A. PROPUESTA PROYECTO DE INVESTIGACIÓN INTERNO SIN FINANCIAMIENTO O AUTOGESTIONADO

1. TIPO DE INVESTIGACIÓN

Básica		**Aplicada**	**x**

2. UNIDAD EJECUTORA

1. Departamento de Informática y Ciencias de Computación

3. LINEA(S) DE INVESTIGACIÓN:

1. Sistemas de Información

2. Seguridad y Privacidad

4. TÍTULO DEL PROYECTO *(mínimo 10 palabras):*

Uso de técnicas de minería de datos para la prevención y detección de ataques a bases de datos por inyección de código SQL

5. RESUMEN *(máximo **200** palabras)*

Muchas empresas actualmente realizan sus operaciones a través de internet usando sitios web de comercio electrónico. La información personal de clientes y de operaciones de la empresa es en general ingresada y consultada usando aplicaciones web que trabajan con información almacenada en bases de datos [1]. La confidencialidad de la información y su integridad no siempre están garantizadas, pues las aplicaciones web son vulnerables a accesos no autorizados y pueden exponer los datos almacenados a ataques de diferentes tipos [2]. Las pérdidas de las empresas por ataques a bases de datos pueden ser muy altas, como las reportadas por PaketLabs en el 2018 indicando perjuicios en miles de millones de dólares [3]. Un tipo especial de ataque se produce por inyección de código SQL, permitiendo al atacante ejecutar instrucciones que afectan a las bases de datos [4]. Existen algunas soluciones para la detección y prevención de este tipo de ataques, sin embargo, estas soluciones no integran técnicas de minería de datos para la prevención y detección de ataques de inyección SQL [5].

Dado este escenario de evolución de distintas amenazas, los centros de respuesta a incidentes de seguridad (CSIRT, por las siglas en inglés de Computer Security Incident Response Team) están cobrando relevancia y poniendo atención en este tipo de ataques [6]. En este sentido, el presente proyecto propone desarrollar un agente de software para prevenir y detectar ataques de inyección de código SQL a base de datos usando estrategias innovadoras, tales como técnicas de minería de datos, priorización de ataques, entre otros. Como caso de prueba se trabajará con un Centro de Respuesta a Incidentes de Seguridad Informática de una institución pública que tenga como finalidad brindar servicios de seguridad a las infraestructuras críticas de TI (Tecnologías de la Información) de la institución, contribuyendo así al desarrollo de la ciberseguridad del Ecuador.

6. PALABRAS CLAVE *(4-6)*

Inyección código SQL, Ataques a bases de datos, Seguridad de bases de datos, data mining, minería de datos.

7. OBJETIVOS

7.1. OBJETIVO GENERAL

Usar de técnicas de minería de datos para la prevención y detección de ataques a bases de datos por inyección de código SQL.

7.2. OBJETIVOS ESPECÍFICOS

a. Realizar un estudio sistemático de trabajos relacionados para identificar los principales ataques de inyección de código SQL.

b. Explorar y comparar las técnicas y herramientas de minerías de datos existentes para identificar las más adecuadas para la predicción de ataques SQL a bases de datos.

c. Desarrollar un agente de software que utilice modelos de minería de datos para la detección y prevención de ataques SQL.

d. Verificar y validar el agente de software para detección y prevención de ataques SQL en un centro de respuesta a incidentes de seguridad informática.

e. Documentar y comunicar los resultados obtenidos.

8. HIPÓTESIS *(opcional)*

a. Se pueden detectar y predecir los ataques de inyección SQL más comunes a las bases de datos de aplicaciones web mediante un agente de software que utiliza técnicas de minería de datos.

9. DETALLE DE LOS RESULTADOS ESPERADOS *(con relación a los objetivos)*

a. Un estudio de publicaciones relacionadas con la investigación.

b. Un agente de software la detección y prevención de ataques más comunes a bases de datos

c. Las conclusiones de la evaluación del caso de prueba

d. Una o varias publicaciones en congresos o revistas científicas.

