CADI/CLADI
CAEDI

5to. Congreso Argentino de Ingeniería
3er. Congreso Latinoamericano de Ingeniería
11vo. Congreso Argentino de Enseñanza de la Ingeniería

Elaboración de un Sistema Integrado de Gestión de la Calidad y de Ciberseguridad

Parra, H.B.[a] ; Ambrústolo, M.B.[b]; Cistoldi, P.A.[c] ; Onaine, A.[b] ; Di Iorio, A.H[c]

a. Universidad Católica de Salta, Facultad de Ingeniería
b. Universidad Nacional de Mar del Plata, Facultad de Ingeniería
c. Universidad FASTA, Facultad de Ingeniería y MPBA.

bgallo@ucasal.edu.ar

Resumen

Brindar a las partes involucradas en un proceso judicial las garantías correspondientes al debido proceso es una obligación de la justicia. La obtención de la evidencia digital debe realizarse respetando principios forenses: evitar la contaminación, actuar metodológicamente y mantener la cadena de custodia. Sin embargo, “mantener la cadena de custodia” respecto de la evidencia digital implica no sólo custodiar el elemento físico sino también trasladar la custodia de la evidencia material a la trazabilidad del elemento digital y de la información que éste contiene. Es aquí donde los aspectos de ciberseguridad y seguridad de la información toman un rol preponderante.

Se presentan en este trabajo los antecedentes, fundamentos y metodología propuesta para el desarrollo del proyecto “Elaboración de una Guía Técnica para el desarrollo de un Sistema Integrado de Gestión de la Calidad y de Ciberseguridad en Laboratorios de Informática Forense”, que. tiene como objeto la elaboración de una guía técnica que incorpore, en los Sistemas de Gestión de la Calidad de los laboratorios de informática forense, las normas de Ciberseguridad y Seguridad de la Información relevantes y pertinentes al actuar judicial pericial, que pueda ser implementada en Laboratorios de Informática Forense tanto judiciales como extrajudiciales. Este proyecto será desarrollado por tres equipos de investigadores interdisciplinarios provenientes del área de calidad, de la informática forense y del ámbito legal-judicial, y pertenecientes a distintas instituciones universitarias, contando con la participación activa de funcionarios y técnicos de laboratorios del sistema judicial y extrajudicial.

Abstract

Providing the parties involved in a judicial process with the guarantees corresponding to due process is an obligation of justice. Obtaining digital evidence must be carried out respecting forensic principles: avoid contamination, act methodologically and maintain the chain of custody. However, “maintaining the chain of custody” regarding digital evidence implies not only guarding the physical element but also transferring the custody of the material evidence to the traceability of the digital element and the information it contains. It is here where the cybersecurity and information security aspects take a preponderant role.

The background, foundations and proposed methodology for the development of the project "Preparation of a Technical Guide for the development of an Integrated Quality Management and Cybersecurity System in Computer Forensic Laboratories" are presented in this work. The purpose of this project is to develop a technical guide that incorporates, in the Quality Management Systems of the forensic computer laboratories, the relevant and pertinent Cybersecurity and Information Security standards when acting judicial expert, which can be implemented in Forensic Informatics Laboratories, both

judicial and extrajudicial. This project will be developed by three teams of interdisciplinary researchers from the quality area, forensic computing and the legal-judicial field, and belonging to different university institutions, with the active participation of officials and laboratory technicians of the judicial and extrajudicial system .

***Palabras clave**:* Ciberseguridad, Informática Forense, Sistemas Integrados, Sistema de Gestión de Calidad.

INTRODUCCIÓN

El crecimiento de la cantidad de dispositivos y aplicaciones tecnológicas es exponencial. También lo es la acumulación de información transmitida y almacenada en esos dispositivos y sistemas. Todo esto impacta en la producción de nuevos conflictos sociales, y en la irrupción masiva de una nueva fuente de prueba judicial: la prueba digital.

La prueba digital tiene características propias, y su utilización en un proceso judicial posee requisitos específicos, para asegurar su preservación y validar su origen e integridad. Por otra parte, los dispositivos digitales contienen información que nada tiene que ver con el caso judicial específico, tanto sobre las partes de un litigio como sobre terceros.

