TRABAJOS FINALES DE MAESTRÍA

Propuesta de Mejoras para la Gestión y Obtención de la Información Sensible desde un Organismo de Control en el Ecuador

Propuesta de artículo presentado como requisito parcial para optar al título de:

Magister en Administración de Empresas de Servicios

Por la estudiante:

Patricia Alexandra GUALOTO ALCIVAR

Bajo la dirección de:

Antonio CEVALLOS GAMBOA, MSIG, MAE, PhD

Universidad Espíritu Santo

Facultad de Postgrados

Guayaquil - Ecuador

Mayo del 2018

MDS-OL-2012-2018

Propuesta de mejoras para la gestión y obtención de la información sensible desde un organismo de control en el Ecuador

Analyzing measurement models of perceived service quality used in hospitality industry

Patricia Alexandra GUALOTO ALCIVAR[1]
Antonio CEVALLOS GAMBOA[2]

Resumen

A través del tiempo se ha podido observar la evolución de las empresas en la forma de obtener y entregar información sensible, utilizando la tecnología como principal aliado y como factor estratégico en el liderazgo y crecimiento de la misma. En el presente artículo se revisa como un nuevo proceso automatizado de gestión genera cambios en la forma de obtener información sensible desde un Organismo de Control en el Ecuador hacia una empresa privada de telecomunicaciones en Ecuador, para ello se aplica la metodología de investigación. Para lo cual se realiza un análisis comparativo del modelo manual vs un modelo automatizado a través de la revisión de herramientas utilizadas para el aseguramiento de la información en el proceso de transferencia en este complejo momento de transformación digital a través del uso de internet. Se destaca finalmente la aceptación del cliente con el nuevo modelo de obtener información sensible para los diferentes fines de investigación pudiéndola tener disponible en el momento que es requerida y con autonomía.

Palabras clave:	Sistema de Información, Información Sensible, Organismo de Control, Seguridad.

Abstract

Over time it has been possible to observe the evolution of companies in the form of obtaining and delivering sensitive information, using technology as a main ally and as a strategic factor in the leadership and growth of it. In this article we review how a new automated management process generates changes in the way to obtain sensitive information from a Control Organization in Ecuador to a private telecommunications company in Ecuador, for which the research methodology is applied. For which a comparative analysis of the manual model vs an automated model is carried out through the review of tools used for the assurance of the information in the transfer process in this complex moment of digital transformation through the use of the internet. Finally, the acceptance of the client with the new model of obtaining sensitive information for different research purposes is highlighted. It can be made available at the time it is required and with autonomy.

Key words	Information system, Sensitive Information, Control company, Security
Clasificación JEL JEL Classification	M31

[1] Licenciada en Sistemas de Información, Universidad Espíritu Santo – Ecuador. E-mail pgualoto@uees.edu.ec
[2] PhD (c) en Ciencias de la Dirección, MSIG, MBA, Ingeniero en Sistemas; Profesor Principal; Decano de la Facultad de Ingeniería en Sistemas, Telecomunicaciones y Electrónica en la Universidad Espíritu Santo - Ecuador; email: acevallos@uees.edu.ec

INTRODUCCIÓN

En el Ecuador los Organismos de Control públicos (Ministerio del Interior, Fiscalías y la Policía Nacional), en la actualidad solicitan información confidencial a determinadas empresas privadas con diferentes fines investigativos. Es así que, la información es solicitada a través de un documento digital en ocasiones impreso con la redacción del requerimiento, que es receptado por la empresa privada para revisión de un administrador el cual genera esta información al interno de la empresa y una vez obtenidos los datos se realiza el proceso de envío a través de dispositivos electrónicos, los cuales no podrían tener la seguridad requerida que se necesita para la protección de su contenido, así como los tiempos de entrega podrían afectarse por los varios requerimientos que podría tener de otras instituciones. (Groenow, 2018).

Si bien los avances en la tecnología a nivel mundial han permitido que el Ecuador forme parte de estos cambios que van dándose en otros países, generando conciencia en las empresas ecuatorianas donde la información es de vital importancia y constituye un activo que requiere seguridad, confidencialidad e integridad por lo tanto las Tecnologías de Información y Comunicación [TIC] han permitido que las empresas privadas puedan generar de forma ágil la prestación de la información que no es de acceso público, utilizando herramientas como la firma electrónica, sellado de tiempo y estándares que están definidos para la protección de la información y que son aplicados en automatizaciones creadas para el usuario cliente que le permite agilizar los procesos de investigación y controles pertinentes reduciendo tiempo y costos de operación. (Guano Llumigusín, 2015).

Es así que, con más frecuencia hay más variables a considerar en el control de la transferencia de documentos con información confidencial y sensible; es por ello que debe garantizarse que no haya sido alterada durante el proceso de trasmisión en el entorno tecnológico. Por lo tanto con la evolución de las tecnologías, se han desarrollado varios métodos o formas para poder hacer válido los documentos que se transfieren en la red internet. En el Ecuador el Banco Central [BCE] en su sección *certificación electrónica* a través de la ley de Comercio Electrónico, Firma Electrónica y Mensajes de Datos vigente desde el año 2002 es la que regula la legalidad del documento además de proteger los datos transmitidos permitiendo que el titular de la información autorice su disposición. (Banco Central del Ecuador, 2014).

De acuerdo a los planteamientos analizados el objetivo de este trabajo es revisar el proceso de obtención de información sensible desde su modelo inicial, no automatizado que fue el estímulo para proponer mejoras tecnológicas en la transferencia de información en la red de internet a través de herramientas, métodos y políticas que actualmente existen para protegerla garantizando la integridad, confidencialidad y disponibilidad. Así también se expone la legislación y artículos en Ecuador y en otros países de América Latina referente a los delitos informáticos a través de un comparativo con cada país permitiendo evidenciar la importancia que ha tenido en las últimas décadas poder regular este tipo de delitos hacia la información cuando se usa internet.

Por lo tanto para evidenciar la propuesta o diseño se establecerá en el documento conceptos, comparativo del modelo anterior vs el modelo actual, comentarios de la experiencia de los usuarios, puntos críticos y mejores prácticas que hace que la investigación a realizarse tengan los fundamentos adecuados aplicables al diseño propuesto, que se detallará a continuación en la lectura del documento.

REVISIÓN DE LA LITERATURA

A continuación se presentan las teorías y conceptos que soportan la propuesta de investigación desarrollada en este documento de investigación.

Gestión de la Información.

Según Leal y Linares (2005) en la década de los años 50 la información era considerada como objeto particular de ciertos espacios del conocimiento. Es así que la información tocaba todas las esferas del saber, siendo unas pocas disciplinas las que estudiaban su producción,

comunicación y su difusión. Del antecedente enunciado se define como sistema de Información "al conjunto de elementos integrados e interrelacionados que persiguen el objetivo de capturar, depurar, almacenar, recuperar, actualizar y tratar datos para proporcionar, distribuir y transmitir información en el lugar y momento en el que sea requerido en la organización" (Domínguez, Sixto , Medina, & José, 2002, pág. 219).

Así para Bustelo-Ruesta (2011) en publicación de tecnología menciona a la gestión de información como creada y recibida por una organización en el transcurso de sus actividades y el desarrollo de sus funciones, además la autora hace una importante aclaración sobre los documentos electrónicos entendiéndose como archivos en varios formatos que contienen información a los que se denomina metadatos convirtiéndose en una verdadera gestión documental que con el rápido crecimiento de la información las organizaciones han considerado importante la implementación de sistemas para la gestión documental. Es así que, para Izquierdo-Campoverde (2015) hace referencia que en las normas ISO 30301 esta expresado como las organizaciones deben implementar los procesos de gestión documental, a través del uso de un software informático que les permitirá aplicar los controles adecuados tanto a los documentos físicos como digitales.