10. IMPACTO DE LA INVESTIGACIÓN (*científico, social, económico u otros)*

10.1 Impacto Social

Continuamente se presentan estudios relacionados con ataques a bases de datos que originan perjuicios importantes a las instituciones y a los dueños de los datos almacenados [7]. Un adversario de una institución o empresa podría robar informaciones sensibles almacenadas en las bases de datos, tales como credenciales de usuarios, secretos comerciales o registros de transacciones, por lo que es importante desarrollar e implementar mecanismos de control [8]. En el sector de la salud, también se maneja información altamente sensible relacionada con los pacientes, su estatus socioeconómico, diagnósticos, tratamientos médicos, información que debe ser protegida [9]. En esta época de pandemia, muchas instituciones y organizaciones han optado por el teletrabajo, por lo que la implementación de los controles de seguridad y

mecanismos de prevención de ataques son de gran importancia. A través de la prevención y detección de ataques SQL a bases de datos, el presente proyecto ayudará a evitar la pérdida de la privacidad de los datos almacenados, brindado de esta manera confianza a los usuarios en el uso de sistemas y tecnologías.

10.2 Impacto Económico

El presente proyecto contribuirá a disminuir los efectos negativos de ataques a bases de datos, como son fraudes, pérdidas y costos de recuperación de información. Existen estudios, principalmente realizados por firmas consultoras de seguridad, que han reportado pérdidas de millones de dólares por ciberataques a bases de datos de sus clientes [10]. Es el caso del hotel Marriot internacional, que sufrió daños en el 2018 por miles de millones de dólares por esta causa. Los autores en [11] presentan numerosos reportes de robos de información de tarjetas de crédito y de información de clientes y productos con impactos en costos, en los seguros y en las bolsas de valores, especialmente en industrias relacionadas con el comercio, el turismo y con el sector hospitalario. Algunas compañías de seguros han decidido no cubrir los riesgos derivados por los ciberataques debido a la frecuencia de los mismos, aunque el impacto macroeconómico no sea muy alto por el período corto de actuación de los ataques antes de ser detectados [12]. Estudios recientes de ciberseguridad han reportado que las instituciones de gobierno y de administración pública están entre las industrias principales que experimentan intentos de ciberataques destructivos [13]. Además, estos estudios indican que el punto de entrada principal de los ataques son las aplicaciones web, las cuales tienen varias vulnerabilidades inherentes las mismas que son utilizadas para lanzar varios tipos de ataques, entre los más comunes los de inyección SQL. Por lo tanto, se requieren soluciones informáticas que permitan detectar y prevenir este tipo de ataques para evitar pérdidas económicas especialmente en este tipo de instituciones.

10.3 Impacto Político

Los ataques a bases de datos han tenido un alto impacto en la seguridad y privacidad de la información que mantienen los estados. Las tecnologías digitales que existen actualmente permiten implementar sistemas de monitoreo mediante cámaras, sistemas de posicionamiento global, escáneres corporales, tecnologías biométricas y otras que recogen información privada de personas y eventos con fines de seguridad. Por otra parte, los estados también almacenan información de comunicaciones oficiales y documentos relacionados muchos de ellos de carácter reservado. Esta información reservada al ser obtenida y difundida origina un gran impacto político como sucedió con el portal WikiLeaks en el que se difundió información considerada de seguridad nacional por gobierno de Estados Unidos [14]. Por estas razones, la información debe ser protegida con los controles adecuados para detectar y prevenir ataques a bases de datos.

La investigación contribuirá a mejorar la relación Universidad – Estado elaborando un agente de software que utilice técnicas de minería de datos para la detección y prevención de ataques SQL y que pueda ser utilizada por varias instituciones en sus centros de detección de incidentes de seguridad informática.