El Estado, como garante de la justicia, debe ser capaz de cumplir, cuanto menos, con estos requerimientos: a) asegurar el valor probatorio de la prueba digital pertinente y útil (protección de la prueba), y b) asegurar la reserva sobre toda la información que no sea pertinente al caso, y evitar el uso indebido de los datos con valor probatorio (protección de datos personales). Nada de esto puede lograrse sin contar con sistemas de gestión integrados que contemplen la ciberseguridad y la seguridad de la información. Y un área crítica donde esta exigencia se pone en juego es la de los Laboratorios de Informática Forense (LIF), pues por ellos pasan los dispositivos y la información digital y, asimismo, de ellos proviene el conocimiento experto para contribuir a que el sistema de justicia en su conjunto brinde estas condiciones de seguridad.

En el actual contexto de la justicia, se observa con preocupación la urgente necesidad de incorporar las Tecnologías de la Información y de la Comunicación (TIC) para la mejora de los procesos de gestión, que han derivado en la implementación de entornos virtuales para el trabajo diario del abogado y de todos aquellos que actúan en la mayoría de los foros judiciales de nuestros país. Es necesario considerar también la CIBERSEGURIDAD, como ámbito de sumo interés para el resguardo de las garantías procesales en la gestión de la justicia. Por lo tanto resulta imperioso generar entornos tecnológicos seguros, con presencia de las cuestiones de reserva de datos y cuidado por la privacidad de las personas, además de considerar procesos ágiles y confiables para el ciudadano en general, y para el ámbito judicial en particular.

La gestión de la justicia involucra múltiples áreas que cumplen roles diferentes, siendo los LIF uno de los ámbitos auxiliares de la justicia de mayor interés, dado el incremento de los delitos mediados por las TIC, que producen numerosas evidencias digitales que deben ser recolectadas y analizadas en el contexto de una causa judicial. Estos laboratorios cumplen un rol fundamental, ya que además de procesar la evidencia digital, se les exige cumplir con estándares rigurosos en cuanto al procesamiento, manipulación y tratamiento en general de esa evidencia digital.

Por otra parte, es sabido que las normas ISO son establecidas por la Organización Internacional de Estandarización (ISO), y se componen de estándares y guías relacionados con sistemas y herramientas específicas de gestión aplicables en cualquier tipo de organización. De ellas se pueden tomar las normas referidas a dos áreas de interés para los LIF: la gestión de calidad y la seguridad de la información.

Se presenta en este trabajo un proyecto de investigación, desarrollo e innovación en el área

de CIBERSEGURIDAD, utilizando las capacidades científicas y tecnológicas de tres instituciones que abordan cuestiones de interés para el DESARROLLO DE PROCEDIMIENTOS DE ACTUACIÓN EN LABORATORIOS DE ANÁLISIS FORENSE DIGITAL basados en criterios de calidad y estandarización que marca la Informática Forense.

La implementación de un Sistema de Gestión de Calidad, de protocolos y diferentes herramientas en los LIF, permite que en todo momento se pueda evidenciar y garantizar la calidad de los procesos llevados a cabo y su actualización permanente. Ello fortalece la confiabilidad de los LIF, la confiabilidad de la prueba digital durante todo el proceso judicial, y contribuye a resguardar los derechos de los titulares de los datos. Dada la criticidad de la información que tratan los LIF, ya sean estos judiciales o extrajudiciales, resulta necesario además integrar, en el sistemas de gestión de la calidad, aspectos de calidad como aquellas normas de ciberseguridad y seguridad de la información que sean relevantes y pertinentes al actuar judicial pericial así como las normas jurídicas involucradas. Es escasa la existencia de experiencias de integración entre este tipo de normas de gestión y no hay modelos desarrollados para la informática forense, siendo un doble desafío concretar esta integración teniendo en cuenta la incorporación de los requisitos de las normas legales relacionadas con estas tareas.

