diario Oficial*. Obtenido de http://www.transparencia.gob.sv/institutions/dc/documents/139830/download

Asamblea Legislativa de El Salvador (2015). Reglamento de la Ley de Firma Electronica. *Diario Oficial*. Obtenido de http://www.transparencia.gob.sv/institutions/minec/documents/127305/download

(IETF), I. E. (s.f.). *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* . Obtenido de Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile : https://tools.ietf.org/html/rfc6818

ETSI. (s.f.). Obtenido de ETSI: http://www.etsi.org

Internet Engineering Task Force (IETF). (s.f.). *Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. Obtenido de https://tools.ietf.org/html/rfc6818

NIST. (s.f.). *Digital Signature Standard (DSS)*. Obtenido de Digital Signature Standard (DSS): https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.186-4.pdf

NIST. (s.f.). *Recommendation for key management*. Obtenido de Recommendation for key management: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

NIST. (s.f.). *Secure Hash Standars (SHS)*. Obtenido de Secure Hash Standars (SHS): https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

NIST. (s.f.). *SHA3 Standar*. Obtenido de SHA3 Standar: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

Scrum Manager Body of Knowledge. (2018). Obtenido de Scrum Manager Body of Knowledge: http://www.scrummanager.net/bok/index.php?title=Scrum_Manager_BoK

WebTrust. (s.f.). Obtenido de WebTrust: http://www.webtrust.net

La importancia de las buenas prácticas en el desarrollo de aplicaciones web seguras y las repercusiones de no implementarlas

Álvaro Zavala
alvarohz@usonsonate.edu.sv
Iván Alvarado
ioalvarado@usonsonate.edu.sv
Facultad de Ingeniería y Ciencias Naturales – Universidad de Sonsonate

*Este artículo ya ha sido publicado anteriormente en: Á. Zavala and I. Alvarado, "The importance of good practices in the development of secure web applications and their repercussions for not implementing them," 2018 IEEE 38th Central America and Panama Convention (CONCAPAN XXXVIII), San Salvador, 2018, pp. 1-5.
doi: 10.1109/CONCAPAN.2018.8596528

Resumen

En este artículo, se elabora un análisis de la importancia de la seguridad en los procesos de desarrollo de software y cómo los errores relativamente simples tienen serias repercusiones en los sistemas, que son cada vez más complejos y, por lo tanto, es cada vez más difícil identificar todas las vulnerabilidades en ellos, para este fin. Se consultó y sistematizó la documentación orientada a la mitigación de riesgos de seguridad en aplicaciones web.

Palabras clave

buenas prácticas, seguridad, desarrollo de software, riesgos, aplicaciones web.

Abstract

In this article, an analysis of the importance of security in software development processes is elaborated and how relatively simple errors have serious repercussions on systems, which are becoming more complex and therefore it is increasingly difficult to identify all the vulnerabilities in them, for this purpose, documentation oriented to the mitigation of security risks in web applications was consulted and systematized.

Keywords

good practices, security, software development, risks, web applications

INTRODUCCIÓN

Actualmente el desarrollo web se encuentra en auge y crece a un ritmo vertiginoso, cada vez son más las aplicaciones que funcionan a través de internet, esto incluye las aplicaciones móviles, y la complejidad del software también se eleva haciendo cada vez más difícil identificar vulnerabilidades antes de ponerlos en producción, sin mencionar que normalmente la seguridad es un factor que a menudo no se le da la importancia en los procesos de desarrollo que esta merece y se cometen errores relativamente simples de evitar.

El propósito del presente documento es exponer la importancia en la implementación de seguridad en el desarrollo de aplicaciones web, pese a la disminución de productividad y eficiencia que estas producen en los aplicativos. Explorando los conceptos preliminares de la seguridad informática, estableciendo el mecanismo de sistematización de los principales riesgos que se enfrentan en el desarrollo de aplicaciones web y las conclusiones respecto a los hallazgos.

Preliminares

Principios de seguridad

En general los tres objetivos de la seguridad informática son:

- Confidencialidad: protección contra accesos no autorizados,
- Integridad:protección contra modificaciones no autorizadas
- Disponibilidad: protección contra interrupciones en el acceso

Tres leyes de la seguridad

- Los sistemas absolutamente seguros no existen.
- Disminuir las vulnerabilidades de un sistema a la mitad implica duplicar los costos de seguridad.
- Típicamente la criptografía no es vulnerada sino brincada.

Principales riesgos

Los problemas de seguridad pueden dañar la imagen, cuestan dinero y tiempo, restan competitividad, reducen la confianza y pueden acarrear implicaciones legales

Los ataques pueden tener diferentes orígenes, pero de forma general y para el presente artículo se consideran los siguientes:

Inyecciones SQL: Un ataque por inyección SQL consiste en la inserción o "inyección" de una consulta SQL por medio de los datos de entrada desde el cliente hacia la aplicación. Un ataque por inyección SQL exitoso puede leer información sensible desde la base de datos, modificar la información (Insert/ Update/ Delete), ejecutar operaciones de administración sobre la base de datos (tal como parar la base de datos), recuperar el contenido de un determinado archivo presente sobre el sistema de archivos del DBMS y en algunos casos emitir comandos al sistema operativo.

Ataques de fuerza bruta y/o diccionario: un ataque de fuerza bruta consiste en un algoritmo que intenta repetidamente todas las combinaciones posibles de contraseñas o claves de cifrado hasta encontrar la correcta y en combinación con un diccionario de contraseñas comunes podría reducir la cantidad de intentos para encontrar la correcta.

