Seguridad de la información en el área Judicial en Bolivia

Yokonda Steel Gutiérrez Callizaya
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
yokonda001@gmail.com

***Resumen*—El objetivo de la presente investigación es mostrar que la seguridad de la información aporta una serie de herramientas y buenas prácticas al área Judicial. Lamentablemente en Bolivia los delitos a nivel de informática han aumentado por la carencia de inversión y poca capacitación. Se debe tomar en cuenta los diversos actores económicos en la era de la información para asegurar una adecuada política de seguridad de la información que, ante la falta de legislación nacional, debe basarse en estándares internacionales. La metodología empleada para explicar las diversas áreas de impacto es la norma ISO 27001 en el dominio que hace referencia al cumplimiento, y políticas que deben implementarse de una manera adecuada. El desarrollo cada vez más acelerado de la tecnología; que influye en el incremento de la utilización del internet en la vida social, económica y cultural, además de los beneficios que refleja para la sociedad; generará nuevas actividades en el área judicial en materia de seguridad de la información, y en la regulación de esta norma y otras.**

Palabras clave—Seguridad de la Información, ISO 27001.

I. INTRODUCCIÓN

La seguridad de la información es el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información. La seguridad puede verse desde dos perspectivas muy definidas: la legislativa y la tecnológica; de la primera se hacen cargo los políticos, quienes tienen por función decidir sobre su importancia, los delitos en que se puede incurrir con su respectivo castigo, teniendo grandes logros en materia de prevención de crímenes, terrorismo y riesgo; en cuanto a la tecnológica, la seguridad está en manos de los tecnólogos y en ocasiones en manos de la dirección de las organizaciones, debiendo tomar en cuenta el grado de concientización de cada uno de nosotros respecto a la importancia de la información [1].

La seguridad de la información aporta al área jurídica una serie de herramientas, recomendaciones y buenas prácticas. ISO/IEC 27001 Tecnología de la información-Técnicas de la seguridad –Requisitos de un Sistema de Gestión de Seguridad de la Información (SGSI) es un estándar reconocido internacionalmente, proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información; como otras normas, adopta un enfoque por procesos y sigue el modelo "planificar-hacer-verificar-actuar" (plan-do-check-act conocido como modelo PDCA). Su objetivo fundamental es la gestión de la confidencialidad, la integridad y la disponibilidad de cualquier bien que tenga valor. Es conveniente aclarar que el sistema de gestión, que se crea bajo la ISO 27001, incluye no solamente la parte informática, sino también los recursos humanos y económicos, patentes, contratos con los clientes, imagen y reputación en las organizaciones apropiadas para poder evaluar riesgos y establecer los controles oportunos, proteger la información de las personas, así como realizar auditorías internas a fin de evaluar el cumplimiento de los objetivos y procedimientos para asegurar la información.

Las políticas de seguridad en el área legal incluyen aspectos técnicos y organizativos, para identificar los flujos de información que pueden ser vulnerados fácilmente. Se aconseja incluir en los contratos una solicitud de aceptación y conformidad de las políticas de seguridad por parte de los empleados; así es posible vincularlos jurídicamente con los ordenamientos referidos, ya que los empleados requieren ser conscientes de sus obligaciones legales y éticas para proteger la información [2].

La aplicación de la seguridad de la información es proteger la información de unidades de memoria con fines de investigación. En Bolivia, son aún insuficientes las inversiones en informática y la formación de recursos humanos especializados, aspectos que requieren mayor atención por parte del estado.

La NITS, la cual está basada en la ISO 27002, explica los aspectos más resaltantes de los controles y su norma; a partir de los cuales se plantea un esquema de gestión de seguridad de información que puede ser empleado por diferentes instituciones en el área jurídica, lo cual permite que ésta cumpla con las normas de regulación vigentes en lo relacionado a la seguridad de información que va difundiéndose.

A pesar de que en Bolivia se establece programas de seguridad de la información respecto a sus operaciones, es necesario empezar a gestionar controles de seguridad para poder garantizar que la información no sea alterada o manejada por personas no autorizadas. Actualmente no se llega aplicar en su totalidad debido a la falta de lineamientos de seguridad que permiten tener el control adecuado del manejo y los accesos a los sistemas de procesamiento de información [3].