Si bien las instituciones participantes del proyecto han comprometido formalmente los recursos humanos, técnicos y presupuestarios suficientes para el desarrollo del proyecto, se ha visto la oportunidad de presentar el proyecto a la convocatoria de cofinanciamiento Proyectos Interinstitucionales en Temas Estratégicos (PITES) del Ministerio de Ciencia y Técnica de la Nación[1], cuyo propósito es fomentar la articulación y coordinación entre diferentes instituciones al sumar capacidades científicas y tecnológicas complementarias, a través de la ejecución de proyectos de investigación, desarrollo e innovación de forma asociativa y multidisciplinaria.

DESARROLLO

A continuación se describen los distintos elementos que componen el proyecto propuesto.

Premisas de Base

El objetivo general del proyecto se plantea en términos de lograr la elaboración de una guía técnica para el desarrollo de un Sistema Integrado de Gestión (SIG) de Laboratorios de Informática Forense, que incorpore las normas de calidad, de ciberseguridad y seguridad de la información relevantes y pertinentes tanto para el actuar judicial como extrajudicial. Los objetivos específicos que se pretenden son los siguientes:

- Relevar y estudiar las normas de gestión y técnicas relacionadas a la ciberseguridad y a la seguridad de la información factibles de ser aplicadas en un LIF.
- Determinar las normas que conformarán el sistema integrado a partir de la estructura de alto nivel definida en el Anexo SL de la ISO.
- Definir y desarrollar los procesos estratégicos, operativos y de soporte que permitan la integración de las normas en los LIF en el ámbito del sistema de justicia y externos.
- Elaborar una guía técnica para el desarrollo de un Sistema Integrado de Gestión en Laboratorios de Informática Forense, que incorpore las normas de ciberseguridad y seguridad de la información adecuadas.
- Validar la Guía Técnica en un laboratorio de informática forense del ámbito judicial y en uno externo.
- Promover la articulación y coordinación de las capacidades científicas y tecnológicas complementarias de las instituciones participantes – UCASAL, UFASTA y UNMDP – a través de la ejecución del presente proyecto de investigación, desarrollo e innovación vinculado al área de CIBERSEGURIDAD, más específicamente a la INFORMÁTICA FORENSE.

Marco teórico inicial

El abordaje del desarrollo de un Sistema Integrado de Gestión de Calidad, basado en las normas de Ciberseguridad y Seguridad de la Información más pertinentes y relevantes para los espacios abocados a los procesos del análisis forense de la evidencia digital, requiere del estudio de estas temáticas desde la mirada específica en la Informática Forense.

A tal fin, se puede definir como marco de estudio inicial las investigaciones salientes sobre las siguientes temáticas: Normas de Seguridad Informática, tratamiento de la Evidencia Digital y Sistemas de Gestión de Calidad.

[1] https://www.argentina.gob.ar/ciencia/financiamiento/pites

La Seguridad de la Información es la Preservación de su Confidencialidad, Integridad y Disponibilidad (ISO/IEC 27000:2014). Refiere a la protección de la información en cualquier soporte y a los recursos de cualquier naturaleza utilizados para gestionarla (Information Security).

La Seguridad Informática es la disciplina que se ocupa de mitigar los incidentes de seguridad de la Información. Es el conjunto de recursos humanos y tecnológicos que, en conjunto con procedimientos y normas, garantizan la confidencialidad, integridad y disponibilidad de la información. Refiere a la protección de la Infraestructura TIC que soporta el conjunto de actividades que lleva adelante una organización. (IT Security).

En cambio, la ciberseguridad es un concepto amplio que va más allá de la seguridad informática y la seguridad de la información. Se centra en la seguridad de las personas y en tratar de prevenir actos disvaliosos, que afecten sus derechos. Es así que la Resolución SGM N° 1523/2019 de la Secretaría de Gobierno del Ministerio de Modernización de la República Argentina aprueba la definición de Infraestructuras Críticas y de Infraestructuras Críticas de Información, enumera criterios de identificación de dichas infraestructuras, determina los sectores alcanzados y presenta un glosario de términos de ciberseguridad. Allí se señala que “Las Infraestructuras Críticas de Información son las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas”.