En lugar de atacar la criptografía los atacantes intentan aprovechar la fragilidad de la entropía o tamaño de las claves, pues normalmente los usuarios hacen malas elecciones que podrían comprometer la seguridad de todo el sistema o simplemente utilizan configuraciones por "default".

Usurpación de identidad: Consiste en apropiarse de la identidad de una persona, en el caso de los sistemas seria obtener acceso con las credenciales de alguien más, este objetivo se puede lograr de muchas formas, desde ataques de fuerza bruta y/o diccionario, ingeniería social, inyecciones SQL o meramente errores de la llamada "capa 8".

Ingeniería social: Un ataque que aprovecha al eslabón más débil de la seguridad y está basado en engañar a los usuarios o administradores en el sitio de destino para revelar información confidencial o sensible. Es importante mencionar que estos ataques son los difíciles de mitigar porque, de que sirve construir la muralla de seguridad más cara en el mundo si un usuario deja la puerta abierta.

Los ataques antes mencionados ponen en riesgo los 3 objetivos de seguridad pues en todos los casos podrían evitar que se cumplan, desde modificaciones a una base de datos que compromete la integridad hasta fuga de información por accesos no autorizados donde se compromete la confidencialidad. La disponibilidad puede verse comprometida por usurpaciones de cuentas de administrador con los permisos necesarios para ello. A veces las medidas para contrarrestar estos ataques solo requieren que se les preste atención durante los ciclos de vida de desarrollo, y solo a veces podrían derivarse de errores "honestos" de los programadores.

Aplicaciones Web

Se denomina aplicación web a aquella herramienta que se accede a través de internet o intranet por medio de un navegador y están alojadas por tanto en un servidor que interpreta un lenguaje de programación y produce como salida un código interpretable por los navegadores.
Actualmente las aplicaciones a las que se accede desde un navegador se han vuelto muy populares, pues no dependen de un sistema operativo para funcionar, son ligeras y solo necesitan una URL para ejecutarse.

Las aplicaciones web son las más vulnerables debido al nivel de exposición en el que se encuentran, esto podría respaldarse por algunas de las estadísticas publicadas, en la cual se puede observar que gran parte de las vulnerabilidades que fueron reportadas en el período entre 2015 y 2016, en el cual se desarrollaron los casos mencionados por dicha publicación, corresponden con aplicaciones web.
El desarrollo de aplicaciones debe considerar una serie de aspectos para minimizar las vulnerabilidades de las aplicaciones como los siguientes:

- Autorización
- Autenticación
- Persistencia
- Sesiones
- Validación de datos de entrada
- Manejo de excepciones, auditoría y trazas
- Servicios Web
- Criptografía

Existen diversas fuentes que ofrecen recomendaciones en el tema de desarrollo de software seguro y han sido considerados para el análisis posterior .

METODOLOGÍA

Durante el desarrollo de la investigación, se hizo revisión bibliográfica en la que se recopilaron e identifican buenas prácticas relativas al desarrollo de aplicaciones. Y posteriormente para poder determinar cuáles son los componentes que cada tecnología, marco de trabajo o herramienta brinda, así como también, para ver qué servicios de seguridad integran con mayor facilidad a los mismos, se realizó un análisis de contenido.

Los criterios utilizados para la revisión bibliográfica son dos:

- Última versión publicada: Contar con fecha de publicación superior al año 2,000 y ser la última edición.

- Alcance: La fuente deberá proporcionar buenas prácticas enfocadas o relacionadas al desarrollo de aplicaciones.

Considerando los criterios citados se identificó 11 fuentes de información documental, provenientes de marcos de trabajo, estándares y libros. Para la extracción de las buenas prácticas.

CMMI DEV, Versión 1.3, SEI

Guía de los fundamentos para dirección de proyectos, quinta edición, PMI. 2012

Agile software requeriments-learn requeriments practices for teams, programas, and the Enterprise, Dean leffinwel, primera edición. 2011.

Rational unified process: overview, rational software corporation, 2001.

Guía práctica de gestión de requisitos, INTECO. 2008

Software engineering quality practices, Ronald Kirk, kandt, primera edición. 2006.

Software requirements, Wiegers & Beatty, tercera edición. 2013.

Software engineering best practices. Carpers Jones, primera edición. 2010.

System engineering Handbook-NASA/SP-2016-610SRev2. NASA. 2017.

SWEBOK, Version 3, IEEE Computer society. 2014.

Requirements Engineering-Fundamentals, Principles, and techniques, Klaus Pohl, primera edición. 2010.

De las 11 fuentes de información se sistematizó un banco de 201 buenas prácticas. Las 201 buenas prácticas se sintetizaron en 72 buenas prácticas. De las 72 buenas prácticas se abordan y desarrollan 13 referidas a la mitigación de riesgos de seguridad.

El análisis de contenido se enfoca en la revisión de las características que las tecnologías ofrecen en los sitios oficiales.

Identificación de buenas prácticas relativas al desarrollo de aplicaciones

A continuación, se establecen trece de las buenas prácticas a emplear para evitar o mitigar los ataques potenciales mencionados en los preliminares.

Emplear sentencias SQL precompiladas, esto significa evitar el uso de escribir sentencias SQL concatenadas como por ejemplo:

```
“..usuario = ‘”+ vUser + “’”;
```

Lo anterior da lugar a inyectar código malicioso en los programas, con las sentencias precompiladas la consulta es primero compilada para más adelante recibir los valores de los parámetros, pero sin posibilidad de que la consulta (tablas, índices, campos, valores y joins) sea modificada.