Considerando que la información trasmitida tiene en su contenido datos sensibles que la Universidad el Bosque (2008) la define como la "denominación que se usa preferentemente en el ámbito del derecho jurídico y tiene que ver con los datos que afectan a lo más propio de la persona, podríamos decir a su intimidad" (pág. 25). Por lo tanto los datos sensibles pueden ser entregados por la misma persona o por quien esté autorizado, es así que quienes reciben los datos sensibles están obligados a manejar con carácter de confidencialidad, mostrando una actitud de respecto a lo que es entregado. Los datos sensibles forman parte de información generada que será utilizada dependiendo el requerimiento donde podría existir información privada y pública según lo expresado en revista de la Universidad el Bosque, 2008.

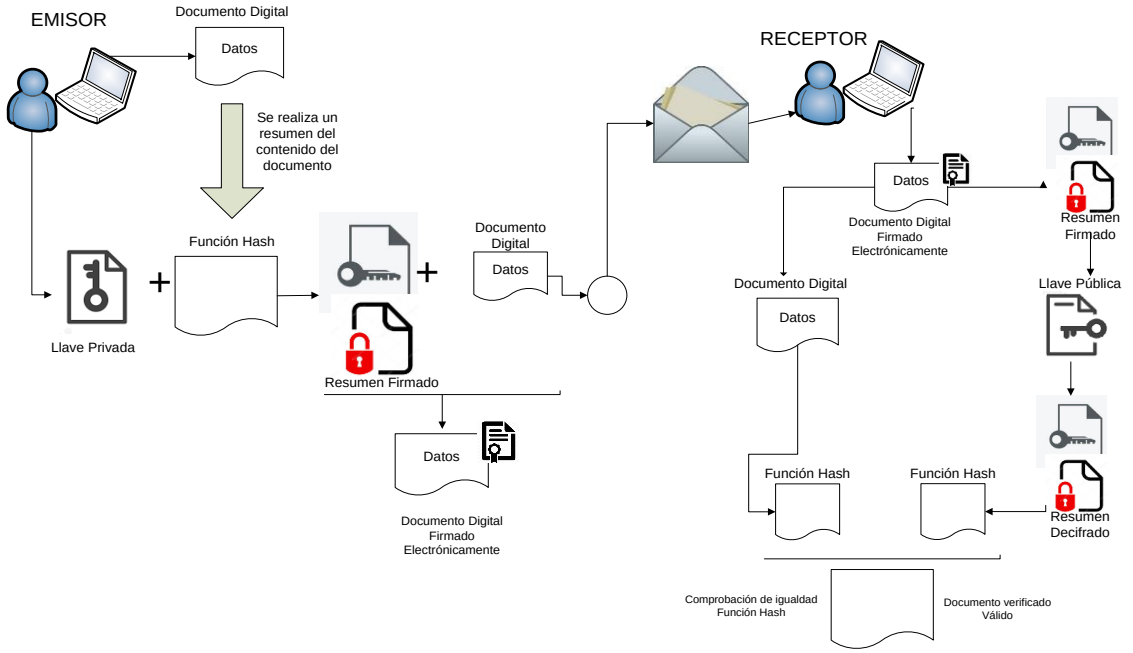
Según Tejerina (2014) la tecnología de hoy permite almacenar grandes cantidades de datos sobre una persona y con la evolución de las comunicaciones permite enviarla en cuestión de segundos de un lugar a otro del mundo, estos datos pueden ser utilizados con finalidades no siempre conocidas, ni mucho menos lícitas lo que significa que cualquiera puede tener información (privada o no) de una persona, y utilizarla para invadir su intimidad o coartar cualquiera otra de sus libertades, por tal motivo la importancia de herramientas, métodos y procesos que protejan la información en el momento que es transferida y así poder garantizar que llegue sin ser alterada. Para el aseguramiento de documentos con información sensible se han desarrollado varios métodos o formas para poder hacerlos válidos en el momento que son transferidos en la red a través de internet, como la firma electrónica que tiene igual validez que una firma manuscrita.

Firma Electrónica

La firma electrónica es definida según López (2003) como "una técnica para verificar que un documento ha sido realizado por el poseedor de determinado algoritmo, lo que se conoce como llave privada" (pág. 43), en consecuencia es uno de los varios métodos para evitar los delitos informáticos que no solo causan perdidas económicas sino va más allá que una usurpación de la identidad3. En Figura 1 se observa como a partir del emisor se genera el documento que va enviarse y sus diferentes partes del proceso para poder aplicar la firma electrónica, el documento es enviado al receptor el cual debe descifrar el documento utilizando una llave pública para que pueda ser visualizado el documento.

[3] Usurpación de la Identidad: modalidad mediante la cual alguien suplanta a alguna otra persona en la titularidad de un derecho o una pretensión para obtener un bien o una prestación. (Gabaldón & Pereira, 2008, pág. 3)

Figura 1. Esquema Firma Electrónica



Fuente: (Ayala Bolaños, 2012, pág. 9)

Pinela (2013, pág. 27) cita a Skoog (2008) quien indica que "La firma electrónica es un medio único, que no está escrito a mano, que sirve para identificar a una persona y que nadie más puede usarla" siendo la firma electrónica contenedora de una amplia gama de metodologías y tecnologías, que permite utilizar procesos internos de una empresa como la aprobación de solicitudes, documentación formal, firmas de documentos críticos incluyendo temas jurídicos hasta transacciones comerciales. Del mismo modo para Fernández y De Castro (2015) en artículo Documento Electrónico y Firma Electrónica menciona a la firma electrónica como datos en formato electrónico que están anexados al documento o incorporados de forma lógica a él, siendo usado como medio de identificación; y destaca a la firma electrónica como una herramienta que otorga agilidad y que en la actualidad las diferentes empresas la utilizan para poder interactuar con organismos públicos en procesos de envío y recepción de datos lo cual hace que se optimice el tiempo y se mejore la calidad del servicio que se está entregando al cliente.

De ahí que, en el Ecuador la Ley de Comercio Electrónico, Firma Electrónica y Mensaje de datos en artículo 13 define a la firma electrónica como:

> **Datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo y que pueden ser utilizados para identificar al titular de la firma en relación con el mensaje de datos e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos** (Lizano Martínez, Madril Romero , & Villao Quezada , 2014, pág. 2).

Es por tal motivo que para hacer uso de la firma electrónica se requiere de manera previa haber gestionado el certificado de firma electrónica el mismo que es emitido por una Autoridad Certificadora [AC], que es la responsable de garantizar la identidad de la persona quien está realizando la gestión, como también la integridad del contenido de lo que se está enviando que puede ser cualquier documento de diferente formato que necesita tenga validez de una firma manuscrita la que será reemplazada por la firma electrónica. En consecuencia, un Certificado Digital "es un documento digital mediante el cual la AC asegura la vinculación entre la identidad del usuario, su clave pública, y privada" (Banco Central del Ecuador, 2009, p. 4). Es por tal motivo que es necesaria la existencia de una entidad u organismo que brinde esta certificación permitiendo el reconocimiento de los miembros que participan entre las organizaciones es así donde se crean las

AC. Así la Ley de Comercio Electrónico (Art. 29) define a las AC como:

> **Empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República.** (pág. 6)

En el Ecuador las AC de acuerdo a página oficial publicada (ARCOTEL, 2017) como listado de las Entidades de Certificación de Información y Servicios Relacionados Acreditados y Terceros Vinculados, debidamente acreditadas son:

Tabla 1: Listado de Entidades de Certificación en el Ecuador

1	BANCO CENTRAL DEL ECUADOR
2	SECURITY DATA SEGURIDAD EN DATOS Y FIRMA DIGITAL S.A.
3	CONSEJO DE LA JUDICATURA
4	ANFAC AUTORIDAD DE CERTIFICACIÓN ECUADOR C.A.

