# Grado de madurez en Bolivia sobre la Seguridad de la Información

Ronald Rocha Zabaleta
*Postgrado en Informática*
*Universidad Mayor de San Andrés*
La Paz - Bolivia
ronrocza@gmail.com

***Resumen*—El grado de madurez de la seguridad de la información en Bolivia puede ser determinado no solo por los avances tecnológicos adoptados en el país, sino también por medio de la forma en que se norma el uso de las tecnologías. Por ello, esta investigación pretende explorar los antecedentes y jurisprudencia de inseguridad de la información en un contexto nacional, considerando los conceptos más relevantes. Dada la naturaleza cualitativa de la indagación, se opta por la revisión bibliográfica especializada y el estudio de casos. Se encontró qué en nuestro país, se presenta una ausencia de regulación respecto al mal uso de las tecnologías de la información y comunicación. Lo que representa un problema qué merece la urgente atención por parte del estado y profesionales entendidos en las tecnologías y las leyes.**

***Palabras clave—ciberseguridad, governance, ciberdelito, sexting***

## I. INTRODUCCIÓN

Con frecuencia hemos venido escuchando, en los últimos años, términos como: seguridad de la información, informática forense, ataques informáticos, seguridad informática, gobierno de la tecnología, hacking ético, delito informático, pero qué tan seguros estamos de entender estos tópicos y cuál es su nivel de aplicación en nuestro contexto nacional.

Con la llegada del Internet desde su creación en la década de los 60´s y su difusión en la década de los 90's, la globalización de la tecnología ha avanzado en igual medida que los nodos conectados a la Red de Redes, sin embargo, a pesar de este fenómeno, los países en vías de desarrollo como el nuestro, se enfrentan a la problemática de la brecha digital, que está asociado a los costos principalmente de hardware y software, que no están acorde al nivel económico deseado del país.

De igual forma, en el aspecto normativo y legislación penal, Bolivia no tiene definido leyes exclusivas que velen por la seguridad de la información en las entidades públicas y menos en las privadas, dejando a los CIO's y Directores TIC sin un lineamiento definido a seguir. Así mismo, el vacío legal sobre los delitos informáticos en Bolivia, permite una alta cifra de criminalidad e impunidad, dejando al ciudadano y a las entidades la responsabilidad de cuidarse a sí misma.

### *A. Conceptos y Definiciones*

*Seguridad de la Información*: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

*Informática Forense:* Es la aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas para realizar los procesos de Preservación, Colección, Análisis y Presentación de evidencia digital, de acuerdo a procedimientos Técnico-Legales preestablecidos, como apoyo a la Administración de Justicia en la resolución de un caso Legal.

*Ataque Informático:* Es un intento organizado e intencionado causada por una o más personas para causar daño o problemas a un sistema informático o red. Los ataques en grupo suelen ser hechos por bandas llamados "piratas informáticos" que suelen atacar para causar daño, por buenas intenciones, por espionaje, para ganar dinero, entre otras. Los ataques suelen pasar en corporaciones.

*Seguridad Informática:* También conocida como ciberseguridad o seguridad de tecnologías de la información, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La definición de seguridad de la información no debe ser confundida con la de seguridad informática.

*Gobierno TI: o IT Governance*, consiste en una estructura de relaciones y procesos destinados a dirigir y controlar la empresa, con la finalidad de alcanzar sus objetivos y añadir valor mientras se equilibran los riesgos y el retorno sobre TI y sus procesos. El Gobierno de TI, es una metodología de trabajo, no una solución en sí. Está orientado a proveer las estructuras que unen los procesos de TI, recursos de TI e información con las estrategias y los objetivos de la empresa [1].

*Hacking Ético:* es la utilización de los conocimientos de seguridad en informática para realizar pruebas en sistemas, redes o dispositivos electrónicos, buscando vulnerabilidades que explotar, con el fin de reportarlas para tomar medidas sin poner en riesgo el sistema [2].