Construir una clase de saneamiento de SQLs, esto implica escribir rutinas que permitan depurar la captura de datos de entrada removiendo caracteres extraños como {“, ‘ , . , \, <, >, | , ~, ;, ! } y todos los caracteres que permitan hacer una inyección que incluso podría afectar a nivel del sistema operativo del servidor y lograr interrumpir el servicio, o lograr accesos no autorizados.

Emplear funciones Hash que no estén “rotas”, una función Hash es una función computacionalmente eficiente de mapeo de cadenas binarias de longitud arbitraria a cadenas binarias de cierta longitud fija, denominadas digestos. Los usos criptográficos más comunes de las funciones Hash en los sistemas son la integridad de datos, confidencialidad y autenticación.

Es debido a esta longitud fija de los digestos que las funciones Hash son vulnerables a romperse, significando que las colisiones pueden ocurrir y por lo tanto dejan de ser seguras como el caso de MD5 y SHA1, una característica primordial de un función Hash es que para una

entrada A solo existe una única salida B, una colisión significa que para una entrada distinta A' puede repetirse la salida B, logrando en el caso de un servicio de autenticación por medio de contraseñas almacenadas usando MD5 que sin conocer la contraseña A, puede usarse otra contraseña A' para generar B y así obtener acceso a un sistema sin conocer la verdadera contraseña, por lo tanto el NIST sugiere el uso de SHA2 en adelante para evitar esta vulnerabilidad.

En algoritmos criptográficos utilizar tamaños de llave de 128 bits de acuerdo con las recomendaciones del NIST.

Un ataque de fuerza bruta y/o diccionario consiste en intentar todas las posibles llaves hasta dar con la correcta. Este tipo de ataque es factible según el número de posibles llaves lo cual suele venir dado por la longitud (tamaño) de la llave.

El objetivo del atacante es usurpar la identidad de un usuario al encontrar sus credenciales de acceso.

Si las consideraciones necesarias son tomadas a la hora de seleccionar el tamaño de llave un ataque de fuerza bruta solamente tendría éxito en unos 5.4 x 10^24 años. Es prácticamente intratable a no ser que surgieran avances tecnológicos importantes que permitan realizar estos ataques de forma más eficiente como la computación cuántica.

No construir algoritmos criptográficos propios, la fortaleza reside en la calidad del algoritmo (principio de Kerckhkoff: el oponente conoce el algoritmo).

Partiendo de la premisa que el oponente conoce el algoritmo la fortaleza de este no debe descansar en que el algoritmo sea secreto pues a través de la historia está demostrado que esto nunca ocurre así, por lo contrario, el secreto siempre ha sido una llave (como ejemplos la criptografía simétrica y asimétrica), por lo tanto, se deben utilizar algoritmos y protocolos estandarizados cuya fortaleza matemática ha sido probada y garantizada por especialistas criptógrafos como criptoanalistas.

Utilizar autenticación multifactor. Esta se basa en tres factores: algo que se (una contraseña), algo que tengo (un teléfono o token) y algo que soy (biometría).

La autenticación multifactor combina 2 ó 3 de estos factores, el objetivo es crear una defensa por capas y hacer que sea más difícil para una persona no autorizada acceder a un objetivo, como una ubicación física, un dispositivo de cómputo, una red o una base de datos. Si uno de los factores se ve comprometido o se rompe, el atacante todavía tiene al menos una barrera más que romper antes de ingresar con éxito en el objetivo, lo anterior garantiza que errores de usuario en la protección de contraseñas, por ejemplo, no tengan la repercusión que tendría si la seguridad solo descansara en un factor.

Implementar reglas para establecer fortaleza de contraseñas, desde que Shannon acuñó el término, "Entropía" se ha utilizado en criptografía como una medida de la dificultad para adivinar o determinar una contraseña o una clave. Claramente la clave o contraseña más fuerte de un particular tamaño es una selección verdaderamente aleatoria.

Se explica cómo estimar la entropía de una contraseña y normalmente se suele añadir aleatoriedad agregando caracteres especiales y combinación de mayúsculas y minúsculas, y con una longitud mínima de 10 caracteres.

Limitar la cantidad de intentos y tiempo entre intentos en las interfaces de inicio de sesión, si se considera que la entropía de una contraseña pudiera verse comprometida una segunda barrera para evitar un ataque de fuerza bruta y/o diccionario son estos límites, pues se vuelve aún más ineficiente intentar vulnerar un sistema de esta forma ya que los intentos están limitados y partir de superar este limite el usuario queda

bloqueado por lo que los posteriores intentos serian totalmente en vano.

Aumentar el tiempo entre intentos se ve típicamente en dispositivos móviles, pero puede ser utilizado en aplicaciones web sin ningún problema, el objetivo al igual que el límite de intentos es hacer el ataque estéril y no dejar que la no aleatoriedad de una contraseña comprometa la seguridad.

Implementar bitácoras o log de eventos por excepciones, modificaciones, errores y toda actividad en el sistema, lo anterior más que mitigar sirve para deducir responsabilidades y obtener indicios de que es lo que ocurrió durante eventos que afectaron el comportamiento, a veces estas alteraciones podrán ser revertidas o por lo menos ayudaran a plantear medidas para contrarrestar errores cometidos antes de que la brecha fuera descubierta y en muchas ocasiones se pueden implementar pistas de auditoria con la intención de establecer control y revisiones periódicas.

Cifrar información sensible en la base de datos, la información debe ser clasificada y debe haber compartimentalización y mientras más delicada y limitada es la cantidad de personas quienes están autorizadas a verla se debe considerar utilizar cifrado simétrico para evitar que, si se compromete la seguridad de la base de datos esta información aun así permanezca confidencial.