10.4 Impacto Científico

El presente proyecto para la prevención y detección de ataques SQL a bases de datos permitirá investigar trabajos relacionados con la aplicación de técnicas de minería de datos en este campo

y realizar una propuesta que ayudará a los centros de respuesta a incidentes de seguridad a realizar mejor su trabajo. Los resultados de la investigación permitirán elaborar publicaciones en congresos y o revistas con impacto científico.

11. INVESTIGACIONES PREVIAS DEL EQUIPO *(máximo tres carillas)*

Ordóñez, P. J., & Hallo, M. (2020). Detection of Taxpayers with High Probability of Non-payment: An Implementation of a Data Mining Framework. In 15ª Conferência Ibérica de Sistemas y Tecnologías de Información (CISTI2020).

Ordóñez, P. J., & Hallo, M. (2019, April). Data Mining Techniques Applied in Tax Administrations: A Literature Review. In 2019 Sixth International Conference on eDemocracy & eGovernment (ICEDEG) (pp. 224-229). IEEE.

Hallo, M., Escobar, M., & Luján-Mora, S. (2018, March). Automatic Extraction and Management of Open Access Bibliographic Information. In 2018 IEEE World Engineering Education Conference (EDUNINE) (pp. 1-5). IEEE.

Suntaxi, G., El Ghazi, A. A., & Böhm, K. (2021). Secrecy and performance models for query processing on outsourced graph data. Distributed and Parallel Databases, 39(1), 35-77.

Suntaxi, G., Ghazi, A. A. E., & Böhm, K. (2020). Preserving secrecy in mobile social networks. ACM Transactions on Cyber-Physical Systems, 5(1), 1-29.

Suntaxi, G., El Ghazi, A. A., & Böhm, K. (2019, May). Mutual authorizations: Semantics and integration issues. In Proceedings of the 24th ACM Symposium on Access Control Models and Technologies (pp. 213-218).

12. DESCRIPCIÓN DETALLADA DEL PROYECTO, INCLUIDO ESTADO DEL ARTE; METODOLOGÍA *(máximo tres carillas)*

Las empresas u organizaciones están expuestas a ataques a bases de datos una vez que publican su acceso por Internet, especialmente aplicaciones y servicios web [15]. Los impactos sociales, políticos y financieros consecuencia de estos ataques son muy importantes, debido a la pérdida de información de clientes, secretos comerciales, registros de transacciones, documentación clasificada, entre otros [16]. En este sentido, es un objetivo primordial el buscar soluciones para salvaguardar la seguridad, privacidad e integridad de la información, los cuales deben ser protegidas con medidas adecuadas de detección y prevención de ataques a bases de datos.

Existen varias formas de comprometer la seguridad de una base de datos: exploración de contraseñas, configuraciones débiles y servicios no usados e innecesarios en los sistemas, inyección de código SQL [17], uso de malware, explotación de vulnerabilidades, incorrecta gestión de la base de datos [18], robo de archivos de respaldo no encriptados, entre otros [18, 19]. En este sentido, los ataques por inyección de código SQL continúan siendo una de las principales amenazas, en especial para aplicaciones Web [21].

La inyección de código SQl es un ataque en el cual se inserta código SQL a los parâmetros de una aplicación y se pasa a un servidor SQL en el que se realiza el parsing y ejecución de la sentencia. Cualquier procedimento que construye sentencias SQL podría ser vulnerable si no se toman las medias de prevención adecuadas. Los ataques pueden darse desde aplicaciones Web, aplicaciones móviles o aplicaciones de escritorio. Al implementar la inyección de código SQL los atacantes pueden ganar acceso no autorizado a las bases de datos obteniendo, removiendo o cambiando los datos en forma fraudulenta y delictiva comprometiendo la funcionalidad de las aplicaciones, la confidencialidad, integridad y privacidad de los datos [22].

