PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

ESMERALDAS

ESCUELA DE INGENERÍA DE SISTEMAS Y COMPUTACIÓN

INFORME ESTUDIO DE CASO:

ANÁLISIS DE LAS VULNERABILIDADES EN GESTORES DE BASE DE DATOS UTILIZANDO EL DOMINIO "CONTROL DE ACCESO" DE ISO 27002

LÍNEA DE INVESTIGACIÓN:

GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN

PREVIO A LA OBTENCIÓN DEL TITULO DE:

INGENIERO EN SISTEMAS Y COMPUTACIÓN

AUTOR:

CAICEDO ALCIVAR ALEXANDER ROMARIO

ASESOR:

MGT. PATIÑO ROSADO SUSANA GABRIELA

Esmeraldas, marzo del 2018

Estudio de caso aprobado luego de haber dado cumplimiento a los requisitos exigidos, previo a la obtención del título de INGENIERO DE SISTEMAS Y COMPUTACIÓN.

TRIBUNAL DE GRADUACIÓN

Título: "ANÁLISIS DE LAS VULNERABILIDADES EN GESTORES DE BASE DE DATOS UTILIZANDO EL DOMINIO "CONTROL DE ACCESO" DE ISO 27002"

Autor: ALEXANDER ROMARIO CAICEDO ALCÍVAR

Mgt. Susana Patiño **f.-** .....
Asesor/a

Mgt. Wilson Gustavo Chango **f.-** .....
Lector #1

Mgt. Jaime Sayago Heredia **f.-** .....
Lector #2

Mgt. Xavier Quiñónez Ku **f.-** .....
Director de Escuela

Ing. Maritza Demera Mejía **f.-** .....
Secretaria General PUCE - Esmeraldas

Esmeraldas, Ecuador, marzo del 2018

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo ALEXANDER ROMARIO CAICEDO ALCIVAR, portador de la cédula de identidad No. 080246899-1 declaro que los resultados obtenidos en la investigación que presento como informe final, previo a la obtención del título de "Ingeniero de Sistemas y Computación" son absolutamente originales, auténticos y personales.

En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto de investigación y luego de la redacción de este documento son y serán de mi sola, exclusiva responsabilidad legal y académica.

……..…….....

Alexander Romario Caicedo Alcivar

C.I. 080246899-1

CERTIFICACIÓN

MGT. Susana Patiño Docente investigador de la PUCESE, certifica que:

El estudio de caso realizado por ALEXANDER ROMARIO CAICEDO ALCIVAR bajo el título "ANALISIS DE LAS VULNERABILIDADES EN GESTORES DE BASE DE DATOS UTILIZANDO EL DOMINIO "CONTROL DE ACCESO" DE ISO 27002" reúne los requisitos de calidad, originalidad y presentación exigibles a una investigación científica y que han sido incorporadas al documento final, las sugerencias realizadas, en consecuencia, está en condiciones de ser sometida a la valoración del Tribunal encargada de juzgarla.

Y para que conste a los efectos oportunos, firma la presente en Esmeraldas, marzo del 2018.

MGT. Susana Patiño.
Asesora

DEDICATORIA

Este trabajo de investigación se lo dedico a mis padres, por todo su esfuerzo y sacrificio, por la confianza brindada, por ser parte fundamental en todo el camino de mi carrera universitaria. A mis hermanos por estar conmigo y acompañarme en cada momento.

AGRADECIMIENTO

En primer lugar, a Dios por haberme guiado por el buen camino hasta ahora; en segundo lugar, a cada uno de los que son parte de mi familia a mis padres y hermanos; por siempre haberme dado su fuerza y apoyo incondicional que me han ayudado y llevado hasta donde estoy ahora.

Agradezco infinitamente a mi querida asesora por guiarme de la mejor manera en mi investigación, por la paciencia que me tuvo y por brindarme sus conocimientos. También agradezco a mis lectores por las observaciones realizadas a mi Estudio de Caso, las cuales ayudaron a la mejora del mismo.

Por último, agradecer a cada uno de mis compañeros y amigos de clases por el apoyo brindado a lo largo de la universidad.