Todas las recomendaciones antes dadas sobre la calidad de los algoritmos y tamaños de llaves deben ser consideradas.

Establecer políticas de gestión de contraseñas, una política simple puede ser obligar a cambiar contraseñas cada mes, que evitaría a un atacante pasivo, quien ya cuenta con contraseñas para llevar acabo accesos no autorizados continúe leyendo información confidencial, dicho evento por ser de carácter pasivo no permite de ninguna forma ser detectado pues el objetivo del atacante es llevar a cabo un robo de información de manera continuada a través del tiempo con propósitos, por ejemplo, de espionaje, o establecer ventajas contra sus adversarios.

Todas las políticas deben estar planteadas y ejecutadas en los sistemas por los desarrolladores de software.

Implementar certificados digitales para cada dominio o subdominio, el conocido ataque man-in-the-middle (hombre-en-el-medio) solo es posible cuando estos certificados no han sido implementados permitiendo la usurpación de identidad y con esto poder leer o alterar los mensajes transmitidos por la red, lógicamente la comunicación debe ser cifrada.

Los certificados digitales vinculan a una persona con su llave pública y son emitidos por entes de confianza conocidos como Autoridades Certificadoras en la cual los usuarios confían y por lo tanto confían en los certificados que esta emite, estos certificados logran que no exista el repudio de un mensaje, es decir que una entidad no pueda negar que la comunicación y los mensajes transmitidos en efecto fueron hechos por ella. Comúnmente un adversario podría usurpar la identidad de una persona si consigue su llave privada, para evitar esto se deben implementar protocolos de almacenamiento seguro de llaves como el que propone el software PGP.

Validar la cantidad de sesiones permitidas por usuario y tiempos de sesión, así como la cache de las páginas para evitar mostrar información no autorizada y establecer roles o perfiles de acceso aplicando el principio del mínimo privilegio.

El propósito es limitar lo que cada usuario puede ver y hacer dentro de los sistemas, mientras más granulares son los permisos requiere que se le dedique mayor tiempo de programación elevando los costos, sacrificio que debe hacerse.

El manejo del tiempo de sesión previene errores típicos de usuario que descuidan sus estaciones de trabajo dejando la “puerta abierta” a

potenciales acciones que podrían comprometer al más seguro de los sistemas.

RESULTADOS

Luego de haber sistematizado la información que se recopiló a través del análisis de contenido especificado en la metodología se presentan los siguientes resultados:

- La bibliografía y la capacitación de los programadores en desarrollo de software seguro es poca o escaza
- Al iniciar un proyecto o adquirir un producto, la seguridad no es un requerimiento por lo que se suele obviar.
- No hay o no se usan métodos de verificación en los programas escritos para comprobar su seguridad.
- Las soluciones son simples en muchos casos, pero no se les da la importancia que requieren
- La seguridad aumenta los costos, tiempo y esfuerzo en el diseño, desarrollo e implementación de los sistemas.

Entre los ataques a la seguridad más destacados, que afectan a las aplicaciones web están:

- Re-direccionamiento web.
- Ataques de inyección de código.
- Ejecución de archivos maliciosos.
- Falsificación de solicitudes entres sitios.
- Comunicación insegura.

CONCLUSIONES

Las buenas prácticas deben formar parte de un ciclo de vida de desarrollo de sistemas, estandarizando controles y guías.

Si bien es cierto aplicar todas las practicas acá mencionadas mitigan los riesgos de ataques, pero nada garantiza un sistema 100% seguro, el propósito es no dejar al azar la seguridad y aplicar todas las medidas respectivas cuando sea necesario.

Ante la diversidad de ataques informáticos que existen en la actualidad, los marcos de trabajo para el desarrollo de aplicaciones web tienen que actualizarse y generar diversos mecanismos que permitan al desarrollador proteger sus aplicaciones ante los mismos.

Quienes toman las decisiones en el área de desarrollo no deben enfocarse principalmente en funcionalidad y dejar de lado el tema de la seguridad, aunque esto implique recursos como tiempo y dinero.

Normalmente las vulnerabilidades son conocidas y a veces las soluciones simples, no aplicar las soluciones oportunamente a los problemas de seguridad pueden dañar la imagen, cuestan dinero y tiempo, restan competitividad, reducen la confianza y pueden acarrear implicaciones legales.

Muchos de los ataques tienen como objetivo primario usurpar la identidad de un usuario con la intención de que los servicios de confidencialidad, integridad y disponibilidad se vean comprometidos.

REFERENCIAS

«Página oficial de SANS,» . (13 de 04 de 2018). Obtenido de «Página oficial de SANS,» : https://www.sans.org/critical-security-controls/#s1

Beatty, K. W. (2013). Software Requirements. Redmond: Microsoft Press.

IEEE. (2014). SWEBOK-Guide to the software engineering Version 3.0. Nueva Jersey: IEEE Computer Society Products and Services.

ISACA . (2017). Cybersecurity Fundamentals Study Guide. (2. Edition, Ed.) Obtenido de Cybersecurity Fundamentals Study Guide.

NIST. (s.f.). Recommendation for key management. Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf

NIST. (s.f.). Digital Identity Guidelines. Obtenido de https://nvlpubs.nist.gov/nistpubs/

SpecialPublications/NIST.SP.800-63-3.pdf

OWASP. (s.f.). Inyección SQL. Obtenido de Inyección SQL: https://www.owasp.org

PGP. (s.f.). The GNU Privacy Guard . https://gnupg.org/.