Además de la continua actualización y corrección de problemas por parte de los proveedores de software, en los últimos años se han propuesto diferentes estrategias para la detección y prevención de este tipo de ataques. En [23], los autores proponen soluciones basadas en búsqueda de patrones de ataques o detección de anomalías del comportamiento normal de los sistemas. Por su parte, los autores en [24] proponen AMNESIA como técnica que combina análisis estático y dinámico para detección y prevención de vulnerabilidades. AMNESIA permite interpretar y validar las solicitudes SQL de forma independiente antes de enviarlas a la base de datos. Por otro lado, se desarrolla SAFELI [25] , una herramienta que analiza el código fuente para detectar ataques de inyección SQL. Sin embargo, el análisis se realiza durante el tiempo de compilación, por lo que no se puede considerar en tiempo real. SQL Prevent [26] utiliza un sniffer (analizador de protocolos) que intercepta tráfico HTTP y descubre operaciones SQL en servicios web. Posteriormente el sistema analiza dichas solicitudes, identifica y bloquea a todas aquellas que son etiquetadas como amenaza. Soluciones adicionales utilizan algoritmos de inteligencia artificial para optimizar la detección de operaciones SQL maliciosas que circulan en la red [27] . Todas estas soluciones se implementan de forma independiente y no existe una hoja de ruta común para homologar las diferentes acciones de detección y prevención de este tipo de ataques. Por otra parte cada vez aparecen nuevas formas de ataques a bases de datos que requieren nuevos estudios.

El presente proyecto propone el desarrollo de un agente de software que integre actividades de prevención y detección de ataques a bases de datos por inyección de código SQL más comunes. Además, el desarrollo del agente de software contemplará la implementación mediante un caso de prueba utilizando nuevas estrategias, tales como técnicas de minería de datos para identificar comportamientos atípicos en el log de transacciones.

METODOLOGIA

Para el desarrollo del proyecto se utilizará la metodología de modelado de diseño de investigación científica DSR por las siglas en inglés de Design Science Research [28] . La metodología propuesta enfoca sus esfuerzos en la creación de nuevo conocimiento a partir del análisis de fenómenos existentes, con el fin de determinar su razón de ser y otorgar artefactos o herramientas para su interpretación. El diseño de una investigación científica, se define como el conjunto de técnicas utilizadas por un investigador para desarrollar nuevas tecnologías para resolver problemas. Además, se utilizará una adaptación de la metodología **CR**oss **I**ndustry **S**tandard **P**rocess for **D**ata **M**ining (*CRISP-DM*), la cual es una metodología utilizada en proyectos de minería de datos. Esta metodología será incorporada dentro de las fases de la metodología de investigación científica DSR.

Los principales pasos de la metodología SDR son:

1. ***Identificar el problema***

En esta fase se identificarán los principales ataques de inyección de código SQL por medio de un estudio sistemático de trabajos relacionados, siguiendo la metodología de Kitchenham [29]. De igual manera, se investigarán las estrategias más relevantes de identificación y mitigación a estos ataques. Finalmente, con la información obtenida, se especificarán los requisitos de diseño que permita integrar adecuadamente las estrategias encontradas en un agente de software..

2. Diseñar la solución

En esta etapa se elaborarán los procedimientos y modelos que permitirán satisfacer los requisitos del agente de software. Con este fin, se definirán a alto nivel las actividades, productos de trabajo (entradas y salidas), roles y técnicas de pruebas a desarrollar, tomando en cuenta el análisis previo de literatura enfocados en prevención y detección de ataques de inyección SQL a bases de datos.