Publicación ARCOTEL

Siendo a partir de octubre del 2008 que se acredita al BCE como la primera autoridad de certificación haciendo de la firma electrónica de igual validez que una firma manuscrita con un rol importante en la falta de seguridad que existe en las transacciones realizadas en Internet, al utilizarla permite garantizar la integridad del mensaje, su reconocimiento y autenticidad es decir que a través de la Firma Electrónica se asegura la identidad del remitente del mensaje, generando la confianza y validez legal en la información recibida en el documento.

Sin embargo la firma electrónica no tiene la característica de indicar cuando se ha firmado el documento electrónico, siendo de importancia para ciertos tipos de documentos donde la fecha y hora es un dato esencial, de tal forma el sellado de tiempo se convierte en un ideal complemento para la firma electrónica, siendo un tercero el que asegura que los datos contenidos en el documento existen desde una fecha establecida. (Madril Romero & Lizano Martínez, 2014)

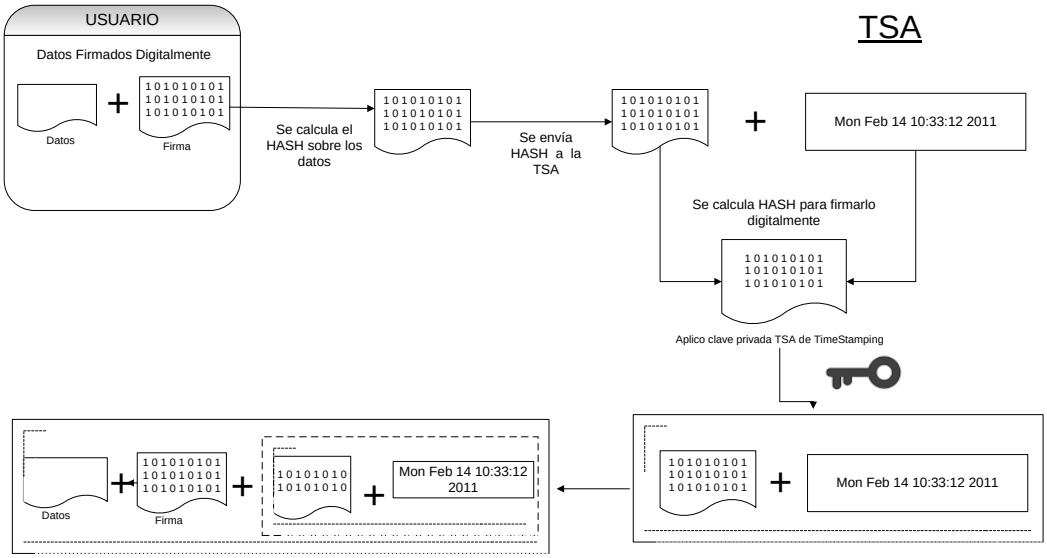
Sellado de Tiempo

Si bien la firma electrónica garantiza la validez del documento por parte del dueño o emisor tiene la debilidad o falencia del instante de tiempo en que fue realizada la transacción, por tal motivo existen métodos como el sellado de tiempo implementados para garantizar la transacción que se emite del emisor y que durante su trayectoria la validez sea aprobada sin alteración alguna. Por tal motivo Rojas (2008) define al sellado de tiempo como:

> **Un mecanismo en línea que permite demostrar que una serie de datos han existido y siguen existiendo y que no han sido alterados desde el instante específico en el tiempo, que es precisamente el que indica el sello. Una autoridad de Sellado de Tiempo actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos desde una fecha y hora concretos**. (p. 13)

Según Sánchez (2016), el sellado de tiempo es una forma de evidenciar que un conjunto de datos tuvieron una forma antes y que ninguno de estos ha sido modificado con el transcurrir del tiempo. Por lo tanto, para la gestión de ciertos documentos como contratos, documentos jurídicos y otros utilizando la red internet es de importancia tener el conocimiento y el tiempo en el que son realizados, siendo necesario solicitar a un tercero con credibilidad y confianza la constancia de la fecha y hora que es fundamental para garantizar el origen y la integridad de la información trasmitida; es así que, como parte de las características del sellado de tiempo llamado Services Time Stamping por sus siglas en inglés se basa en los mecanismos de firma electrónica y a menudo es un servicio adicional que es prestado por las autoridades de certificación. La tercera parte de confianza es aceptada por el emisor y también por el receptor que da la fe de fecha y hora de una transacción, con esto se enfatiza que las partes o actores del proceso aceptan a una tercera parte de confianza de fecha y hora de una transacción añadiendo el dato "tiempo" (Diaz, Macía, Molinari, Venosa, & Sabolansky, 2010) .

Figura2. Proceso de Firmado con Sellado de Tiempo



Fuente: (Paulin, Robledo, & Brusa, 2014, pág. 9)

Del mismo modo, en Figura 2 se esquematiza el proceso de firmado con sellado de tiempo con cada uno de sus pasos que para Diaz, Macía, Molinari, Venosa, y Sabolansky (2010) en el proceso de sellado de tiempo intervienen las entidades como el solicitante que es la entidad que tiene la información que a través de un documento o correo electrónico requiere se incluya el sello de tiempo, continua el verificador entidad que valida o comprueba que los datos sellados recibidos contengan un sello de tiempo válido y correcto, por último la autoridad de sellado de tiempo entidad que es el proveedor del servicio que tiene la finalidad de comprobación de los datos a sellar y generar el sello de tiempo que irá unido a los datos asegurando que existan en el instante de tiempo en que fueron generados, encontrando como principal ventaja la unión de la firma electrónica con el sellado de tiempo el agregar seguridad a las transacciones que permitan protegerla de las varias amenazas, llamadas con diferentes denominaciones tales como “delitos informáticos”, “delitos relacionados con la computadora”, “delitos electrónicos”. (Levene & Chiaravalloti, 1998)

Delitos Informáticos

Con la aparición de las tecnologías y la necesidad del ser humano de poder trasmitir y manejar la información, han salido nuevas formas en las que se puede delinquir lo que ha generado variedad de delitos llamados informáticos. En consecuencia los métodos de firma electrónica avanzada y sellado de tiempo son algunos de los varios que permiten al usuario proteger la información trasmitida a través de la red; siendo cada uno importante para así poder disuadir este tipo de delito.

Para Levene y Chiaravalloti (1998) definen al delito informático como:

> **Todas aquellas conductas ilícitas sancionadas por el ordenamiento jurídico objetivo, donde se hace uso indebido de los sistemas de informática como medio o instrumento para la comisión de un delito, y así mismo aquellas otras conductas que van dirigidas en contra de la información automatizada convirtiendo a está en su fin u objetivo** (p. 4)**.**

Sin embargo para Cuenca Espinosa (2012) en su definición personal lo cataloga como:

> **Toda actividad en la cual se utilizan medios computacionales, telemáticos o electrónicos para el cometimiento de un delito; delitos que constituyen nuevas formas penales que incluyen como elementos primogénitos al internet como instrumento abstracto y a la computadora como instrumento físico** (pág. 3)**.**

Es así que organismos internacionales como la Organización de Naciones Unidas [ONU] realizan recomendaciones para que sean aplicadas en cada legislación de los

países, por esta razón en el décimo tercer Congreso sobre Prevención del Delito y Justicia Penal, hace mención al término ciberdelincuencia dándole la definición académica como "conjunto de hechos cometidos en contra o a través del uso de datos o sistemas informáticos". (Naciones Unidas, 2015); es así que al mismo tiempo indica como de manera efectiva la ciberdelincuencia utiliza las tecnologías globalizadas de la información y las comunicaciones de forma específica a través de internet para efectivizar actos delictivos de un alcance transnacional.