Pohl, K. (2010). Requirements Engineering - Fundamentals, Principles, and Techniques, Springer-Verlag.

Shannon›s, C. (s.f.). A Mathematical Theory of Communication. https://culturemath.ens.fr/sites/default/files/p3-shannon.pdf.

Stallings, W. (2011). Cryptography and Network Security.

Modelo vectorial ampliado ACP de indexación semántica latente en el Procesamiento del Lenguaje Natural para la búsqueda y recuperación de información en documentos electrónicos

Daro Cristian Arias Jaco*
daro.arias@usonsonate.edu.sv
Facultad de Ingeniería y Ciencias Naturales – Universidad de Sonsonate

*Este artículo ya ha sido publicado anteriormente en: D. C. Arias Jaco, "Extended vectorial model ACP of latent semantic indexation in the natural language processing for the sarch and retrieval of information in electronic documents," 2018 IEEE 38th Central America and Panama Convention (CONCAPAN XXXVIII), San Salvador, 2018, pp. 1-6.
doi: 10.1109/CONCAPAN.2018.8596587

Resumen

Este artículo trata el tema de la indexación semántica tardía, visto como un modelo vectorial extendido donde se pueden analizar los componentes principales, se describe el modelo vectorial y el modelo vectorial extendido, aplicando el análisis de los componentes principales a la indexación semántica latente. Finalmente, se proporciona un análisis general sobre la implementación de este método aplicado.

Palabras clave

lenguaje natural, semántica, indexación, recuperación de información, modelo vectorial, valores singulares, vectores propios

Abstract

This paper deals with the issue of late semantic indexing, seen as an extended vector model where the principal components can be analyzed, the vector model is described as well as the extended vector model, applying the analysis of the main components to the latent semantic indexation. Finally, a general analysis on the implementation of this applied method is provided.

Keywords

natural language, semantics, indexing, information retrieval, vector model, singular values, eigenvectors.

INTRODUCCIÓN

El origen del Procesamiento de Lenguajes Naturales se remonta a 1950 cuando Alan Turing publicó Computing machinery and intelligence el cual proponía lo que hoy llamamos test de Turing como criterio de inteligencia (O´connor, s/f). El test de Turing (o prueba de Turing) es una prueba de la habilidad de una máquina de exhibir un comportamiento inteligente similar, o indistinguible al de un humano. Alan Turing propuso que un humano evaluara conversaciones en lenguaje natural entre un humano y una máquina diseñada para generar respuestas similares a las de un humano (Beavers, 2013).

El presente estudio profundiza en un modelo vectorial extendido para la indexación semántica latente como método para la búsqueda y recuperación de información en documentos electrónicos aplicando el análisis de componentes principales como apoyo al modelo general.

DESCRIPCIÓN DE LA INVESTIGACIÓN

Procesamiento de lenguaje natural

El PLN (Procesamiento de Lenguajes Naturales), o NLP por sus siglas en inglés (Natural Language Processing) es un campo de las ciencias computacionales y más en concreto de la inteligencia artificial y la lingüística, esta estudia las interacciones entre las computadoras y el lenguaje humano descrito como un lenguaje natural según la jerarquía de Chomsky (R. Alllen, 2002).

Mediante el PLN se formulan mecanismos eficaces para la comunicación entre personas y computadoras mediante lenguajes naturales, en otras palabras poder establecer una comunicación tan explícita como conversar desde un chat o poder sostener una conversación con una computadora haciendo uso de un sintetizador de voz en la computadora para emular la voz de una persona, el hecho de poder sostener una conversación conlleva a que la computadora pueda entender y aprender un lenguaje natural, es precisamente de lo que trata el procesamiento de lenguaje natural.

Una de las principales aplicaciones que tiene el PLN es la búsqueda y extracción de información en documentos digitales área de aplicación en la que se enfoca esta investigación, aunque cabe destacar que el PLN es usado también en reconocimiento de voz, síntesis de voz, teoría de compiladores traducción automática y en general en inteligencia artificial.

Búsqueda y recuperación de información en documentos digitales

La Búsqueda y Recuperación de Información ,Search and Retrieval Information (ISR) por sus siglas en inglés, es una aplicación del procesamiento del lenguaje natural que trata sobre la búsqueda de información en documentos electrónicos y cualquier tipo de colección documental digital, encargada de la búsqueda dentro de éstos mismos, ya sea a través de internet, una intranet, y como objetivo realiza la recuperación en textos, imágenes, sonido o datos de otras características, de manera pertinente y relevante aunque el presente estudio está enfocado en la búsqueda y recuperación de texto.

La recuperación de información es un estudio interdisciplinario. El proceso de recuperación de información comienza cuando un usuario hace una consulta al sistema. Una consulta a su vez es una afirmación formal de la necesidad de una información. En la recuperación de información una consulta no identifica únicamente a un objeto dentro de la colección. De hecho, varios objetos pueden ser respuesta a una consulta con diferentes grados de relevancia.

La mayoría de los sistemas de recuperación de información computan un ranking para saber cuán bien cada objeto responde a la consulta, ordenando los objetos de acuerdo con su valor de ranking. Los objetos con mayor ranking son mostrados a los usuarios y el proceso puede tener otras iteraciones si el usuario desea refinar su consulta.

Para recuperar efectivamente los documentos relevantes por estrategias de recuperación de información, los documentos son transformados en una representación lógica de los mismos. Cada estrategia de recuperación incorpora un modelo específico para sus propósitos de representación de los documentos, a continuación, se presenta un modelo vectorial extendido para la búsqueda y recuperación de información.