Pese a que la resolución citada es aplicable solamente a organismos del Poder Ejecutivo Nacional, los conceptos y criterios allí establecidos pueden ser trasladados al ámbito forense. Es indudable que las tecnologías y la información asociada que forman parte de la operatoria de los Laboratorios de Informática Forense pueden cumplir con uno o varios criterios de impacto previstos en dicha resolución (impacto en la vida humana, impacto económico, impacto en el ejercicio de los derechos humanos y las libertades individuales, impacto público o social, y/o impacto en el ejercicio de las funciones del Estado, incluido el Poder Judicial).

Si bien la temática principal del proyecto se enfoca al desarrollo de un sistema integrado de gestión, desde el punto de vista del tratamiento de la evidencia digital, será importante abordar algunas tecnologías emergentes o escenarios tecnológicos en donde podría encontrarse una evidencia digital que luego debe trabajarse atendiendo a los criterios de procesamiento seguro que requiere el análisis forense digital.

Por otro lado, la investigación sobre “Soluciones de seguridad, privacidad y arquitecturas informáticas en la niebla” de [1], además de los estudios de Galarza et al.[2] y el de Álvarez [3], pueden servir para estudiar la problemática de la seguridad informática en los servicios en la nube. Leglisse [4], por su parte, estudió sobre la implementación de algoritmos SHA en arquitecturas ARM. Tito et al.[5] plantea un ejemplo de aplicación de la seguridad de servicios AWS que pueden tomarse como modelo al momento de tener que definir algunas herramientas de Cloud Computing que se necesitarán en los LIF. El estudio de Pourvahab y Ekbatanifard [6] sobre una arquitectura forense digital para la recopilación de pruebas y la preservación de la procedencia en el entorno de la nube de IAAS utilizando tecnología sdn y blockchain también se considera relevante. En [7] se estudian problemas de la seguridad abierta, que también son de interés para la presente investigación.

Respecto de las normas de seguridad informática, una primera base de estudio será el contexto de la Serie 27000 de las ISO/IEC. Además de considerarlas particularmente para la incorporación en el sistema de gestión integrado, será necesario estudiar los inconvenientes o problemática que otros hayan investigado en la aplicación de casos concretos. Así, se puede hacer un estudio comparativo considerando los trabajos de Valencia Duque [8], Armendáriz [9], Tjirare [10] y Meriah [11]. Y respecto de los estudios sobre calidad aplicados al proceso forense digital, se considerarán los trabajos de Di Iorio et al. [12], López [13], Romero Castro[14] y el estudio sobre Controles de Seguridad y Privacidad realizado por el National Institute of Standards and Technology (NIST) [15].

El procedimiento que rige la prueba judicial posee una serie de filtros. En primer lugar, se encuentra el análisis de validez y admisibilidad de un elemento probatorio. La prueba obtenida ilícitamente, y la prueba cuya incorporación en un proceso judicial concreto no es permitida, son excluidas del conjunto del material que luego será valorado. Paralelamente, todo aquello que nada tiene que ver con las cuestiones controvertidas (prueba no pertinente) y lo que

podrá ser probado a través de otros elementos (prueba sobreabundante), también terminará fuera del análisis del tribunal.

Por último, el material probatorio se analiza en cuanto a su confiabilidad, es decir, su aptitud para probar aquello que se pretende probar o esclarecer mediante su incorporación. La confiabilidad está sujeta a dos clases de valoración. La primera es simplemente comparativa (cuál es la prueba más confiable respecto de un punto controvertido), y la segunda se relaciona con el nivel de certeza requerida en cada legislación procesal (estándar probatorio). Es en este ámbito en el cual examina si el origen de una evidencia es comprobable, si la misma no ha sido eliminada o alterada total o parcialmente, y en qué medida todo ello afecta o no el valor probatorio esperado respecto de las cuestiones específicas que esa evidencia estaba destinada a probar.