3. Desarrollar la solución

En esta etapa el diseño propuesto será implementado, obteniendo como salida una versión del agente de software que utilice modelos de minería de datos para la detección y prevención de ataques de inyección SQL. En el caso de ser necesario se definirá el diseño, por ejemplo, cuando se requiere considerar requisitos adicionales. En este sentido, el proyecto para desarrollar el modelo seguirá una adaptación de la metodología CRISP-DM. Esta metodología contempla las siguientes fases:

- Comprensión del negocio: en esta fase se definen los objetivos y requisitos del proyecto y se convierte este conocimiento en un problema de minería de datos.
- Estudio y comprensión de los datos: se ocupa de recolectar datos iniciales que sean de calidad y permitan un acercamiento con el problema. Además, se realiza una descripción, exploración y verificación de los datos obtenidos para descartar datos innecesarios que impidan construir un conjunto de datos finales.
- Análisis de los datos y selección de características: consiste en preparar, seleccionar, limpiar, integrar, normalizar los datos obtenidos, de tal manera que los datos estén acorde a un formato apropiado para la técnica de minería de datos que se utilizará en pasos posteriores.
- Modelado: en esta fase se selecciona la técnica de modelamiento adecuada para el proyecto de minería de datos que se está desarrollando. Además, se cubre tareas como la generación del plan de prueba y construcción del modelo.
- Evaluación: consiste en evaluar el modelo efectuado en pasos anteriores. Además, se mide si se cumplieron de manera correcta los objetivos del negocio y evalúa los resultados obtenidos.
- Despliegue: en esta fase se realiza la planificación del despliegue del modelo, generación de reportes, revisiones del proyecto y sus mejoras a futuro.

Ejecutar, verificar y validar

En esta etapa el agente de software desarrollado será evaluado según lo establecido en el objetivo del proyecto. De este modo, se asegura que el agente de trabajo presentado tendrá la funcionalidad planteada inicialmente. Con este fin, la solución presentada será probada en un Centro de Respuesta a Incidentes de Seguridad Informática de una institución pública con una base de datos de una aplicación en funcionamiento.

4. Comunicar los resultados de la investigación

Esta fase permitirá comunicar los resultados y contribuciones del trabajo realizado a la comunidad científica. El agente de software será desarrollado de forma iterativa e incremental y los resultados serán publicados al menos en un artículo de una revista indexada y/o en un congreso internacional. De este modo, el agente de software quedará disponible para nuevas implementaciones y trabajos futuros.

Referencias Bibliográficas

[1] Singh M. (2015) Information Exploration in E-Commerce Databases. In: Kumar N., Bhatnagar V. (eds) Big Data Analytics. BDA 2015. Lecture Notes in Computer Science, vol 9498. Springer, Cham. https://doi.org/10.1007/978-3-319-27057-9_3.

[2] Kulkarni, S., & Urolagin, S. (2012). Review of Attacks on Databases and Database SecurityTechniques. International Journal of Emerging Technology and Advanced Engineering, 2(11), 253-263.

[3] PacketLabs (2018). How does SQL Injection impact customers?, https://www.packetlabs.net/sql-injection/

[4] Kar, D., & Panigrahi, S. (2013). Prevention of SQL Injection attack using query transformation and hashing. In 2013 3rd IEEE International Advance Computing Conference (IACC) (pp. 1317-1323). IEEE.

[5] Kumar, P., & Pateriya, R. K. (2012, July). A survey on SQL injection attacks, detection and prevention techniques. In 2012 Third International Conference on Computing, Communication and Networking Technologies (ICCCNT'12) (pp. 1-5). IEEE.

[6] Vasilomanolakis, E. (2019). Network entity characterization and attack prediction. Future Generation Computer Systems, 97, 674-686. Commerce databases. In International Conference on Big Data Analytics (pp. 41-56). Springer, Cham.

[7] VJTI, M. (2013). E-commerce applications: Vulnerabilities, attacks and countermeasures. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2(2).

[8] Bamrara, A. (2015). Evaluating database security and cyber attacks: A relational approach. The Journal of Internet Banking and Commerce, 20(2).

[9] Moreira, Q., & Alexander, M. (2019). Estudio de la seguridad de la información de los pacientes en los hospitales públicos tipo ii de ecuador (Master's thesis).