*Delito Informático:* Un delito informático o *ciberdelito* es toda aquella acción típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet. Debido a que la informática se mueve más rápido que la legislación, existen conductas criminales por vías informáticas que no pueden considerarse como delito, según la "Teoría del delito",

**Para referenciar este artículo (IEEE):**
[N] R. Rocha, «Grado de madurez en Bolivia sobre la Seguridad de la Información», *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 8, pp. 173-175, 2020.

por lo cual se definen como abusos informáticos (los tipos penales tradicionales resultan en muchos países inadecuados para encuadrar las nuevas formas delictivas), y parte de la criminalidad informática [3].

Este paradigma ha sido superado hace ya varios años, pero en Bolivia aún subsiste la escuela antigua; no por tratarse de tecnologías nuevas sino por una ausencia de parte del estado y entendidos en el tema que de forma colaborativa se trabaje para conformar una base jurídica normativa nacional, o en su defecto partir de la experticia y la habilidad de los operadores de justicia para adecuar los tipos penales a las nuevas formas en que se presentan los incidentes.

Según esta visión, Bolivia no podría tener jurisdicción en el internet ya que carece de leyes que gobiernen el ciberespacio, lo cual es muy conveniente para los ciberdelincuentes.

### *B. Los casos más recurrentes en Bolivia.*

*Phishing*: Los autores, quienes pueden operar desde cualquier parte del mundo desarrollan una página web alterna y fraudulenta de alguna entidad financiera en la que sus víctimas, que son clientes de la entidad financieras, son contactadas mediante correo electrónico y les envían el portal falso del banco y bajo pretexto de que la institución está en un proceso de actualización piden datos y PIN de la tarjeta de crédito o débito.

*Clonación de tarjetas*: La víctima es afectada desde que asiste a un local o un centro comercial donde entrega su tarjeta de crédito para pagar sus compras o consumo, y el delincuente duplica su tarjera en un escáner sofisticado y se dan modos para seguirla y averiguar claves, con la que después vacían su cuenta.

*Sabotaje informático*: Este ciberdelito sucede cuando alguna persona, que puede ser ingeniero en sistemas, informático o conocedor de la internet, de forma maliciosa obstaculiza, modifica o comete cualquier otra acción que atente contra el normal funcionamiento de un sistema de información personal o de una institución.

*Falsedad y amenazas*: La falsificación y suplantación de identidad está ya contemplada en la legislación boliviana, consiste en que cierta persona averigua la contraseña de un correo electrónico ajeno y una vez que consigue ingresar modifica el contenido de cartas o documentos, o envía mensajes con diferentes fines a destinatarios [4].

## II. Materiales y Métodos de Investigación

Para la investigación se aplica una metodología mixta que aborda preguntas de investigación, desde lo deductivo, hasta lo analítico; considerando técnicas de recogida de datos con un enfoque cualitativo y documental de investigación.

Las Técnicas de la investigación aplicadas son:

*Investigación de campo:* A realizarse directamente donde se desarrolla las actividades de administración de la información producto de operaciones y actividades de empresas del medio.

*La observación:* Principalmente en las actividades que se llevan a cabo dentro del ambiente de una empresa, a nivel comercial y principalmente a nivel de administración de TI.

*Entrevistas a expertos:* Consulta a los especialistas del área de la infraestructura de tecnología, y en especial a los oficiales de seguridad de la información, para conocer sus experiencias respecto al tema.

*Investigación documental:* Selección de documentación relacionada al trabajo de investigación, principalmente a nivel normativo, experiencias en del sector privado/público y administración de la seguridad de la información en contextos cercanos a la realidad boliviana.