El criterio corresponde al experto Sergio Luna, investigador forense y seguridad de la información, en cuya experiencia, la falta de protocolos para resguardar y proteger el manejo de

Para referenciar este artículo (IEEE):
[N] Y. Gutiérrez, «Seguridad de la información en el área Judicial en Bolivia» *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 108-111, 2020.

información y tecnología de mediana actualización son tareas pendientes que requieren ser superadas con prontitud.

Refiere Luna: "Muchas veces la información rescatada es mal manipulada por personal inexperto, ésta puede ser mal interpretada lo que pone en riesgo la propia investigación".

Desde el análisis de los expertos, el país carece de laboratorios, medidas preventivas y políticas de seguridad de la información con los que se pueda recurrir a estudios de carácter lógico, electrónico y físico eficientes de las unidades de memoria, aspecto que hace de esta actividad actualmente imprescindible en el ámbito de la seguridad de la información.

Según cálculos iniciales, contar con un laboratorio razonable y políticas para lograr resultados garantizados en investigación forense demanda al menos treinta mil dólares, además de capacitar recursos humanos en países donde los avances tecnológicos permiten avances reales, son inversiones que el estado debe tomar con responsabilidad y dejar exclusivamente a la iniciativa privada.

Desde la experiencia de Luna, en el país no existe más de 10 expertos seguridad de la información quienes trabajan de manera individual y privada. "El desarrollo de la informática es tan vertiginoso que estar constantemente actualizados es un requisito primario que no podemos descuidar como Estado" [4].

La seguridad de la información es importante porque beneficia al gestionar incidentes donde las evidencias y cálculos pueden presentar problemas ante la materialización de un incidente. Es posible presentar de forma clara las posibles soluciones para la mitigación correctiva o preventiva de estos eventos no deseados, y de esta forma poder garantizar que la inversión cubra las brechas de seguridad más importantes [5].

La aplicación de seguridad de la información en Bolivia tuvo un gran desarrollo, pero tenemos que ir capacitando y hacer conocer los beneficios que ésta nos presenta.

II. MÉTODOS

En el presente trabajo se utilizó la investigación con un enfoque mixto; que representa un conjunto de procesos sistemáticos, empíricos y críticos de investigación, e implican el análisis de datos cuantitativos y cualitativos; así como su integración y discusión conjunta. El método inductivo es una forma de razonamiento que va de los hechos concretos y particulares para llegar a establecer principios generales. Se realizó una síntesis que consiste en ir de lo simple a lo compuesto de las partes al todo. También se define como el proceso por el cual a partir de situaciones de carácter particular se emplea la investigación con este tipo de enfoque a razón de que se estudiaran datos cuantitativos en un principio en la protección de datos para posteriormente realizar un análisis cualitativo, así se tendrá una visión más completa respecto al impacto de la seguridad de la información en Bolivia y en el manejo de la información en la ciudad de La Paz [6].

La investigación es de carácter explicativo, ya que durante el periodo de investigación se explica que las estadísticas de Yanapti 2018 indican que mensualmente se genera cientos de programas cuyo principal objetivo es robo financiero y manipulación de datos, poniendo en riesgo la información confidencial. Se utilizó la investigación transversal que recolecta los datos en un solo momento, y en un tiempo único. El propósito es describir variables y analizar sus incidencias e interrelaciones en un momento dado. El tema investigado abarcara el contexto actual además de que para un mejor desarrollo del mismo se apoya en varias disciplinas como ser el área jurídica y seguridad de la información.

A. Seguridad de la Información

La Seguridad de la Información es la ciencia y medidas preventivas que permiten resguardar, proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos, obtener y presentar información que ha sido resguardada correctamente, manteniendo protocolos de seguridad. Debería ser más habitual el uso de nuevas tecnologías que permitan el manejo de la información de manera correcta y así aportar técnicas de seguridad para evidencia o información, para poder ayudar en casos policiales o judiciales sobre la seguridad y poder colaborar en el área judicial y la seguridad del estado como los peritos informáticos forenses que utilizan herramientas y procedimientos específicos [7].