[10] Cashell, B., Jackson, W. D., Jickling, M., & Webel, B. (2004). The economic impact of cyber-attacks. Congressional research service documents, CRS RL32331 (Washington DC), 2.

[11] Arcuri, M. C., Gai, L., Ielasi, F., & Ventisette, E. (2020). Cyber attacks on hospitality sector: stock market reaction. Journal of Hospitality and Tourism Technology.

[12] Haislip, J., Kolev, K., Pinsker, R., & Steffen, T. (2019). The economic cost of cybersecurity breaches: A broad-based analysis. In Workshop on the Economics of Information Security (WEIS) (pp. 1-37).

[13] Symantec. (2015). 2015 Internet Security Threat Report 20. Recuperado Agosto 28, 2021, de https://docs.broadcom.com/doc/istr-15-april-volume-20-en [14] Tambini, D. (2013). WikiLeaks, National Security and Cosmopolitan Ethics. In Ethics of media (pp. 232-254). Palgrave Macmillan, London.

[15] Ping, C. (2017). A second-order SQL injection detection method. IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), (págs. 1792-1796). Chengdu.

[16]Racciatti, H. M. (2002). Técnicas de SQL Injection: un Repaso. https://www.redeszone.net/content/uploads/Tecnicas-de-SQL-Injection.pdf

[17] Sermpinis, T. (2017). Web Application Hacking Advanced SQL Injection and Data Store Attacks. Warszawa, Polonia: Hacking Media Sp. z o.o.

[18] Malik, M., & Patel, T. (2016). Database Security - Attacks and Control Methods. International Journal of Information Sciences and Techniques. https://doi.org/10.5121/ijist.2016.6218

[19] Thusoo, A., & Jethava, G. B. (2015). A Survey: Intrusion detection system for database using data mining techniques. 8.

[20] Coffin Murray, M. (2010). Database Security: What Students Need to Know. Journal of Information Technology Education: Innovations in Practice. https://doi.org/10.28945/1132

[21] Boyd, S. W., & Keromytis, A. D. (2004, June). SQLrand: Preventing SQL injection attacks. In International Conference on Applied Cryptography and Network Security (pp. 292-302). Springer, Berlin, Heidelberg.

[22] Kamtuo, K., & Soomlek, C. (2016, December). Machine Learning for SQL injection prevention on server-side scripting. In 2016 International Computer Science and Engineering Conference (ICSEC) (pp. 1-6). IEEE.

[23] Costante, E., Fauri, D., Etalle, S., Den Hartog, J., & Zannone, N. (2016, May). A hybrid framework for data loss prevention and detection. In 2016 IEEE Security and Privacy Workshops (SPW) (pp. 324-333). IEEE

[24] W. G. J. Halfond and A. Orso, "Preventing SQL injection attacks using AMNESIA," presented at the Proceedings of the 28th international conference on Software engineering (ICSE), ACM, Shanghai, China, Pages: 795-798, May 20–28, 2006, 2006.

[25] X.Fu, X. Lu, B. Peltsverger, S. Chen, G. Southwestern, K. Qian, and S. Polytechnic, “A Static Analysis Framework For Detecting SQL Injection Vulnerabilities” 31st Annual International Computer

[26] P.Grazie., PhD, “SQL Prevent thesis”, University of British Columbia (UBC) Vancouver, Canada, 2008.

[27] E. Stalmans and B. Irwin, “A framework for DNS based detection and mitigation of malware infections on a network”, IEEE Information Security South Africa, Johannesburg, pages. 1–8, 2011.

[28] Wirth, R., & Hipp, J. (2000, April). CRISP-DM: Towards a standard process model for data mining. In Proceedings of the 4th international conference on the practical applications of knowledge discovery and data mining (pp. 29-39). London, UK: Springer-Verlag.