- Artículos digitales e impresos
- Periódicos y revistas
- Tesis y otras investigaciones referentes
- Seguimiento de reportajes

## III. Resultados: Casos de Criminalidad y delitos informáticos

*Manipulación de código para evitar descuentos en planilla, por retraso y faltas.*

En la entidad Pública el desarrollador alteró el código fuente del programa para la generación de planillas, para excluir a cierto personal del descuento mensual por retrasos o faltas. Concluido el proceso de planillas el desarrollador restituía el programa original.

*El brutal asesinato de Blanca R. por psicópatas y extorsionadores.*

El 28 de noviembre del 2013, la joven fue contactada a través de la utilización de una cuenta falsa de Facebook por RCh, fingiendo ser docente del Colegio Militar, quien prometió ayudar a Blanca ingresar a esa instancia; sin embargo, la joven fue encontrada días después muerta, golpeada y torturada en la vivienda del supuesto docente, que también intentó extorsionar a la familia. A estos delitos de los denomina suplantación de identidad y falsificación informática.

*Estafa agravada y manipulación informática en Cooperativa de Ahorro y Crédito.*

La Jefe de Crédito de la Cooperativa logró desviar dinero en beneficio personal, la suma de 169.600 $us, en coordinación con otras dos personas con quienes tenía cuentas de ahorro mancomunadas, gracias a manipulaciones de la información y documentos, aprovechando su condición de responsable del procesamiento de información crediticio.

*El sexting que sufrió una presentadora de televisión.*

Una presentadora de televisión fue víctima de extorsión de su expareja, quien pidió dinero para que un video privado no sea difundido en internet; sin embargo, la defensa de la víctima realizó la denuncia a la fiscalía donde se dictamino detención domiciliaria para el presunto extorsionador; esto después de que el video fue subido a la nube.

*Gobiernos Municipales, entre grandes y mediados.*

Personal de cajas y de sistemas utilizaban la herramienta FOXPRO para indagar las bases de datos donde se registraban los cobros de recaudaciones y los parámetros de construcción de inmuebles para el cálculo de impuestos, para luego modificar dichos parámetros y ejecutar un reproceso de la recaudación diaria, reduciendo importes a pagar por concepto de impuestos, reimprimiendo boletas de pago, para quedarse con el saldo del dinero en efectivo del cobro efectuado y reprocesado. La Contraloría General de la República detectó el fraude el 2001.

## IV. Discusión: Situación y El contexto nacional

Ante la creciente importancia de la Seguridad Informática en países desarrollados, se tienen definidas políticas que establecen

la creación de organismos oficiales relacionados a la Seguridad de la Información, tales como INCIBE Instituto Nacional de Ciberseguridad de España, el EC3 Centro Europeo de Ciberdelincuencia de la Unión Europea, el NCAZ Centro Nacional de Defensa Cibernética de Alemania, el NSA Agencia de Seguridad Nacional de Estados Unidos; incluso en américa latina se han creado organismos como: CERTuy de Uruguay y arCERT de Argentina.

En el contexto nacional, además de la AGETIC (Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicaciones) y la ADSIB (Agencia para el Desarrollo de la Sociedad de la Información), solo tenemos una división de Informática Forense de la Policía en la Fuerza Especial de Lucha Contra el Crimen FELCC, que recibe denuncias de delitos informáticos en el país, de las cuales sólo un 70% sigue una investigación, en su mayoría los casos no son resueltos, por su complejidad o por falta de profesionales peritos informáticos tanto en la policía, como en los operadores de la justicia, para atender ese tipo de casos.

La legislación boliviana es muy pobre respecto a delitos informáticos, pues se tiene tipificado solo dos delitos en el Código Penal (Manipulación informática y alteración, acceso y uso indebido de datos informáticos), de igual forma, en la nueva Constitución Política del Estado se tiene una mención muy escueta respecto a la seguridad de la información.

Bajo el actual contexto tanto entidades, como el ciudadano común, que son víctimas de los delitos informáticos, optan por no concluir un proceso penal, ante la falta de profesionales, respaldo legal, costos elevados y principalmente el desprestigio público que puede sufrir la entidad o la persona, sin obtener un resultado favorable.