En el Ecuador los delitos informáticos se encuentran tipificados en la legislación ecuatoriana en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos [LCEFEMD] conocida como Ley 67 en Sup.557 de Abril del 2002, donde se incluye un importante avance en la inclusión de penalidades a los ilícitos informáticos, con lo cual junto al Código Penal se integran normas para ser aplicadas en la Sociedad de la Información. (Ley de Comercio Electrónico, firmas electrónicas y mensajes escritos, 2002)

Algunos casos conocidos e importantes en Ecuador son detallados en publicación referente al delito informático en el Ecuador, y como se ha convertido en una nueva tendencia criminal del nuevo siglo XXI; delitos como el caso Emetel 1996 - redondeo de cantidades, Phishing Banco del Pichincha entre los años 2009 al 2012 - trasferencias electrónicas sin autorización y Carding a Bancos ecuatorianos entre los años 2010 al 2011 – uso ilegal de tarjetas de crédito. (Cuenca Espinosa, 2012)

Entonces resulta que, para Ferruzola Gomez y Cuenca Espinoza (2014) en su publicación "cómo responder a un delito informático" en la LCEDMD los delitos informáticos incluidos al Código Penal están tipificados en: incumplimiento a los delitos contra la información protegida Art.57 (Art.202.1), obtención y utilización no autorizada de información Art. 58 (Art. 202.2), destrucción maliciosa de documentos Art. 59 (Art. 262), falsificación electrónica Art. 60 (Art. 353.1), daños informáticos Art. 61 (Art. 415.1), apropiación ilícita Art.62 (Art. 553.1), para concluir con la violación del derecho a la intimidad según los establecido en la Ley 67 Art. 64 (Art. 606 Inc.20).

Por lo tanto, para Criado y Rojas Martín (2013) para poder disminuir los riesgos de ataques informáticos, como son las fugas de información, publicación de información confidencial o sensible, robo de datos y cualquier otro tipo de delito informático, es indispensable garantizar la seguridad tecnológica donde se aloja la información y así poder minimizar estos riesgos, con el uso de métodos que permitan protegerla durante el proceso de transferencia.

Por esta razón el profesor Phill Williams[4] manifiesta la necesidad e importancia de no solo tener leyes e instrumentos compatibles y tambien eficaces que permitan una cooperación idónea para poder luchar contra la delincuencia informática, sino que también resalta como la infraestructura técnica como la de un recurso humano calificado permita hacerle frente a estos nuevos tipos de delitos transnacionales. (Acurio del Pino, SF)

Entidades de Control

Es definido como un organismo de control para (Aguilar A., 2007), cuando se refiere a una específica clase de control el que puede ser llamado control gubernamental y cita a Luis Hidalgo López refiriéndose "a la administración de recursos financieros ajenos de propiedad colectiva por parte de los empleados públicos con destino a la obtención de fines predeterminados la hacienda pública y su control global". En la Constitución Política de la República del Ecuador de acuerdo a lo citado por (Aguilar A., 2007) en Título X denomina a los organismos de control a: la Contraloría General del Estado, la Procuraduría General del Estado, el Ministerio Público, la Comisión de Control Cívico de la Corrupción y las superintendencias que ejercen diferentes actividades de control gubernamental con responsabilidades y atribuciones como entes de control. Es así que, el trabajo de investigación se enfoca a entes de control como el Ministerio del Interior, Fiscalías y la Policía Nacional. De modo que para el Ministerio del Interior del Ecuador (2018) en la sección objetivos indica que su objetivo es "el garantizar el

[4] Profesor de Estudios de Seguridad Internacional, Universidad de Pittsbugh

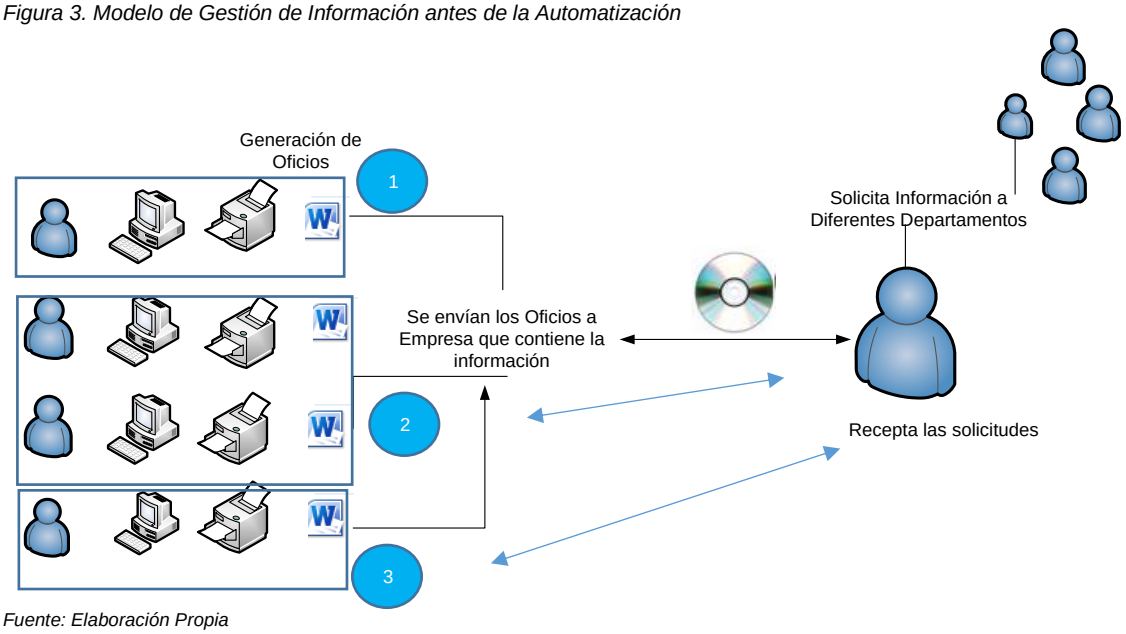
derecho de las personas a ser y sentirse protegidos de la violencia y cometimiento de delitos y contravenciones"; en consecuencia, la Policía Nacional tiene como su misión: "atender la seguridad ciudadana y el orden público, proteger el libre ejercicio de los derechos y la seguridad de las personas dentro del territorio nacional" (Policía Nacional del Ecuador, 2018).

Con la revisión de los diferentes conceptos y métodos que existen para asegurar la trasmisión de información en la red internet, es de vital importancia la aplicación de estos en la propuesta que a continuación se detallará, que permitan a las entidades de control poder realizar las solicitudes de información con la tranquilidad, confianza que la empresa privada le brinde en estos sistemas web llamado sistema de información para poder utilizarlos de acuerdo a la necesidad del caso a investigarse.

PROPUESTA DE MEJORA.

Modelo de Gestión de Información antes de la Automatización.

Figura 3. Modelo de Gestión de Información antes de la Automatización



Fuente: Elaboración Propia

En entrevista realizada a usuario (Groenow, 2018) quien administra el proceso de solicitar información sensible a través de requerimientos, menciona que se utilizaban documentos físicos que eran enviados hacia la empresa privada dueña y custodia de la información, la que era generada utilizando un sistema de información local instalado en la empresa privada; que en cierta medida dependiendo de la región las solicitudes eran atendidas en la costa o sierra a través de la persona autorizada en cada región. Por lo general las solicitudes con los requerimientos en su mayoría era algo simple, pero si se requiere de algo más elaborado necesitaba fuera llenado por los custodios de la información respectiva dentro de la empresa. Una vez generada la información se documentaba a nivel de Excel la información para completarla con lo solicitado y se envía a través del Courier con la respectiva carta de soporte hacia el solicitante. Los clientes Fiscalías y Juzgados emitían el requerimiento hacia la empresa privada la operadora con un tiempo de atención que no podía ser mayor a 72 horas.