Análisis de componentes principales

El análisis de componentes principales (ACP) es una técnica utilizada para reducir la dimensionalidad de un conjunto de datos. Técnicamente, el ACP busca la proyección según la cual los datos queden mejor representados en términos de mínimos cuadrados. Esta convierte un conjunto de observaciones de variables posiblemente correlacionadas en un conjunto de valores de variables sin correlación lineal llamadas componentes principales.

El ACP se emplea sobre todo en análisis exploratorio de datos y para construir modelos predictivos. El ACP comporta el cálculo de la descomposición en autovalores de la matriz de covarianza, normalmente tras centrar los datos en la media de cada atributo.

Debe diferenciarse del análisis factorial con el que tiene similaridades formales y en el cual puede ser utilizado como un método de aproximación para la extracción de factores.

El ACP construye una transformación lineal que escoge un nuevo sistema de coordenadas para el conjunto original de datos en el cual la varianza de mayor tamaño del conjunto de datos es capturada en el primer eje (llamado el Primer Componente Principal), la segunda varianza más grande es el segundo eje, y así sucesivamente. Para construir esta transformación lineal debe construirse primero la matriz de covarianza o matriz de coeficientes de correlación. Debido a la simetría de esta matriz existe una base completa de vectores propios de la misma. La transformación que lleva de las antiguas coordenadas a las coordenadas de la nueva base es precisamente la transformación lineal necesaria para reducir la dimensionalidad de datos. Además, las coordenadas en la nueva base dan la composición en factores subyacentes de los datos iniciales.

Indexación Semántica Latente apoyada por ACP

La idea fundamental que plantea el modelo vectorial es que la colección de documentos y la consulta se representan como vectores multidimensionales. El espacio vectorial sobre el que se definen estos vectores está generado por el conjunto de vectores términos. De esta idea se pueden definir formalmente las siguientes expresiones.

La Indexación Semántica Latente (ISL) es un método de indexación y recuperación que utiliza un método numérico llamado Descomposición en Valores Singulares (SVD por sus siglas en inglés) para identificar patrones en las relaciones entre los términos contenidos en una colección de textos no estructurados. La ISL se basa en el principio de que las palabras que se utilizan en el mismo contexto tienden a tener significados similares. La característica fundamental de la ISL es su habilidad para extraer el contenido conceptual de un documento, estableciendo asociaciones entre aquellos términos que ocurran en contextos similares.

La ISL fue patentada en 1988 por Scott Deerwester, Susan Dumais, George Furnas, Richard Harshman, Thomas Landauer, Karen Lochbaum y Lynn Streeter (Turtle, 2002).

La idea principal de un modelo vectorial extendido aplicado al modelo de indexación semántica latente es emparejar por conceptos en lugar de por términos, o sea, un documento podría ser recuperado si comparte conceptos con otro que es relevante para la consulta dada. Esto se consigue mapeando los documentos (vector índice de términos) y los vectores como consultas dentro de un espacio dimensional reducido el

cual está asociado con conceptos, y puede que la recuperación de información en este espacio reducido sea superior a la obtenida en el espacio de términos indexados. Se usa también una forma de análisis denominada Descomposición en Valores Singulares (SVD).

Los documentos se representan como un vector en donde los términos de búsqueda i se indexan en el documento j, donde w representa el peso asociado al término indexado i en el documento j.

$$\vec{d}_j = \sum_{k=1}^{n} w_{i,q}\ \vec{t}_i$$

Las consultas se representan como un vector en donde los términos de búsqueda i se indexan en el documento j, donde w representa el peso asociado al término indexado i en la consulta q.

$$\vec{q} = \sum_{k=1}^{n} w_{i,q}\ \vec{t}_i$$

El ranking que determina cuan relevante es un documento a una consulta q y se determina como la magnitud del coseno del ángulo entre ellos

$$sim(\vec{d}_k, \vec{q}) = \cos(\vec{d}_k, \vec{q}) = \frac{\vec{d}_k * \vec{q}}{\left|\left|\vec{d}_k\right|\right| ||\vec{q}||}$$

Al plantear los documentos en forma matricial se tiene:

$$W = \begin{vmatrix} w_{11} & \dots & w_{1n} \\ . & . & . \\ . & . & . \\ . & . & . \\ w_{m1} & \dots & w_{mm} \end{vmatrix}$$

Donde:

$$D = (\vec{d}_1, \dots, \vec{d}_m)^T$$

$$t = (\vec{t}_1, \dots, \vec{t}_n)^T$$

Si se plantea de igual manera la función de similitud en forma matricial queda de la siguiente forma:

$$WG\vec{q} = S$$

Donde:

$$G = \begin{vmatrix} \vec{t_1} * \vec{t_2} & \dots & \vec{t_1} * \vec{t_n} \\ . & . & . \\ . & . & . \\ . & . & . \\ \vec{t_n} * \vec{t_1} & \dots & \vec{t_n} * \vec{t_n} \end{vmatrix}$$

La representación anterior es una generalización del modelo vectorial clásico, pues este se puede obtener como caso particular haciendo G = I (Matriz Identidad), de lo cual se puede decir que en este caso t es ortogonal.

La correlación de dos términos indexados depende de la cantidad de documentos en los que ellos aparecen juntos. El modelo vectorial generalizado se basa en esta idea para determinar el grado de correlación de dos términos. Se muestra como el producto escalar de los vectores de términos determina el grado de correlación entre estos, demostrando así que la ecuación 5 es la representación correcta del modelo vectorial general, lo que refleja implícitamente la relevancia a la dependencia entre términos.