La admisibilidad de la prueba es una cuestión de carácter práctico, derivado principalmente del accionar legal y jurisprudencial. La prueba está regulada por leyes, interpretadas por los tribunales y en tal sentido las decisiones de los jueces, manifestadas en los fallos de la corte resultan un material de consulta importante, tales como se lee en [16], [17], [18], [19] y [20]

Actividades Centrales

Mediante el correspondiente plan de trabajo que define responsabilidades, recursos y tiempos, el proyecto prevé un conjunto de actividades, que en breve detalle se enuncian a cotinuación:

- Relevamiento: Revisar las normas de gestión y técnicas de ciberseguridad y seguridad de la información vinculadas a las operaciones informático forenses de un laboratorio del ámbito judicial y de un laboratorio externo. Analizar ejemplos de integración de sistemas a partir de la aplicación de la estructura de alto nivel de las normas de sistemas de gestión de acuerdo al Anexo SL.
- Selección: Elaborar un instrumento de selección para analizar la pertinencia y la relevancia de aplicación de normas de acuerdo a los servicios prestados por los LIF, para determinar las normas de gestión y técnicas de ciberseguridad y seguridad de la información que integrarán el sistema integrado.
- Desarrollo de Mapas de Procesos: Elaborar un mapa de procesos orientado a LIF del ámbito judicial y externos.
- Desarrollo de Procesos: Definir y desarrollar los procesos estratégicos, operativos y de soporte necesarios, que permitan la integración de las normas seleccionadas en los LIF del ámbito judicial y externos.
- Elaboración de la Guía Técnica: Elaborar un sistema integrado que incorpore las normas de seguridad de la información al sistema de gestión de calidad en LIF.
- Testeo de la Guía: Validar la Guía técnica en un LIF interno al sistema de justicia y uno externo. Los espacios seleccionados a tal fin son el Laboratorio de Informática Forense del Ministerio Público de la Provincia de Buenos Aires-Departamento Judicial Mar del Plata (LIF-MdP) y el Laboratorio de Informática Forense DigiLab de la Universidad Católica de Salta.
- Adaptación de la Guía: Aplicación de las mejoras encontradas en el ítem 6 para la conformación de la versión final de la Guía.

Estrategias de Sostenibilidad

En este tipo de proyectos interinstitucionales existen metodologías que proponen transitar un proceso de construcción colectiva, en el que los actores involucrados debatan y diseñen alternativas de desarrollo que resulten transformadoras, innovadoras, sustentables y significativas. La metodología conocida como “Potenciar Comunidades” propone diferentes niveles de intervención, definiendo para cada uno una combinación de herramientas de gestión preexistentes y el diseño de modelos propios tendientes a la sostenibilidad del proyecto en el tiempo, más allá de la duración pautada en su formulación inicial. Un ejemplo concreto de esta metodología se analiza en[21]. En el caso particular del proyecto que aquí se presenta, los niveles de intervención son los siguientes:

1) Los ámbitos de la justicia en el que coexisten diferentes expresiones organizativas (Poder Judicial, Ministerio Público, jueces, peritos, entre otros) son fundamentales para motorizar iniciativas. Allí se perciben en profundidad las necesidades y oportunidades y, en muchos casos, por poseer un conocimiento de la cultura local y el entorno, dichas instancias se encuentran legitimadas para considerar el entorno de base para este proyecto;

2) Los ámbitos de la investigación y el desarrollo tecnológico, que también desde sus organizaciones propias (universidades, institutos judiciales, espacios multidisciplinarios de discusión académica), cuentan con recursos y herramientas y están dispuestos a realizar un aporte para el estudio de problemáticas desde diferentes enfoques, atendiendo a criterios que le son propios (la calidad en los procesos del análisis forenses por ejemplo); y
3) Otros ámbitos interesados en el Análisis Forense (profesionales independientes, laboratorios forenses extrajudiciales privados, fuerzas de seguridad nacionales y provinciales), que pueden recurrir a los resultados de este proyecto para su propio crecimiento y desarrollo.