B. Principios de Seguridad de la Información

El primero de los tres principios de la seguridad de la información que aplicamos es la integridad, la cual nos permite garantizar que la información no ha sido alterada en su contenido, por tanto, es íntegra. El principio de la confidencialidad de la información tiene como propósito el asegurar que solo la persona correcta acceda a la información que queremos distribuir. Una vez que nos aseguramos que la información correcta llegue a los destinatarios o usuarios correctos, ahora lo que debemos garantizar es que llegue en el momento oportuno, y precisamente de esto trata el tercer principio de la seguridad de la información: la disponibilidad. Para que una información se pueda utilizar, deber a estar disponible. Es importante, además, que todos los empleados de donde trabajen tomen conciencia sobre el manejo de la información de forma segura, ya que de nada sirve cualquier sistema de seguridad, por complejo y completo que éste sea, si los empleados, al facilitar su usuario y contraseña a personas dejan abierta la puerta a posibles ataques o filtraciones de información crítica al exterior.

C. Políticas de Seguridad

Para elaborar una política de seguridad de la información es importante tomar en cuenta las exigencias básicas y las etapas necesarias para su producción.

D. Exigencia de Políticas de Seguridad

La política es elaborada tomando como base la cultura de la organización y el conocimiento especializado en seguridad de los profesionales involucrados en su aplicación y compromiso. Es importante considerar que para la elaboración de una política de seguridad institucional se debe:

- Integrar el comité de seguridad responsable de definir la política (equipo multidisciplinario).
- Elaborar el documento final (preocupaciones de la administración, atribución de las responsabilidades de las personas involucradas, legislación y cláusulas contractuales, prevención contra amenazas, educación y formación en seguridad de la información) documentados de tal manera;
- Hacer oficial la política una vez que se tenga definida (aprobación por parte de la administración, mecanismos

de comunicación efectiva a socios, empleados, proveedores y clientes de la empresa).

E. Etapas de Producción de Políticas

Elaborar una política es un proceso que exige tiempo e información. Es necesario saber cómo se estructura la organización y como son dirigidos en la actualidad sus procesos.

- Objetivos y ámbito (presentación del tema de la norma);
- Entrevista (identificar junto con los usuarios las preocupaciones que ellos tienen con los activos, los procesos de negocio);
- Investigación y análisis de documentos (se identifica y analiza los documentos existentes en la organización);
- Reunión de política (se discuten los temas y se redactan las políticas);
- Glosario de la política (aclaración de dudas conceptuales alrededor de la política)
- Responsabilidades y penalidades (identificar a los responsables por la gestión de la seguridad y cumplimiento de tareas [8].

III. Resultados

Se analizó la seguridad de la información, políticas de seguridad de información y, según Yanapti 2018 [9], los índices de delitos se multiplicaron paralelamente al incremento de la criminalidad. Se describió los principios de políticas de seguridad, sus exigencias y etapas. Se analizó que es importante que todos los empleados o usuarios tomen conciencia sobre el manejo de su información de forma segura ya que de nada sirve implementar políticas de seguridad complejas si no hay capacitación.

El trabajo de investigación del Dr. Fabián Espinoza 2019 [10] permite observar cifras razonables y muy indicativas. A nivel de Bolivia, se muestra un indicador sobre los delitos informáticos y delitos con vinculación al internet de manera general, relacionados con la seguridad de la información en los 9 departamentos, con el detalle correspondiente y una breve descripción de determinados hallazgos cualitativos en determinados asientos judiciales desde el Órgano Judicial, y a su vez tópicos referidos a 4 Ministerios del Órgano Ejecutivo.

En el estudio se procedió a establecer una estadística descriptiva censal concentrada en el Órgano Judicial, recabando información de fuente primaria concerniente a la existencia de procesos y otros delitos relacionados con el internet de manera directa o indirecta en los diversos asientos judiciales, el estudio incorpora datos sobre las cifras más relevantes en los asientos judiciales de los 9 departamentos del país, incluyendo la jurisdicción de El Alto, así como ciudades del interior conforme a la información proporcionada por las autoridades judiciales, obteniéndose como resultado el siguiente cuadro:

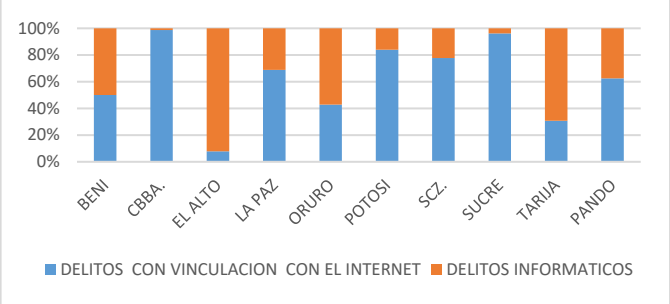

Fig. 1. Delitos a nivel de Bolivia.
Fuente: Órgano Ejecutivo de Bolivia y Ministerio Público 2017