La mayoría de los problemas estaban relacionados cuando el sistema tenía inconvenientes afectaciones y por ser el único de donde se extraía la información para entregarse existían demoras. Además del riesgo generado con el uso del medio donde se enviaba la información que pudiera ser modificada o dañada por tratarse de dispositivos como CDs y papel que podrían tener algún tratamiento una

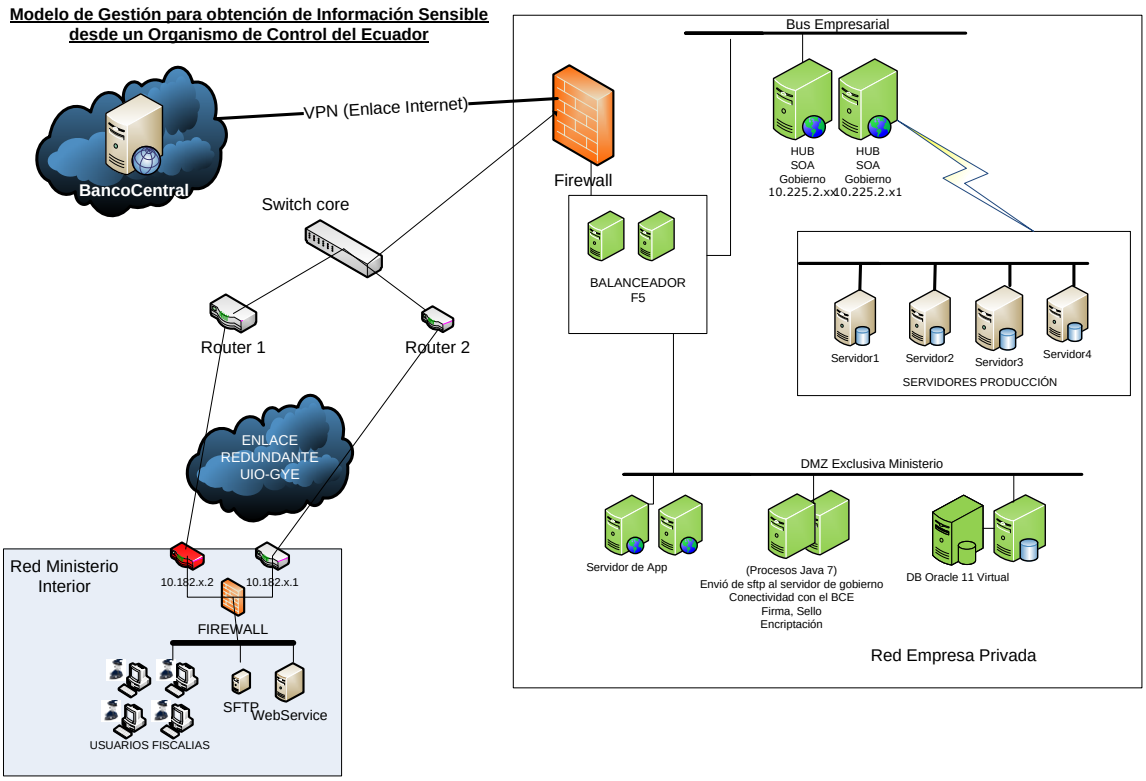
vez que este fuera de la empresa privada por no tener las seguridades necesarias en la transferencia de la información.

Actualmente, el Ministerio del Interior se encuentra ubicado en la ciudad de Quito para la atención de las diferentes solicitudes para las cuales esta creado, físicamente cuenta con una sala de policías los cuales como parte de sus funciones esta la atención de los requerimientos de información confidencial solicitada por las fiscalías para atender temas de investigación por casos de secuestros o investigación a realizarse por diferentes delitos que atentan a la seguridad del ciudadano.

Propuesta de Modelo de Gestión en la obtención de información sensible desde un Organismo de Control hacia la empresa privada.

La iniciativa de la automatización surge del requerimiento del Ministerio del Interior hacia las Fiscalías y ellas hacia las empresas privadas de Telecomunicaciones, para que sea implementado un sistema de información a través del cual pueda obtenerse la información de manera autónoma, lo cual permitirá dar mayor atención a los requerimientos de casos de secuestros y delincuencia. La implementación del nuevo sistema generó una disminución notable de oficios que llegaban a la operadora, dado que cada solicitud era elaborada por la fiscalía a nivel nacional y esta llegaba al Ministerio del Interior para que pueda ser gestionada de manera autónoma utilizando el sistema el que podía ser utilizado las 24 horas del día.

Figura 4. Propuesta de Modelo de Gestión en la Obtención de Información



Fuente: Elaboración Propia

La automatización generó grandes cambios tanto a nivel de infraestructura como en la forma de obtener la información, utilizando un sistema Web con el cual son ingresados los requerimientos y son censados por un proceso de despacho de solicitudes para la atención correspondiente.

A continuación se visualiza en un cuadro comparativo las diferencias entre el modelo manual y el modelo automatizado.

Tabla 2: *Diagrama Funcional - Comparar implementación con la infraestructura actual.*

PROCESO ANTERIOR – NO AUTOMATIZADO	PROCESO ACTUAL – AUTOMATIZADO
Solicitud de información mediante oficio	Ingreso de solicitud en sistema
Envío de solicitud, por valija, a entidad que proporcionará información	La solicitud ingresada llega de forma inmediata a la entidad privada para ser procesada de acuerdo al requerimiento
Espera de la información solicitada conforme a los acuerdos establecidos de entrega dependiendo el tipo de solicitud.	Alta disponibilidad de acceso al sistema - Generación inmediata de la información con tiempos de respuesta acordados dependiendo el tipo de solicitud.
	Seguridad - Generado el archivo este es firmado y sellado por el BCE previo a enviarlo al solicitante
Una vez lista la información la entrega de la misma es a través de dispositivos externos poco seguros	Alta disponibilidad de acceso a datos - El archivo está listo para ser enviado con la seguridad respectiva y es enviado al solicitante.
Espera en la llegada de la información	La información llega de manera automática y segura

Fuente: Elaboración Propia

Actualmente se mantiene la atención de requerimientos de forma manual aunque son en menos proporción que son recibidos de las unidades judiciales o juzgados los que son enviados directamente a la empresa de telecomunicaciones.

Seguridad en la Transmisión de la Información

Como parte del aseguramiento y privacidad en la transmisión de la información ante las vulnerabilidades actuales que existen, son utilizadas herramientas como Firewall, un Balanceador llamado F5, Sistema de Prevención de Intrusos con su traducción en inglés Intrusion Prevention System [IPS] y Web Application Firewall [WAF], así como los servicios de firma electrónica y sellado de tiempo que son contratados al BCE para ser aplicados en los documentos a transferirse garantizando con ello la confidencialidad, integridad, disponibilidad y no repudio de la información enviada en la transacción de requerimiento de información sensible y que será utilizado por el Ministerio del Interior con propósitos de investigación.

Para el aseguramiento de la confidencialidad de los accesos que vienen desde el Ministerio del Interior hacia la empresa privada de Telecomunicaciones es necesario establecer como primer punto de seguridad una conexión Firewall to Firewall, lo que significa que ambas empresas tengan un Firewall de tipo empresarial para protección de datos, permitiendo levantar un túnel seguro que es por donde viaja la información. De ahí que la conexión se establece en un puerto TCP definido previamente, bloqueando cualquier otra conexión que no se haya configurado permitiendo tener la seguridad que los datos solo viajarán por dicho puerto.