La sostenibilidad del proyecto parte de una estrategia de intervención participativa basada en el abordaje simultáneo de las potencialidades del contexto, las instituciones vinculadas al proyecto y los equipos humanos que las conforman. Las políticas institucionales referentes a la extensión y transferencia de conocimiento de las tres universidades son coincidentes. En concreto, la sostenibilidad se asienta en un conjunto de elementos, entre los que se pueden destacar los siguientes. La vinculación interinstitucional entre UFASTA y UNMDP y entre UCASAL y UFASTA, que se manifiesta en acciones anteriores al proyecto motivo de este trabajo, mostrando una trayectoria de intereses comunes y estrategias de trabajo colaborativo, que se toman como fortalezas institucionales. Cada una, por su parte, está comprometida en la generación de acciones tendientes al desarrollo del proyecto en el tiempo, definiendo las siguientes líneas de continuidad: a) La auto-sustentación del proyecto se logra a través de la capacitación y el desarrollo de habilidades, lo cual permitirá continuar las acciones luego de terminado el proyecto; b) En el caso de los laboratorios forenses extrajudiciales, se prevén actividades de servicios a terceros y asistencia técnica dirigida al ámbito público y privado relacionado a la temática particular de la Informática Forense; c) La capacidad institucional de las universidades participantes, en cuanto a la función sustancial de transferencia del conocimiento, está implementada en la conformación de redes con diferentes entornos, que a su vez, marcan el camino para la maduración de proyectos de este tipo; y d) La característica sustancial de este proyecto -integración de normas de calidad y de ciberseguridad- desarrolla capacidades en el equipo de trabajo y aprendizajes que pueden replicarse en otros ámbitos de aplicación.

Impacto esperado

Fundamentalmente, el proyecto tiene un alto impacto en la admisibilidad y confiabilidad de la evidencia digital. También colabora en el respeto de las garantías procesales y contribuye a evitar demoras en los tiempos procesales.

El principal impacto redundará en mejores prácticas que permitan asegurar la calidad de los procesos en el ámbito de los LIF internos y externos al sistema de justicia, otorgando mejores resultados y la posibilidad de un mejor tratamiento y custodia de la evidencia digital. Es, en este punto propio de la cadena de custodia digital, donde entran especialmente en juego normas de seguridad informática, seguridad de la información y ciberseguridad, para garantizar la integridad de la evidencia digital y evitar un uso ajeno al marco del litigio judicial.

La implementación de un protocolo de actuación en informática forense debe realizarse en ambientes que cuenten con un Sistema Integrado de Gestión de la Calidad que respete los aspectos básicos y garantice las condiciones para su cumplimiento. En todo momento, se debe poder evidenciar y garantizar la calidad de los procesos llevados a cabo en estos laboratorios, y la actualización permanente en el uso de las mejores prácticas forenses, a efectos de fortalecer la prueba digital.

Constituyen destinatarios directos los investigadores judiciales y los peritos informáticos forenses. Los mismos dispondrán de guías que les permitan estudiar y optimizar prácticas de gestión, incluyendo aspectos de calidad e integrando los elementos necesarios para implementar ciberseguridad.

Los beneficiarios indirectos incluyen a todos los LIF, ya que mejorarán su gestión con la aplicación de esta guía. También serán beneficiarios el equipo de investigación, a través de la generación de un equipo interdisciplinario que compartirá saberes, metodologías de trabajo y abordaje de situaciones complejas; y, las universidades participantes, que generarán lazos de trabajo, fortaleciendo sus actividades de ciencia y técnica. Ello a su vez, se seguirá traduciendo en el desarrollo de herramientas que

contribuyan a mejorar la calidad de la resolución de los conflictos judiciales, impactando así de manera positiva y directa en la sociedad.

En general y respecto de los restantes actores del Sistema Nacional de Ciencia, Tecnología e Innovación, este proyecto permitirá la vinculación e interacción con aquellas instituciones que requieran de herramientas científicas y formales para el desarrollo de sistemas integrados de gestión de calidad y ciberseguridad. En particular, es posible sumar aportes de interés para la Red de Laboratorios Forenses de Ciencia y Tecnología del MinCyT.

También el proyecto se vinculará con el Instituto Federal de Innovación, Tecnología y Justicia de la Ju.fe.jus[2] (Junta Federal de Cortes y Superiores Tribunales de Justicia de las Provincias Argentinas y Ciudad Autónoma de Buenos Aires); así como con el Consejo Federal de Procuradores de la República Argentina[3] dependiente del Consejo Federal de Política Criminal. En particular, interesa la vinculación con la Red Nacional de Laboratorios de Ciencias Forenses (perteneciente al Ministerio de Justicia de la Nación), que entendemos es el espacio adecuado para promover este proyecto.