En la Fig. 1 se pudo evidenciar que los delitos a nivel de Bolivia aumentaron. La ausencia de políticas a nivel de seguridad de información genera un impacto negativo en la justicia porque no existe un mecanismo idóneo para registro de causas. Existen autoridades judiciales que asumen el cargo por el área de estudio y experiencia; no ventilan procesos relacionados directa o indirectamente a delitos relacionados con la informática. En muchos casos la intervención de las tecnologías de la información y comunicación únicamente están en las etapas preliminares de investigación y de manera complementaria a los medios probatorios tradicionales. La Paz cuenta con la mayor cantidad de procesos registrados relativos a delitos informáticos relacionados con la seguridad información. Porque no se cumplieron ciertos protocolos, Cochabamba registra los más altos índices de violencia vinculados con el ciberespacio.

Lamentablemente hay una brecha digital en la cual existen hallazgos que permiten evidenciar que existen jurisdicciones que no cuentan con acceso a internet, y el personal de la administración de justica entiende que no es parte de sus funciones tratar estos procesos por la falta de capacitación en el área judicial. Por el momento, no existe un juzgado para tratar exclusivamente procesos especializados en el área de informática y tecnología [10].

IV. Discusión

Se analizó el manejo de información en la seguridad de la información y como proporciona medidas preventivas que permitan resguardar y proteger la información.

Se comprobó que la seguridad de la información provee métodos y procesos de buenas prácticas para el manejo adecuado de la información utilizando medidas preventivas.

El buen uso de la seguridad de la información en el manejo de la información da soluciones a casos desestimados.

Con una correcta aplicación de las diferentes técnicas y procedimientos estrictos y rigurosa seguridad, siempre apoyándose en el método científico, se aporta a la protección y prevención en el análisis y en la validación de toda clase de pruebas digitales.

V. Conclusiones

Las políticas deben ser claras, concisas, contextualizadas a una realidad, enfocadas ya sea en el ámbito judicial o empresarial. Según las cifras presentadas en estudios relacionados con seguridad informática, en el área judicial más de un 60% de casos fueron observados porque no cumplieron ciertos protocolos de seguridad. Es responsabilidad de las

personas que están a cargo tener capacitación constante en seguridad de la información. Con esto, se permite dar un nuevo enfoque y dar soluciones necesarias en nuestro país, en cuanto al manejo de la información o evidencia digital.

REFERENCIAS

[1] Aimeur, Esma; Schonfeld, David (2011). "The ultimate invasion of privacy: identity theft". In: Ninth Annual intl conf on privacy, security and trust, pp. 24-31.

[2] Juan Carlos Serrano Antón ISO 27001. Responsable Unidad Técnica de Seguridad de la Información OCA Cent

[3] Villena M.A. (2018) Sistemas de seguridad de la información. Bolivia.

[4] Sánchez E.R. (2019) Análisis en Seguridad Informática y seguridad información basado en la norma ISO/IEC 27001. La paz Bolivia.

[5] Luna I.S. (2018). Informática forense e investigación un criminal, son tareas pendientes. La Paz.

[6] Espitia, D. S. (2017). Seguridad de la Información. España.

[7] Fernández P. Seguridad de la Información como se usa para resolver casos policiales o judiciales. PIXABAY, 25.

[8] Jimmy Cano PhD, Introducción a la Informática forense y seguridad. España.

[9] Uriona M.G. (sf) Informática forense La Paz: Yanapti Securing your e-life.

[10] Fundación construir Dr. Fabián Mendoza ODIB (Observatorio de delitos informático Bolivia) Diagnostico sobre la ciberdelincuencia

Breve CV de la autora

Yokonda Steel Gutierrez Callizaya es Licenciada en Informática por la Universidad Mayor de San Andrés, La Paz. Actualmente realiza la Maestría en Informática Forense, Seguridad de la Información y Auditoría Informática en el Postgrado en Informática UMSA. Ejerce la docencia universitaria y el desarrollo de sistemas. Email: yokonda001@gmail.com.