Resumen

La presente investigación se la realizó con el objetivo de analizar las vulnerabilidades de los gestores de bases de datos de las instituciones Pontificia Universidad Católica Sede Esmeraldas y el Gobierno Autónomo Descentralizado de la Prefectura de Esmeraldas. Se desarrolló una lista de chequeo basándose en la ISO 27002 el dominio "Control de Acceso" complementándose con el nivel de madurez del CMMI para determinar el nivel de los gestores de bases de datos de las instituciones involucradas en el estudio. La metodología empleada fue de tipo cuantitativo y para el levantamiento de la información se utilizaron las técnicas de entrevista, observación y prueba, para la cual se empleó la herramienta SqlMap. Las preguntas de la lista de chequeo fueron agrupadas de acuerdo con sus objetivos de control a través de diagramas radiales para visualizar los resultados obtenidos, demostrando que las dos instituciones en el objetivo de control "Responsabilidad de los usuarios" consiguió el mayor nivel de acuerdo con el modelo de madurez CMMI con un valor de 5. Mientras que el objetivo de control "Requisitos de negocio para el control de acceso" adquirió el menor nivel con el valor de 1.6 para las dos. Con lo anteriormente mencionado, se aplicó la lista de chequeo en la que se evidenció las vulnerabilidades que presentaban los gestores, con el fin de aplicar controles para mitigar dichas vulnerabilidades.

Palabras clave: Vulnerabilidades, ISO 27002, Gestores de base de datos, CMMI

Abstract

This research is conducted with the aim of analyzing the vulnerabilities of the managers of databases of the Pontifical University Catholic headquarters emeralds and the Government autonomous decentralized of the Prefecture of Esmeraldas institutions. Developed a checklist based on the ISO 27002 the domain "Access Control" complemented with the CMMI maturity level to determine the level of the managers of the institutions involved in the study database. The methodology used was quantitative and the techniques of interviewing, observation, and test, which used the tool SqlMap were used to gather the information. The checklist questions were grouped according to their objectives of control through Radial diagrams to visualize the results, showing that the two institutions in order to control 'Responsibility to the users' It got the highest level according to the model of maturity CMMI with a value of 5. While the objective of control "Access control business requirements" acquired the lowest level to the value of 1.6 for the two. With the above, applied the checklist which showed the vulnerabilities that had managers, in order to apply controls to mitigate these vulnerabilities.

Key words: Vulnerabilities, ISO 27002, Database managers, CMMI

ÍNDICE DE CONTENIDOS

ÍNIDICE DE TABLAS

ÍNDICE DE ANEXOS

ÍNDICE DE DIAGRAMAS

ÍNDICE DE IMAGENES

1. INTRODUCCIÓN

El uso de sistemas informáticos lleva a las instituciones a incorporar políticas y medidas de protección, con el fin de asegurar sus operaciones y salvaguardar los datos que manejan. El activo más importante y fuente principal para que gerentes y administrativos tomen decisiones basadas en ella es la información; esto se debe al procesamiento diario de un sin número de datos que las instituciones manipulan (Franck y Romero, 2016).

> (Villalobos Murillo, 2012) menciona que la gran mayoría de los datos sensibles del mundo están almacenados en sistemas gestores de bases de datos comerciales tales como Oracle, Microsoft SQL Server entre otros, y atacar una base de datos es uno de los objetivos favoritos para los criminales.

Los atacantes buscan vulnerar los gestores de bases de datos, con el propósito de modificar o robar la información sensible, lo cual puede convertirse en una perdida para las empresas. Por eso se realiza auditorias que permitan conocer las vulnerabilidades existentes, con el objetivo de reducirlas.

En la investigación se analizó las vulnerabilidades de los gestores de bases de datos de la Pontificia Universidad Católica Sede Esmeraldas y el Gobierno Autónomo Descentralizado de la Prefectura de Esmeraldas, aplicando una lista de chequeo.

La elaboración de la lista de chequeo que se implementó está estructurada y fue aplicada basándose en la norma ISO 27002 el dominio “Control de Acceso”, el cual contiene controles para realizar el análisis a los gestores de bases de datos.