Tanto UCASAL como UFASTA participan de redes institucionales orientadas al estudio e investigación de la informática forense, tales como la Red de Universidades con Investigaciones en Informática Forense (Red UNIF) y la Red Iberoamericana de Investigadores y Docentes en Informática y Derecho (Red CIIDDI). UFASTA integra además la Red Temática de Ciencias Forenses, ámbito interdisciplinario y multisectorial de alcance latinoamericano. En todos estos casos, los eventos académicos anuales que los representan, resultan en el espacio más adecuado para la discusión de los avances y resultados de este proyecto.

Resultados a lograr

Se espera que una vez finalizado el proyecto se cuente con una Guía Técnica para la integración de normas de Ciberseguridad y Seguridad de la Información a un Sistema de Gestión de Calidad en Laboratorios de Informática Forense. Esta guía contempla los procedimientos, instrumentos y herramientas para implantar un Sistema Integrado de Gestión de la Calidad, Ciberseguridad y Seguridad de la Información requeridas en los LIF judiciales y externos. El conocimiento contenido en la Guía podrá hacerse extensivo a laboratorios de otros organismos.

Esta guía técnica pretende, además, complementar e integrar la Guía Técnica para la Implementación de un Sistema de Gestión de Calidad en Laboratorios de Informática Forense, la Guía Integral de Empleo de la Informática Forense en el proceso penal y a la Guía Técnica para el Diseño, Implementación y Gestión de Laboratorios de Informática Forense Judiciales, adoptados por el Ministerio Público de la Provincia de Buenos Aires.

4) CONCLUSIONES

El desarrollo de un Sistema Integrado de Gestión de la Calidad en LIF permitirá integrar las cuestiones fundamentales para el abordaje de la problemática de calidad, la gestión del riesgo y la ciberseguridad dentro de las temáticas más relevantes a partir del uso de la estructura de alto nivel definida en el Anexo SL de la ISO.

Las universidades están comprometidas en llevar adelante este proyecto. No obstante, los recursos financieros solicitados en el marco de un proyecto PITE, serán de interés para fortalecer y acelerar el desarrollo de esta propuesta.

El potencial de la articulación interinstitucional se sustenta en los recursos humanos que conforman los grupos de I+D+i que participan del proyecto, además del abordaje de las temáticas que cada grupo tiene a su cargo y que conforman el *corpus* del marco teórico y práctico del proyecto.

Por otra parte, se esperan beneficios intangibles relacionados a la actividad conjunta interinstitucional, logrados a partir del espacio de comunicación y trabajo colaborativo entre los equipos de investigadores de cada parte, y así promover la capacidad madurativa de los recursos humanos involucrados, y del entorno de interacción que cada institución debe desarrollar a la par del proyecto.

Asimismo, el trabajo de este equipo permitirá generar mayores lazos entre las universidades intervinientes. A partir de la experiencia de este proyecto, se podrá avanzar hacia el abordaje de problemáticas afines o en otras áreas donde las instituciones se desempeñan.

[2] http://www.jufejus.org.ar/
[3] http://www.consejompra.org/

REFERENCIAS

[1] W. Shafik and S. A. Mostafavi, “Fog Computing Architectures, Privacy and Security Solutions,” *J. Commun. Technol. Electron. Comput. Sci. Issue*, vol. 24, no. 24, 2019.

[2] B. Galarza, G. Zaccardi, M. Belizán, D. Duarte, M. Morales, and D. Encinas, “Performance de Cloud Computing para HPC: Despliegue y Seguridad,” pp. 984–987, 2018.

[3] J. F. Alvarez, “Las necesidades de la seguridad en la nube,” 2019.

[4] A. Francisco, D. A. Leglisse, and G. G. García, “IMPLEMENTACIÓN DE LA FUNCIÓN SHA3-3 EN UNA ARQUITECTURA ARM Resumen,” vol. 39, no. 04, pp. 187–204, 2017.