Del mismo modo para asegurar la integridad y no repudio de la información participan activamente un IPS y/o WAF, los mismos que se encargan de realizar un análisis de manera más “inteligente” ya que se basan en la inspección de código que viaja en la conexión, mediante algoritmos pre-establecidos que podrían detectar algún código maligno embebido en el paquete de datos la que es realizad a bajo nivel. Estas conexiones cuando son constantes y fluidas los IPS o WAFs aprenden este comportamiento y lo cataloga como una conexión confiable. Las conexiones del Ministerio del Interior siempre ingresan por una misma dirección IP que en la lógica de programación del sistema tienen definidas las consultas hacia objetos de las diferentes bases de datos para la extracción de la información, si en algún momento algún elemento de estos cambia por ejemplo consultas queriendo alcanzar otras tablas utilizando una nueva IPS de origen el equipo de seguridad detecta la anomalía y puede llegar a tratar esta conexión como no confiable. El no repudio es asegurado a través del uso de bitácora de acceso, donde se almacena la IP, fecha/hora y el usuario que ingreso al sistema de información a través del aplicativo para la obtención de la información.

Con referencia a la disponibilidad se utilizan herramientas de balanceo de carga de información utilizando el F5 que permite aliviar la carga de trabajo de

servidores, como equipos en modo clúster que permiten trabajar con varios firewall u otro equipo de seguridad presentándose con una única IP lo que facilita el acceso a los aplicativos en lugar de apuntar a varias direcciones. Además es considerado el tipo de conexión eléctrica con una infraestructura que tiene fuentes eléctricas redundantes y que a su vez están conectadas en una solución de UPS que permita varias horas de trabajo en caso de un desastre técnico.

Además se tiene en cuenta la importancia de tener contingencia como medida preventiva, para tal motivo se implementa el proceso de respaldos válidos y actualizados, lo cual se logra con procesos backup que involucra la participación una persona para la selección de la información que se considere prioritaria utilizando como herramientas de respaldo cintas magnéticas; como buena práctica aplicada se somete a los sitios publicados detrás de un firewall y/o equipos de seguridad a un Ethical Hacking5 el cual mediante pruebas de acceso intenta identificar riesgos asociados a servicios de la empresa desde una visión interna y externa a la compañía.

Además en la investigación realizada se detectan algunos riesgos o puntos críticos dentro del proceso los cuales a continuación se detalla cómo fueron mitigados de acuerdo a su urgencia y necesidad del proyecto.

PUNTOS CRÍTICOS

En el desarrollo del nuevo modelo de gestión para la obtención de información desde un organismo de control hubieron diferentes momentos donde se identificaron puntos de mejoras a las debilidades que se fueron evidenciando los que son llamados puntos críticos, a continuación se detallan los relevantes y su correspondiente proceso de mitigación.

1. Servicio de Entidad Certificadora caído no pueden firmarse ni sellarse los archivos.

Para la atención (24/7) del sistema que provee la información al Organismo de Control como parte del proceso se encuentra la Entidad Certificadora quien da el servicio de sellado y firma el cual es de indispensable necesidad previo a enviar el archivo con la información solicitada, por tal el BCE ha implementado un equipo de redundancia y balanceo para poder atender este tipo de riesgo.

2. Solicitudes no procesadas por tablespace.

Se desarrollan controles a nivel de la BD con apoyo del equipo técnico implementando notificaciones configuradas a un umbral establecido para que pueda mitigarse la falta de espacio en tablespace, evitando que las solicitudes no se procesen por falta de espacio en la base de datos que es donde se genera la información previa a ser cargada en los archivos que posteriormente serán enviados al Ministerio del Interior.

DISCUSION

En exposición del nuevo modelo automatizado se pueden evidenciar varias de las ventajas con las que actualmente usa el Ministerio del Interior, destacando una de las principales como los es la disponibilidad considerada principal ventaja en este nuevo modelo automatizado que les permite realizar acceso a los datos a través del sistema de información con el ingreso de solicitudes, que si bien es cierto en el modelo manual eran entregado en el mismo tiempo de atención la percepción del cliente solicitante es satisfactoria al utilizar un aplicativo instalado en sitio para realizar los requerimientos de acuerdo a la demanda que exista por los casos de investigación.

Además es importante destacar la seguridad aplicada en la comunicación y transferencia de información a través de internet, donde de acuerdo a lo explicado en redacción del documento inicia con una infraestructura que es el primer vínculo para poder conectarse así también la aplicación de otros controles para que el documento con la información viaje seguro desde su emisor hasta el receptor como lo son la aplicación de la firma electrónica y el sellado de tiempo, permitiendo que se mantenga la confidencialidad y la no alteración de los datos garantizando el no repudio.

[5] Proceso por el cual se utilizan las mismas técnicas y herramientas que un black hat para atacar a una organización y descubrir las vulnerabilidades de la misma.

Es factible considerar el nuevo modelo de gestión de la información para obtener información sensible para que pueda ser aplicado a otros organismos de control que pudieran requerir el mismo tipo de información o de no ser así poder implementar nuevas solicitudes con información pero ya con una base establecida de seguridades a nivel de la infraestructura y controles correspondientes para el aseguramiento de la información que es trasmitida desde la empresa de telecomunicaciones dueña de la información hasta el ente de control que está solicitando dicha información con carácter de confidencialidad.

CONCLUSIONES

La evolución de la tecnología y aplicación de las TIC han permitido poder gestionar de manera segura y en tiempos cortos la obtención de información sensible para fines de investigación desde un organismo de control en el Ecuador a una empresa privada de telecomunicaciones en el Ecuador. Es así que el artículo realiza una revisión a través de investigación de la evoluciòn del proceso manual a un proceso automatizado en la obtención de información permitiendo al cliente dar autonomía en la realización de sus actividades diarias en el ingreso de solicitudes para la obtención de información sensible.

Como resultado se evidencia principalmente la satisfacción del cliente al realizar el ingreso de la solicitud sin el uso de papel como medio para detallar la solicitud de informaciòn, sino mas bien el requerimiento de informaciòn sensible es ingresado en un sistema de información instalado en sitio con resultados en tiempos cortos, disponible 24/7 para ser usado de manera autónoma por el personal, para que de esta forma puedan generar la información que requieran para cada caso de investigación. La disponibilidad genera confianza y credibilidad del cliente al momento de solicitar la información.

Se destacan principales beneficios entre el método manual vs el método automatizado que a través de la investigación se propone y expone las mejores prácticas en infraestructura que permiten que el nuevo modelo se diferencie del anterior destacando la seguridad aplicada a través de la firma electrónica y el sellado de tiempo en los documentos que se transfieren así como herramientas para proteger la información de ataque de intrusos cuando está siendo trasmitida a través de internet con infraestructura que la proteja dentro de un túnel seguro con una conexión firewall to firewall, WAF y asegurando la disponibilidad de la atención de los requerimientos mediante un balanceo de las solicitudes que permitan ser atendidas ágilmente y de forma segura.

Con la ayuda de la literatura son revisados algunos conceptos necesarios para poder exponer las herramientas que fueron aplicadas en el modelo automatizado lo que garantiza que la información sea transferida de forma segura, siendo muy importante fomentar una cultura en seguridad.

En la investigación realizada se destaca como algunos países de América Latina ya tienen implementadas regulaciones para los varios delitos informáticos ver anexo 1 y 2, y como cada vez, con el transcurrir del tiempo, es importante y es de vital importancia considerar la información como un activo intangible pero de gran importancia en cada una de las empresas.

El siguiente artículo da como pauta el poder realizar un análisis de factibilidad en aplicar este modelo automatizado en otras empresas privadas que no sean de telecomunicaciones en la forma de entregar información sensible a entidades de control en el Ecuador con las herramientas e infraestructura que se detallaron en la redacción del texto.

Bibliografía

Acurio del Pino, S. (SF, SF SF). El Delito Informático y su realidad procesal en el Ecuador. *Delitos Informáticos Generalidades*.

Aguilar A., J. (2007). Compromiso Político y organismos de control. *Revista de Derecho, No 7. UASB-Ecuador / CEN Quito, 2007*, 14.