2. OBJETIVOS

2.1. Objetivo General

Evaluar la seguridad de la información mediante la elaboración de una lista de chequeo para la identificación de las vulnerabilidades en los gestores de base de datos.

2.2. Objetivos Específicos

- Identificar las vulnerabilidades de los principales gestores de base de datos.
- Elaborar una lista de chequeo para la identificación de las vulnerabilidades que pueden ser explotadas por las amenazas en los gestores de base de datos.
- Implementar la lista de chequeo en el proceso de administración de base de datos en las instituciones de la ciudad de Esmeraldas.

3. INFORME DEL CASO

3.1. DEFINICIONES DEL CASO

Para iniciar el estudio de caso, se repasan conceptos sobre base de datos, amenaza, vulnerabilidad y riesgo.

Rubinos y Nuevo (2011), definen a las **bases de datos** como" una sucesión de datos organizados que se encuentran relacionados entre sí; los mismo que son agrupados y analizados por los sistemas de información de las empresas o negocios".

Las bases de datos son una parte importante para los sistemas, estas deben contar con una seguridad adecuada para evitar incidentes. Las amenazas, vulnerabilidades y riesgos siempre están presentes en las base de datos, para Quiroz y Macías (2017) una **amenaza**, es todo suceso o incidente no deseado que pueda tentar en contra de los sistemas informáticos de una organización; una **vulnerabilidad,** es toda debilidad que puede presentar un sistema informático, el cual es explotado por una amenaza; un **riesgo,** es la probabilidad de que suceda un evento que perjudique un sistema.

Saraswat y Tripathi (2014), indican que existen muchas formas en que una base de datos puede verse comprometida, las más relevantes son:

Elevación de Privilegios: Ocurre cuando el atacante convierte los privilegios de acceso de un usuario normal a los de un administrador de datos.

SQL Injection: Sucede cuando un atacante inserta sentencias SQL no autorizadas en un canal de datos SQL vulnerable.

DBMS (Data Base Management System) sin parches: Ocurre cuando los proveedores de base no realizan actualizaciones, dejando aún más vulnerables los DBMS para los atacantes.

Configuraciones erróneas: Una configuración errónea de la base de datos permite a los atacantes eludir los métodos de autenticación y obtener acceso a información sensible.

Autenticación débil: Los atacantes pueden obtener las credenciales de inicio de sesión de todos los usuarios que cuentan con contraseñas débiles.

Privilegios excesivos e inutilizados: Ocurre cuando se asigna privilegios de base de datos que no corresponde con el puesto de trabajo del usuario.

Para el estudio es indispensable conocer sobre los controles del dominio "Control de acceso" de la ISO 27002 para evaluar cada una de las preguntas de la lista de chequeo. A continuación, se detalla cada uno de los controles.

- Es importante en toda empresa o institución contar con políticas de control de acceso, esto permite proveer las normas que se deben cumplir, ayudando a tener un control adecuado en los gestores de base de datos. La falta de políticas de control de acceso es una vulnerabilidad para cualquier entidad.

- Contar con políticas de almacenamiento de base de datos para las entidades es importante. Realizar los backup de las bases de datos y guardarlos en un lugar seguro, ayuda a la protección de la información de las entidades. Sin embargo, no contar con políticas significaría una vulnerabilidad, podría darse el caso de pérdida de información y no tener un backup correcto significaría una perdida para las empresas o instituciones.

- El acceso y los servicios de red deben ser manejados solo por usuarios autorizados, de no ser así esto se convertiría en una vulnerabilidad para las entidades, tener una configuración errónea, permite a los atacantes tener mayor facilidad para obtener información sensible.