[5] E. Tito, E. Alarcón Ayquipa, and L. Apaza Quispe, ““IMPACTO DE LA IMPLEMENTACIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE AMAZON WEB SERVICES EN EL SISTEMA DE RECURSOS HUMANOS DE FRACTAL SAC LIMA,” *Univ. Científica del Sur*, pp. 1–40, 2019.

[6] M. Pourvahab and G. Ekbatanifard, “Digital Forensics Architecture for Evidence Collection and Provenance Preservation in IaaS Cloud Environment Using SDN and Blockchain Technology,” *IEEE Access*, vol. 7, pp. 153349–153364, 2019.

[7] M. Caprolu, R. Di Pietro, F. Lombardi, and S. Raponi, “Edge Computing Perspectives: Architectures, Technologies, and Open Security Issues,” *Proc. - 2019 IEEE Int. Conf. Edge Comput. EDGE 2019 - Part 2019 IEEE World Congr. Serv.*, no. July, pp. 116–123, 2019.

[8] F. J. Valencia-Duque and M. Orozco-Alzate, “A methodology for implementing an information security management system based on the family of ISO/IEC 27000 standards,” *RISTI - Rev. Ibèrica Sist. e Tecnol. Inf.*, no. 22, pp. 73–88, 2017.

[9] D. N. López Armendáriz, “Modelo de gestion de los servicios de tecnologia de informacion basado en COBIT, ITIL e ISO/IEC 27000,” *Rev. Tecnológica - ESPOL*, vol. 30, no. 1, pp. 51–69, 2017.

[10] D. J. Tjirare and F. B. Shava, “A gap analysis of the ISO/IEC 27000 standard implementation in Namibia,” *2017 IST-Africa Week Conf. IST-Africa 2017*, pp. 1–10, 2017.

[11] I. Meriah and L. B. A. Rabai, “Comparative study of ontologies based iso 27000 series security standards,” *Procedia Comput. Sci.*, vol. 160, pp. 85–92, 2019.

[12] A. Di Iorio, S. Lamperti, L. Coppes, and B. Constanzo, “Guía técnica para el diseño de laboratorios judiciales de informática forense,” no. June, 2019.

[13] R. A. López, *Sistema de Gestión de la Seguridad*. 2017.

[14] M. I. Romero Castro *et al.*, *Introducción a la seguridad informática y el análisis de vulnerabilidades*. 2018.

[15] NIST SP800-53, “Security and privacy controls for federal information systems and organizations,” *NIST Spec. Publ.*, vol. 800, p. 53, 2013.

[16] Instituto de Investigaciones (Corte Suprema de Justicia de la Nacion), “Corte Suprema de Justicia de la Nación: C. 1757. XL. RECURSO DE HECHO Casal, Matías Eugenio y otro s/ robo simple en grado de tentativa Ccausa N° 1681C.,” pp. 1–62, 2005.

[17] D. Accatino, “Certezas, dudas y propuestas en torno al estándar de la prueba penal,” *Rev. derecho*, no. 37, pp. 483–511, 2011.

[18] M. Gascón Abellán, “Prueba científica: un mapa de retos,” *Estándares prueba y prueba científica. Ensayos Epistemol. jurídica*, pp. 181–201, 2013.

[19] M. Gascón Abellán, J. J. Lucena Molina, and J. González Rodríguez, “Razones científico-jurídicas para valorar la prueba científica: una argumentación multidisciplinar,” *D. la Ley*, vol. 31, no. 7481, pp. 1–11, 2010.

[20] C. Vázquez-Rojas, “Sobre la cientificidad de la prueba científica en el proceso judicial,” *Anu. Psicol. Juridica*, vol. 24, no. 1, pp. 65–73, 2014.

[21] N. Morales Heriberto, N. de la P. J. Pablo, and G. G. Jaime, “Siete Conceptos Clave Para Potenciar Iniciativas De Proyectos Basados En Creación De Valor Compartido E Innovación Social,” *Mem. del IX Congr. la Red Int. Investig. en Compet.*, pp. 210–225, 2015.