Se puede suponer entonces que la colección de documentos está representada por un conjunto de vectores binarios, Entonces el k-ésimo documento de la colección se representa como:

$$\vec{d}_k = (\propto_{k1}, \dots, \propto_{k1})$$

Donde $\propto 1=1$ si el K-ésimo documento contiene el término indexado i y $\propto 1=0$ si el K-ésimo documento no contiene el término indexado i.

Para obtener la representación explicita del vector término t1 se suman los vectores que representan a los términos, multiplicándolos por su factor de correlación asociado al término indexado i y se normaliza el vector.

$$\vec{t}_l = \sum_{k=1}^{r} \frac{c_k(t_i)\vec{m}_k}{\sqrt{\sum_{j=1}^{r} C_j(t_i)^2}}$$ ecir que:

Donde:

$$c_k(t_i) = \sum_{a \in I(t_i,k)} \propto_{ai}$$

$$I(t_i, k) = \{a | d_a \in f(m_k) \mathbb{C}\ f(t_i)\}$$

El producto escalar entre dos vectores términos proporciona una medida "normalizada" de la cantidad de documentos en los que ellos aparecen. Representar los documentos como vectores de valores reales lo único que modifica es el factor de correlación asociado a un término indexado, tomando como base la definición general de modelo vectorial tenemos que:

$$c_k(t_i) = \sum_{a \in I(t_i k)} \propto_{ai}$$

Obteniéndose, de manera general, como grado de correlación entre dos términos indexados:

$$\vec{t_1} * \vec{t_2} \; \dot{\iota} \sum_{\forall k \in H_{ij}} \frac{c_k(t_i) * c_k(t_j)}{\sqrt{\sum_{p=1}^{r_i} C_p(t_i)^2 * \sqrt{\sum_{p=1}^{r_j} C_p(t_j)^2}}}$$

En los modelos clásicos de búsqueda básicamente se trata de medir la relevancia de un documento en base al número de concurrencia de las palabras contenidas en dicho documento con las palabras de la consulta. Una deficiencia de esta forma de medir la relevancia es que no se tiene en cuenta el contexto semántico de la palabra, y como consecuencia de esto van a aparecer dos problemas fundamentales en la búsqueda de información con estos métodos, la sinonimia (términos distintos con el mismo significado) y la polisemia (términos iguales con distintos significados).

En los modelos clásicos no se van a tomar como relevantes documentos que contengan términos con el mismo significado que una de las palabras de la consulta este hecho perjudicará el denominado factor de recall, pero sin embargo se devolverán como relevantes documentos que contengan términos iguales a la consulta, aunque tengan distinto significado, este hecho hará que se reduzca la "precisión".

La indexación semántica latente, propone un método para solucionar estos problemas. La idea es pasar de un conjunto de términos a un conjunto de entidades donde podamos sacar la estructura latente en la asociación entre términos y documentos.

Para el análisis de la estructura semántica latente se forma una matriz rectangular de términos por documentos. Se forma una matriz integrada por términos y documentos, donde cada celda de la matriz indica el número de veces que un término aparece en un documento.

Esta matriz rectangular se descompone en el producto de tres matrices por el proceso llamado "descomposición en valores singulares".

$$X = T_0 S_0 D'_0$$

Donde T0 es una matriz ortogonal, S0 es una matriz diagonal y D0' es la traspuesta de la matriz ortogonal D0. Las columnas de T0 son los autovectores de X transpuesta por X y las columnas de D son los autovectores de X por la transpuesta de X y S0 la matriz de valores singulares. T0 representaría el espacio vectorial de los términos y D0 el espacio vectorial de los documentos.

Se ordenan los valores singulares de en S de mayor a menor, se escogen los primeros k valores y el resto se descartan, se tiene entonces una nueva matriz singular S de rango k, además se eliminan las columnas correspondientes de T y D y tenemos T y D respectivamente.

El resultado es una nueva matriz X' de rango menor. Es decir, se ha reducido el modelo a k dimensiones. Cada término y documento va a ser representado ahora por un vector de factores en un espacio de k dimensiones. El valor de k, es decir cuánto reducimos las dimensiones del modelo, es algo que se elige experimentalmente midiendo para cada k elegido la eficacia de recuperación.

$$X' = TSD'$$

Se obtiene una nueva matriz X' a partir de la reducción de los valores singulares de la matriz S de la cual se puede obtener comparaciones

fundamentales para la búsqueda y recuperación de información.

Comparaciones fundamentales del modelo

Comparación de dos términos: El producto escalar entre dos filas de la matriz X' dará la similitud entre dos términos a través de todos los documentos (el producto escalar da la medida del coseno del ángulo). El producto de matriz X' por su traspuesta da la matriz de los productos escalares término a término. Se puede demostrar que este producto es:

$XX' = TS^2T'$ (Chandler, 1977)

Comparación de dos documentos: El producto escalar entre dos columnas de la matriz X' dará la similitud entre dos documentos a través de sus términos. El producto de la transpuesta de la matriz X' por ella misma da la matriz de los productos escalares documento a documento. Se puede demostrar que este producto es:

$X'X = DS^2D$ (Beavers, 2013)

Comparación de un término con un documento: El principal elemento de medida para la comparación entre un término y un documento es el valor de la celda de la matriz X' cada celda de esta matriz relaciona un documento con un término.