ARCOTEL. (2017, 06 01). Retrieved from Listado de las Entidades de Certificación de Información y Servicios Relacionados Acreditados y Terceros Vinculados, debidamente acreditadas: http://www.arcotel.gob.ec/listado-de-las-entidades-de-certificacion-de-informacion-y-servicios-relacionados-acreditados-y-terceros-vinculados-debidamente-acreditadas/

Astudillo, K., & Palomeque Avila , J. G. (2015, 09 22). *Implementación de certificados y firmas digitales para sistemas de información transaccionales en una empresa gubernamental.* Retrieved from http://www.dspace.espol.edu.ec/xmlui/handle/123456789/30019

Ayala Bolaños, G. (2012, 09 27). La Firma Electrónica e-commerce. Retrieved from https://es.slideshare.net/gabriel21472/la-firma-electrnica-14490617

Banco Central del Ecuador. (2009, 06 SF). DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN Y POLÍTICAS DE CERTIFICADOS DE LA ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN DEL BANCO CENTRAL DEL ECUADOR. Retrieved from http://www.bce.fin.ec/documentos/ServiciosBCentral/SistemaPagos/ManualUsuarioPKI-MP031.pdf

Banco Central del Ecuador. (2014, 02 10). Certificación Electrónica. Retrieved from https://es.wikipedia.org/wiki/Firma_electr%C3%B3nica

Bustelo-Ruesta, C. (2011). Los grandes temas relacionados con la gestión de documentos: desafíos y oportunidades. Marzo-abril.

Chiriboga, G. R. (2014, Agosto). *repositorio.espe.edu.ec.* Retrieved from El Impacto Social y la incidencia que tiene el uso de la firma electrónica (token), en los pequeños y medianos exportadores ecuatorianos: http://repositorio.espe.edu.ec/bitstream/21000/9529/2/T-ESPE-HC-002409.pdf

Criado, J., & Rojas Martín, F. (2013). Las redes sociales digitales en la gestión y las políticas públicas. Avances y desafíos para un gobierno abierto. Barcelona. doi:10.2436/10.8030.05.1

Cuenca Espinosa, A. (2012). EL DELITO INFORMÁTICO EN EL ECUADOR "UNA NUEVA TENDENCIA CRIMINAL DEL SIGLO XXI" SU EVOLUCIÓN, PUNIBILIDAD Y PROCESO PENAL. Quito, Ecuador.

Diaz, F. J., Macía, N., Molinari, L., Venosa, P., & Sabolansky, A. J. (2010, mayo s.f). *Repositorio Institucional de la UNLP.* Retrieved from Importancia de contar con un servicio de sellado digital de tiempo en una PKI: http://hdl.handle.net/10915/19430

Diaz, J. L. (2010). *Universidad del Azuay - Facultad de Ciencias Jurídicas* . Retrieved from Los Mensajes de Datos, la firma electrónica y los certificados de firma electrónica dentro del ordenaminto jurídico ecuatoriano: Pendiente

Diaz, J., Macías , N., Molinari, L., Venosa, P., & Sabolansky, A. (2012, 08 10). *Repositorio Institucional de la UNLP.* Retrieved from Repositorio Institucional de la UNLP: http://hdl.handle.net/10915/19430

Domínguez, A., Sixto , J., Medina, G., & José, A. (2002). La Gestión de los sistemas de información en la empresa. In A. Domínguez, J. Sixto, G. Medina, & A. José, *La Gestión de los sistemas de información en la empresa* (Ediciones Pirámides ed., p. 219). Madrid.

Entidad de Certificación del Consejo de la Judicatura. (2016, 08 09). *POLÍTICA DE CERTIFICADOS.* Retrieved from https://www.icert.fje.gob.ec/dpc/empresa_institucion.pdf

Fernández, G., & De Castro, M. (2015). El documento electrónico y la firma electrónica.

Ferruzola Gomez, E. C., & Cuenca Espinoza, H. A. (2014, 06). CÓMO RESPONDER A UN DELITO INFORMÁTICO. Retrieved from http://repositorio.unemi.edu.ec/handle/123456789/3036

Gabaldón, L., & Pereira, W. (2008, julio - diciembre). Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico.

Garcia, C. P. (2009, 03). *Universidad Internacional SEK.* Retrieved from Universidad Internacional SEK: http://hdl.handle.net/123456789/271

González García, R., & Chaires Enríquez, S. (2005, Diciembre). *Seguridad en Internet: un estado del arte.* Retrieved from http://ri.ujat.mx/bitstream/20.500.12107/1549/1/890-3208-1-PB.pdf

Groenow, G. (2018, 03 14). Guayaquil.

Guano Llumigusín, J. (2015, SF SF). LAS TIC,s Y SU INFLUENCIA EN LA COMUNICACIÓN

ORGANIZACIONAL EN LAS INSTITUCIONES PÚBLICAS: CASO AGENCIA NACIONAL DE TRÁNSITO. Quito.

ISEC-Information Security Inc. (2014, SF SF). *Firma y Factura Electrónica.* Retrieved from http://www.isec-global.com/Education_Center/capacitaciones.html

Izquierdo Campoverde, I. (2015). *Sistema cero papeles para la gestión documental del Grupo de Intervención y Rescate GIR.* Retrieved from http://www.dspace.uce.edu.ec/handle/25000/4301

Javier, S. A. (2011, 05 23). *Repositorio Institucional de la UNLP.* Retrieved 11 28, 2013, from Repositorio Institucional de la UNLP: http://hdl.handle.net/10915/4025

Leal Labrada, O., & Linares Columbié, R. (2005). La información y sus espacios disciplinarios: un acercamiento a sus orígenes, desarrollo e interrelaciones. Acimed. Retrieved from http://scielo.sld.cu/scielo.php?pid=S1024-94352005000100003&script=sci_arttext&tlng=pt

Levene, R., & Chiaravalloti, A. (1998). *Delitos Informáticos.* Retrieved from http://www.chiaravalloti_asociados.dtj.com.ar/links_1.htm

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. (2002, 04 17). *Firma Electronica en el Ecuador y su beneficio en la gestión empresarial.* Retrieved from https://www.eci.bce.ec/documents/10180/28929/Presentaci%C3%B3n+Firma+electr%C3%B3nica.pdf/7644b0c6-2d5f-4698-98d8-69c7191b292b

Ley de Comercio Electrónico, firmas electrónicas y mensajes escritos. (2002, s.f s.f). Retrieved from http://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf

Ley de Comercio Electrónico, Firmas y Mensajes de Datos. (2014). Ley de Comercio Electrónico, Firmas y Mensajes de Datos.

Lizano Martínez, R., Madril Romero , C., & Villao Quezada , F. (2014, Mayo 26). *Artículos de Tesis de Grado - FIEC* . Retrieved from Aplicaciones de la firma electrónica en Ecuador: http://www.dspace.espol.edu.ec/xmlui/handle/123456789/25385

Lopez, L. F. (2003). *La Firma Electrónica en el Derecho Privado.* EBSCO.

Madril Romero , C. H., & Lizano Martínez, G. (2014). Retrieved from Aplicaciones de la Firma Electrónica en el Ecuador.

Ministerio del Interior del Ecuador. (2018, 03 18). Retrieved from http://www.ministeriointerior.gob.ec/

Naciones Unidas. (2015, Abril 12 a 19). 13er Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal.

Navarro, A. L. (2006, 11 24). *Gobierno del Principado de Asturias.* Retrieved from Gobierno del Principado de Asturias: http://ria.asturias.es/RIA/handle/123456789/63

Paulin, G., Robledo, M., & Brusa, G. (2014, SF SF). Diseño e implementación de Time-Stamping bajo un servidor confiable de fecha y hora .

Pérez, H., & Chávez, Y. (2012). Gestión documental, Gestión de información y Gestión del conocimiento: nociones e interrelaciones.