- Debe existir un procedimiento de asignación de derechos de acceso en el que se contemple reportes de ingreso y baja de usuarios, sin este procedimiento no se podría llevar un control adecuado de usuarios. Se debe realizar controles en la asignación y uso de privilegios de acceso para evitar la elevación de privilegios no autorizados, es decir los atacantes podrían elevar sus accesos de un usuario normal a uno de administrador. Las entidades deben realizar un proceso formal de gestión de información secreta de autenticación de los usuarios, para poder llevar de mejor manera dicha información. También es importante realizar revisiones de los derechos de acceso de usuario, con el fin de observar que todos los usuarios tengan los privilegios que les son correspondientes. Las empresas deben

realizar la reasignación o retira de los derechos de acceso de usuario cuando este ha finalizado sus actividades en ellas, para evitar cualquier tipo de manipulación en los datos no autorizados, o que algún usuario tenga asignado privilegios que no corresponden con el puesto de trabajo.

- La información sensible debe ser conocida por el usuario autorizado, es por eso por lo que las empresas deben contar con un administrador de gestor de base de datos que controle en el uso de la información secreta de autenticación, con la finalidad de evitar cualquier actividad ilegal o poco ética con la información. Las empresas deben restringir el acceso a la información y a las funciones de las aplicaciones a usuarios no autorizados, con la intención de proteger la información sensible. Contar con un procedimiento seguro de inicio de sesión en el cual se valide correctamente el usuario y contraseña es importante para evitar que terceras personas ingresen a cuentas que no les corresponden. Para esto último se debe exigir que las contraseñas sean seguras y robustas, tratando de evitar la autenticación débil por parte de los usuarios.

- Llevar registros de auditoria donde se evidencie las acciones de los usuarios ayuda a detectar de una manera eficaz si se está o no trabajando de manera correcta. Es importante también realizar las actualizaciones en los gestores de base de datos, para evitar fallas en las mismas.

3.1.1. Presentación del caso

La preocupación que existe en la seguridad de los gestores de base de datos debido a las vulnerabilidades existentes llevó a realizar estudios para poder reducir los inconvenientes que puedan existir en los gestores.

En el estudio con el tema “Solución basada en el Razonamiento Basado en Casos para el apoyo a las auditorías informáticas a bases de datos”, de los autores Azán et al. (2014), se realizó un proceso de auditoría a los Sistemas Gestores de Bases de Datos, en el Departamento de Seguridad Informática de ETECSA a través de matrices de diagnóstico o listas de chequeo. Los expertos determinaron los niveles de riesgos de la seguridad de la información en alto, medio y bajo después de un análisis de los SGBD. En este estudio se implementó la técnica de Razonamiento Basado en

Casos (RBC) en la etapa de evaluación de riesgo de seguridad de la información, esto permite dar solución basándose en auditorias similares a las de este tipo. El estudio tuvo como resultado la construcción de un sistema que permite monitorear los SGBD: PostgreSQL, MySQL, SQL Server y Oracle, los cuales son los gestores utilizados por ETECSA.

Quisbert (2014), en su investigación para mitigar las vulnerabilidades que existen en las bases de datos, realizó un modelo de sistema multi-agente para percibir, evaluar y alertar ex-antes la detección de vulnerabilidades a los repositorios de bases de datos. El sistema utilizó agentes inteligentes, el cual es una tecnología que hace uso de reglas de razonamiento que se encuentran almacenadas en una base de datos de conocimiento bajo un patrón de vulnerabilidad, con el fin de avisar a tiempo sobre alguna vulneración, esto permite a los administradores de bases realizar las acciones correspondientes.

El autor mencionando, en su investigación indica que el 70% de las vulnerabilidades son internas y el 30% externas. Los ataques internos se deben a errores de desarrollo donde se deja ciertos espacios por donde se puede ingresar a la base de datos, en este caso puede ser con intención o no, por otra parte, también se da el caso de descuido por parte del usuario al revelar la clave de acceso de los gestores de bases de datos, y también ocurre por deshonestidad de los usuarios para sus beneficios. Los ataques externos ocurren por errores de seguridad física, es decir, por una mala configuración del hardware o del software, también por ataques remotos.

En el presente estudio se realizó el análisis de las vulnerabilidades de los gestores de bases de datos de algunas instituciones de la ciudad de Esmeraldas. Para realizar el análisis fue necesario la implementación de una lista de chequeo la cual se elaborado en base al dominio “Control de acceso” de la ISO 27002, dicho análisis permitió conocer las vulnerabilidades existentes en las instituciones involucradas en el estudio.