Comparación de la consulta (query) con un documento: Para ello se utiliza un pseudo-documento Dq que va a representar a la consulta. Este Dq se calcula de la siguiente manera:

$D_q = X_qTS^{-1}$ (Jurafsky, 2008)

Donde Xq es el vector de términos de la consulta. Este Dq es como si fuera una fila de la matriz D y puede ser usado para comparar con otros documentos con el producto escalar.

Las filas de las matrices reducidas de vectores singulares se toman como coordenadas de los puntos que representan a los documentos y términos en un espacio de dimensión k cuyos ejes están reescalados por cantidades relacionadas con los valores de la diagonal de la matriz S. Los productos escalares (coseno del ángulo) entre los puntos darán las relaciones de similitud entre los distintos puntos. Para la consulta, al ser esta un pseudo-documento estará representada como un nuevo punto del espacio.

El modelo ISL en la actualidad siendo tema de estudio, la "Indexación Semántica" es un nombre para una familia de tecnologías para buscar y organizar colecciones de datos, apoyándose de descomposiciones y modelos matriciales que aumentan de diversas formas su eficacia o eficiencia en cualquier de los casos es preciso mencionar que el ACP aplicado al ISL es solo un modelo vectorial extendido que pretende dar solución no solo a la sinonimia y la polisemia sino a realizar un búsqueda y agrupación por términos reduciendo la dimensionalidad del problema creando un modelo más eficiente en cuanto búsquedas más especializadas en donde la semántica sea un enfoque primordial y este tome en cuenta el contexto de la búsqueda . El fin es encontrar patrones en datos no estructurados (documentos sin descripciones tales como palabras claves o tags especiales) y usar esos patrones para ofrecer una búsqueda más efectiva y servicios de categorización.

CONCLUSIONES

Un modelo vectorial extendido aplicado a la indexación semántica latente resulta una buena aproximación de solución a dos de los principales problemas de las consultas booleanas: la sinonimia y la polisemia.

Se puede utilizar para realizar una categorización automática de los documentos y particionarlos. Dado que es estrictamente matemático, es independiente del lenguaje, por lo tanto, puede extraer el contenido de cualquier documento independientemente del idioma en que está escrito sin estructuras auxiliares como los diccionarios y permite la búsqueda de términos de un idioma en documentos redactados en otro o varios idiomas, devolviendo resultados

conceptualmente similares. Se adapta automáticamente a terminología cambiante y se ha comprobado que es muy tolerante a ruido.

Una de las ventajas del ACP para reducir la dimensionalidad de un grupo de datos, es que retiene aquellas características del conjunto de datos que contribuyen más a su varianza, manteniendo un orden de bajo nivel de los componentes principales e ignorando los de alto nivel. El objetivo es que esos componentes de bajo orden a veces contienen el aspecto "más importante" de esa información.

Maneja efectivamente datos diversos, ambiguos y contradictorios. Mientras menor sea la nueva dimensión mayor será el recobrado e increíblemente un valor en los cientos puede incrementar la precisión. Al igual que el modelo vectorial permite el macheo parcial y el ranking, además tiene en cuenta la dependencia entre términos.

Inicialmente, los mayores problemas de la ISL fueron la escalabilidad y el rendimiento, pues el costo temporal y espacial es relativamente alto con respecto a otras técnicas. Afortunadamente, la existencia en la actualidad de procesadores de alta velocidad y de memoria barata, han disminuido considerablemente esta situación.

También resulta problemático determinar el valor óptimo de la nueva dimensión a utilizar, aunque experimentalmente se ha comprobado la efectividad de los valores propuestos previamente. Funciona mejor en aplicaciones donde haya poco solapamiento entre las consultas y los documentos. No hay formas cómodas de expresar negaciones de términos ni condiciones booleanas.

BIBLIOGRAFÍA

Beavers, Anthony (2013). «Alan Turing: Mathematical Mechanist». En Cooper, S. Barry; van Leeuwen, Jan. Alan Turing: His Work and Impact. Waltham: Elsevier. pp. 481-485.

Chandler, Alfred (1977). The Visible Hand: The Managerial Revolution in American Business. Cambridge, Massachusetts: Belknap Press

D. H. D. Warren. Logic programming and compiler writing. Software, Practice and Experience, 1980, pp.97–125.

Deerwester, S., Dumais, S. T., Furnas, G. W., Landauer, T. K., & Harshman, R. (1990). Indexing by latent semantic analysis. Journal of the American Society for Information Science, 41(6), 391-407

E. Visser. A survey of rewriting strategies in program transformation systems. In Proceedings of the Workshop on Reduction Strategies in Rewriting and Programming (WRS 01) (2001), Utrecht, The Netherlands..

Jurafsky, J. H. Martin. Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition. Published by Pearson Prentice Hall, 2008.

O'Connor, John J.; Robertson, Edmund F. , MacTutor History of Mathematics archive, Universidad de Saint Andrews.

R. Allen and K. Kennedy (2002). Optimizing Compilers for Modern Architectures. Morgan Kaufmann.

R. Vallée-Rai, P. Co, E. Gagnon, L. Hedren, P. Lam, and V. Sundaresan. Soot (1993) – a Java bytecode optimization framework. In Proceedings of the 1999 Conference of the Centre for Advanced Studies on Collaborative Research, pp. 13– 23, Mississauga, Canada, 1999.

TURTLE, H.R. y CROFT, W.B. (1992): "A Comparison of Text Retrieval Models." The Computer Journal , 35, 3, pp. 279-290.

W. Oard. The surprise language exercises (2003). ACM Transactions on Asian Language Information Processing (TALIP) 2, 2,pp. 79-84.

Impreso en
Talleres Gráficos UCA,
en marzo del 2019
San Salvador, El Salvador, C. A