[29] Kitchenham, O. P. Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering – a systematic literature review,” Information and Software Technology, vol. 51, no. 1, pp. 7 – 15, 2009.

13. INFRAESTRUCTURA Y EQUIPOS

Equipos	
Nombre del Recurso	**Ubicación del Recurso**
Computadora portátil EPN	Domicilio en teletrabajo
Computadora portátil colaboradores	Domicilio en teletrabajo
Bases de datos científicas ACM, IEEE, Google scholar, Scopus	Web
Datos de prueba del CIRST-EPN y o institución pública alternativa	DGIP

B. DATOS INFORMATIVOS

1. INFORMACIÓN DEL DIRECTOR, COLABORADORES Y COLABORADORES TÉCNICOS

Apellidos y nombres	No. de Cédula	HSS*	Departamento**	Rol	Título de mayor nivel y mención.
Hallo Carrasco María	1801087147	8	DICC	Director	PhD
Suntaxi Gabriela	1716583958	4	DICC	Colaborador	PhD

*HSS =Horas Semana Semestre: Es el número de horas que se dedica por semana a la investigación.

** En el caso de que los colaboradores sean de otro departamento se debe adjuntar el aval de las horas de dedicación del Jefe de Departamento.

C. DECLARACIÓN FINAL
DECLARACIÓN DEL DIRECTOR DEL PROYECTO

El equipo de investigadores, representado por el Director del Proyecto declara lo siguiente:

- Que el presente proyecto es una creación original de mi autoría y del equipo de investigadores, y por tanto asumimos la completa responsabilidad legal en caso de que un tercero alegue la titularidad de los derechos intelectuales del proyecto, exonerando a la EPN de cualquier acción legal que se derive por esta causa.

- Que el presente proyecto no ha sido presentado en ninguna convocatoria de otra institución pública o privada. El incumplimiento será causal para que el proyecto no sea tomado en consideración.

- Que si el proyecto genera algún producto o procedimiento susceptible de obtener derechos de propiedad intelectual, de los cuales se deriven beneficios, aceptamos que éstos serán compartidos entre los investigadores y la institución o las instituciones participantes en el proyecto, conforme a lo establecido en el COESC.

- Que el equipo de investigadores y/o instituciones participantes se comprometen a mantener la confidencialidad de la información si ésta podría ser susceptible de protección por patentes, y solicitar la valoración de propiedad intelectual respectiva previa a cualquier publicación o difusión.

- Que para el caso de derechos de autor otorgamos una licencia de uso exclusivo con fines académicos para la o las instituciones participantes en el proyecto.

- Que aceptamos conocer y cumplir con la normativa vigente para la gestión de proyectos.

Firma del Director del Proyecto
Nombre: María Hallo
C.I.:1801087147

ESCUELA POLITÉCNICA NACIONAL

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y VINCULACIÓN

Proyecto de Investigación Interno

CRONOGRAMA DE ACTIVIDADES DEL PROYECTO

Título del Proyecto: Uso de técnicas de minería de datos para la prevención y detección de ataques a bases de datos por inyección de código SQL

AÑO 1

Nº	Actividad	Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6				Mes 7				Mes 8				Mes 9				Mes 10				Mes 11				Mes 12			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Realizar el estudio de trabajos relacionados con la investigación.																																															
1,1	Revisión bibliográfica	x	x	x	x	x	x	x	x																																								
2	Desarrollar un agente de software para la prevención y detección de ataques a bases de datos priorizando los más comunes																																															
2,1	Delimitación del problema					x	x																																									
2,2	Diseño del agente de software							x	x	x	x	x	x	x																																			
2,3	Desarrollo y pruebas											x	x	x	x	x	x	x	x	x	x	x	x	x																							
3	Implementación																					x	x	x	x	x	x	x	x	x	x	x	x	x															
3,1	Evaluación																													x	x	x	x	x	x	x	x												
4	Publicación de los resultados de la investigación																											x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x				
5	Documentación							x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x