Pinela, R. E. (2013, agosto 21). *Repositorio Institucional de la Universidad de Guayaquil.* Retrieved from Análisis de la necesidad de la firma digital en las exportadoras e importadoras Guayaquileñas para la creación de una empresa de certificación: http://repositorio.ug.edu.ec/handle/redug/1219

Policía Nacional del Ecuador. (2018, 03 18). Retrieved from http://www.policiaecuador.gob.ec

Proasetel. (2003). *Proasetel Proyecto y Asesoria en Telecomunicaciones*. Retrieved from Proasetel Proyecto y Asesoria en Telecomunicaciones: http://www.proasetel.com/paginas/articulos/firmadigital.htm

Ramírez Romero, J. A. (2017, 02 SF). *El tratamiento del documento electrónico en los procesos judiciales en Colombia.* Retrieved from http://hdl.handle.net/10983/14202

Rico Carrillo, & Mariliana. (2005). Comercio electróncio, internet y Derecho.

Rojas, W. A. (2008, sf sf). Retrieved from IMPLEMENTACIÓN DE FIRMA DIGITAL EN UNA PLATAFORMA DE COMERCIO ELECTRÓNICO: http://m.tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/352/GARC%c3%8dA_WALTER_IMPLEMENTACI%c3%93N_DE_FIRMA_DIGITAL_EN_UNA_PLATAFORMA_DE_COMERCIO_ELECTR%c3%93NICO.pdf?sequence=1&isAllowed=y

ROYER, J.-M. (2004). *Seguridad en la informática de empresa/ Riesgos, amenazas, prevensión y soluciones.* Española. Retrieved from https://books.google.com.ec/books?id=K8XdRni4t94C&pg=PA23&dq=datos+confidenciales&hl=es&sa=X&ved=0ahUKEwjOrNae-cjOAhXIJB4KHWleCfkQ6AEIITAB#v=onepage&q=datos%20confidenciales&f=false

Sánchez Curbelo, B. (SF, SF SF). Revista Técnica de la Empres de Telecomunicaciones de Cuba S.A. *Las Nuevas Tecnologías y los Delitos Informáticos*. Retrieved 04 25, 2018

Sánchez, D. (2016). Ciberseguridad judicial y sellado de tiempo. 52 - 53.

Soler, J. (2008). La preservación de los documentos electrónicos.

Tejerina, R. O. (2014). *Seguridad del Estado y privacidad.* Madrid: Editorial Reus.

Temperini, M. (SF, SF). Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte.

Universidad el Bosque. (2008). *Revista de Colombiana de Bioética.* enero-junio.

Valdiviezo Black, A. G. (2010, 11 s.f). Retrieved from http://bibdigital.epn.edu.ec/handle/15000/3698

Villarreal, G. (2013). La firma electrónica y los certificados electrónicos: mecanismos de seguridad del mensaje de datos. *REVISTA DE LA UNIVERSIDAD DEL ZULIA 3ª época* , 54-73.

Anexos:

Anexo 1: Cuadro de la legislación que norma lo referente a delitos informáticos en algunos países de Latinoamérica. (Temperini, SF, pág. 7)

País	Legislación	Características Generales
Argentina	Código Penal, Ley 26.388 (2008), Ley 25.326 (2000)	A partir de Junio de 2008, la Ley 26.388 conocida como la "ley de delitos informáticos" ha incorporado y realizado una serie de modificaciones al Código Penal argentino. Es decir, la misma no regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias o independientes, sino que dicha ley modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia. Se modificó el Epígrafe del Capítulo III cuyo nuevo título es "Violación de Secretos y de la Privacidad", Los artículos que modifica o agrega son: 128, 153, 153 bis, 155, 157, 157 bis, 173, 183, 184, 197, 255. El art. 157 bis ya había sido incorporado por la Ley 25.326 de Protección de Datos Personales (2000) pero fue modificado por la Ley 26.388.
Bolivia	Código Penal, Ley 1.768 (1997), Ley 3325 (2006)	La Ley 1.768 realiza una reforma general al Código Penal. Allí incorpora como Capítulo XI, del Título XII, del Libro Segundo del Código Penal, el de "DELITOS INFORMÁTICOS". Dentro de este capítulo, se incorporan 2 artículos: 363 bis y ter, en cuyos textos se tipifica algunos delitos informáticos.
Brasil	Ley 12.737 (2012), Ley 11.829 (2008)	La Ley 12.737 es una ley reciente (año 2012), en la cual se dispone la tipificación criminal de los delitos informáticos y otras providencias. En su regulación incorpora modificaciones para los artículos 154-A, 154-B, 266 y 298. Por su parte, la Ley 11.829 regula el Estatuto de la Niñez y la Adolescencia, para mejorar la lucha contra la producción, venta y distribución de pornografía Infantil, así como tipificar como delito la adquisición y posesión de dicho material y otros comportamientos relacionados con la pedofilia en Internet.
Chile	Ley 19.223 (1993), Ley 20.009 (2005), Ley 18.168 (2002)	La Ley 19.223 es una ley "Relativa a Delitos Informáticos" de acuerdo a su propio título, donde regula cuatro artículos, desde los cuáles se tipifican varios delitos informáticos. La Ley 20.009 regula la responsabilidad para el caso de robo, hurto o extravío de tarjetas de crédito, en cuyo texto se sancionan algunas conductas relacionadas con estos aspectos. La Ley 18.168 (modificada por diferentes normativas) regula de manera general las telecomunicaciones, incorporando algunos tipos penales sobre la interferencia o captación ilegítima de señales de comunicación.
Colombia	Ley 1.273 (2009), Ley 1366 (2009)	La ley 1.273, de reciente sanción legislativa (año 2009), modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos". Se afirma que dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. A través de esta incorporación, suma el CAPITULO I, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", a partir del cual regula una serie de artículos penales que van desde el artículo 269A hasta el artículo 269J. Adicionalmente se incorpora el artículo 58, considerando como agravante general "si la realización de alguna de las conductas punibles, se realicen utilizando medios informáticos, electrónicos o telemáticos".
Ecuador	Ley Nº 67/2002 (2002)	La Ley No. 67/2002 regula el Comercio Electrónico, Firmas y Mensajes de datos. En dicha norma, dentro del Capítulo I del Título V, titulado "DE LAS INFRACCIONES INFORMÁTICAS", el art. 57 afirma que "Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley." En artículo siguiente, agrega y modifica varios artículos al Código Penal, incorporando diferentes figuras de delitos informáticos.
México	Reforma 75 del Código Penal Federal (1999)	Mediante reformas se crearon en el Código Penal Federal, los artículos 211 bis 1 al 211 bis 7, que buscaron tipificar los delitos informáticos clásicos teniendo en consideración la fecha de su incorporación. Se destaca la diferente que atentan contra los sistemas de cómputo que pueden o no, ser parte del sector financiero mexicano. Es importante destacar, que algunos Estados Mexicanos tienen además sus propias normas penales, incorporando otros delitos informáticos no analizados en este trabajo.

Anexo 2: Cuadro comparativo clasificado de acuerdo a los delitos informáticos analizados en algunos países de Latinoamérica. Se considera como referencia sin ser textual (Temperini, SF, pág. 8)

País	Acceso ilícito	Intercepción ilícita	Atentado contra la integridad de los datos	Atentado contra la integridad del sistema	Abuso de los dispositivos	Falsedad informática	Fraude o estafa informática
Argentina	SI	SI	SI	SI	NO	SI	SI
Bolivia	SI	NO	SI	NO	NO	NO	SI
Brasil	SI	NO	SI	SI	SI	NO	NO
Chile	SI	SI	SI	SI	NO	NO	NO
Colombia	SI	SI	SI	SI	NO	NO	SI
Ecuador	SI	NO	SI	NO	NO	SI	SI
México	SI	SI	SI	SI	SI	NO	NO