En contraste, en las empresas privadas, principalmente el sector de la banca y de las telecomunicaciones, se puede encontrar que se tiene un gran avance en la modernización de sus instalaciones en *datacenters* e la infraestructura tecnológica en general, paralelamente la Autoridad de Supervisión del Sistema Financiero ASFI y la Autoridad de Telecomunicaciones y Transporte ATT han desarrollado un compendio normativo medianamente completo, que incluye la obligatoriedad de certificaciones internacionales, tales como PCI DSS (*Payment Card Industry Data Security Standard*), pero aún sin un claro lineamiento nacional, que guie cómo implementar un Sistema de Seguridad de la Información SGSI, para luego obtener una certificación PCI DSS o ISO27001 que proteja la inversión en tecnología.

A nivel nacional pocas empresas cuentan con una certificación de este tipo, quienes usan la certificación más para fines de marketing y promoción empresarial; por otro lado, tampoco contamos con profesionales especializados que coadyuven la obtención de una certificación y menos instituciones que brinden este tipo de capacitación requerido.

## V. Conclusiones: Necesidad de un modelo de seguridad de la información

Bolivia como país se encuentra en un grado de madurez sobre la Seguridad de la Información muy bajo y se espera que con el pasar de los años este aspecto mejore, sin embargo, las empresas bolivianas que invierten mucho dinero en infraestructura tecnológica no pueden permitirse dejar de lado la implementación de medidas de seguridad informática, protegiendo el activo más valioso, la información.

Es por eso que se ha visto la necesidad de contar con un urgente modelo de seguridad de la información adaptable a nuestro contexto nacional, que considere aspectos de los principales estándares internacionales, normas, mejores prácticas, metodologías y documentos oficialmente reconocidos, tales como:

- ISO 17799 – Estándar para la Seguridad de la Información.
- Serie ISO 27000 – Familia de estándares que proporcionan un marco de gestión de la seguridad de la información.
- ISO 27001 – Estándar Internacional para la implementación del SGSI que permite a una organización evaluar su riesgo e implementar controles apropiados.
- ISO 27002 – Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información
- ISO 20000 se concentra en la gestión de problemas de tecnología de la información.
- COBIT – Control Objectives for Information and Related Technology
- ITIL – Information Technology Infrastructure Library

A pesar de la distancia entre el estado actual versus el estado deseado del nivel de madurez sobre seguridad de la información en el país, se tiene la ventaja de poder aplicar métodos y conceptos ya probados para poder desarrollar un modelo de Seguridad de la Información, explotando experiencias y documentos relevantes como los anteriormente descritos, que ataque principalmente al eslabón más débil y vulnerable de la seguridad de la información, el factor humano, con un plan estructurado de capacitación y concientización muy bien pensado, y que esté respaldado por una política de seguridad de la información que englobe los aspectos más importantes de un SGSI, en la búsqueda constante de la mejora continua.

## Referencias


[1] Gobiernoti, (2011). ¿Qué es gobierno TI? Obtenido de: https://gobiernoti.wordpress.com/2011/06/19/gobierno-ti/

[2] Enter.co, (2014). El hacking ético y su importancia para las empresas. Obtenido de: http://www.enter.co/guias/tecnoguias-para-empresas/que-es-el-hacking-etico-y-por-que-es-necesario/

[3] Noticias de Tecnología y Telecomunicaciones, (2008). Cincuenta delitos informáticos están sin resolver por falta de peritos en esa materia. Obtenido de: http://www.telecombol.com/2008/12/cincuenta-delitos-informticos-estn-sin.html

[4] Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), (2018), Estado TIC, La Paz, Bolivia.

[5] Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), (2019), Juventudes TIC, La Paz, Bolivia.

[6] Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB) y la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), (2018), Estudios Jurídicos Comparados con relación al Gobierno Electrónico, La Paz, Bolivia