3.1.2. Ámbitos de estudio

La investigación fue desarrollada en la ciudad de Esmeraldas, específicamente en la Pontificia Universidad Católica Sede Esmeraldas y el Gobierno Autónomo Descentralizado de la Prefectura de Esmeraldas. El estudio está dirigido a las vulnerabilidades que presentan las instituciones en sus gestores de base de datos.

3.1.3. Actores implicados

Los gestores de bases de datos necesitan ser administrados de la mejor manera posible, por lo que su administración lo debe realizar un experto en el tema. Las instituciones cuentan con personas encargadas de la administración de los gestores de bases de datos, los cuales llevan el nombre de administradores de base datos.

Los administradores de bases de datos son los encargados de gestionar y mantener las bases de datos, seguras y actualizadas.

3.1.4. Identificación del problema

Para las empresas la información almacenada en las bases de datos es importante debido a que su existencia permite la continuidad de las actividades en las empresas, siendo necesaria la aplicación de normas y reglamentos para salvaguardarlas. Según Lopez y Zuluaga (2013), unos de los activos más significativos en las empresas es la información, la cual permite realizar actividades de manera rápida y eficaz, también ayuda a la toma de decisiones por parte de los gerentes o administrativos de una empresa. Solo las personas autorizadas pueden tener acceso a los datos, los administradores tienen la responsabilidad de garantizar lo dicho.

Es importante disponer de un entorno seguro para alojar y acceder a la información de base de datos. A continuación, se mencionan ataques realizados a varias empresas y los problemas que surgieron.

Según Ramos et al. (2013), el 27 de mayo del 2011 el sitio web de MySQL sufrió un ataque SQL Injection por parte de los hackers TinKode y Ne0h, del grupo Rumano Slacker.Ro, los cuales aprovecharon las vulnerabilidades presentes en la aplicación web que se conectaba a la base de datos, para realizar el volcado de la base de datos y sustraer las credenciales de los usuarios del servidor MySQL. También mencionan que a principios de febrero del 2011 la firma de seguridad HBGary Federal sufrió un ataque por parte de Anonymous, los cuales robaron más de 50.000 cuentas de correo de HBGary, así como información sensible.

Con los ataques mencionados anteriormente se puede observar lo perjudicial que puede ser para la empresa contar con bases de datos no seguras. Las empresas pueden correr el riesgo de acceso de personal no autorizado a la información sensible de la empresa, también pueden sufrir robo de información: como nombres de usuarios, contraseñas, correos electrónicos, etc. Existe también la posibilidad de que los atacantes puedan manipular los datos a su conveniencia consiguiendo darse privilegios de administrador de la base de datos, e incluso pueden llegar a eliminar datos que pueden causar pérdidas económicas a las empresas.

3.2. METODOLOGÍA

La metodología empleada es de tipo cuantitativo, se aplicó el método deductivo, la población son todas las empresas que tienen un departamento de desarrollo y manejan gestores de base de datos, en este caso se tomó una muestra por conveniencia los cuales son la Pontificia Universidad Católica Sede Esmeraldas y el Gobierno Autónomo Descentralizado de la Prefectura de Esmeraldas debido a que cuentan con un departamento de tecnología, y tienen personal responsable de la administración de los gestores de base de datos.

La información recopilada para el estudio se la obtuvo mediante la implementación de una lista de chequeo creada en base al dominio “Control de Acceso” de la norma ISO 27002, según la ISO 27000 (2013), el Control de Acceso tiene como fin controlar mediante restricciones y excepciones el acceso a la información como medida de seguridad informática. Esta lista fue realizada al personal responsable de la administración de los gestores de bases de datos de las entidades involucradas en el estudio.

3.2.1. Fuentes de información

La información adquirida la proporcionó los administradores de los gestores de bases de datos de las entidades implicadas en el estudio.

3.2.2. Técnicas de recolección de información

Para la validación de la información se realizó la triangulación, es decir la aplicación de 3 técnicas para el levantamiento de los datos: entrevista, observación y prueba.

Entrevista

Se evaluó cada parámetro de la lista de acuerdo con el criterio del administrado de base de datos. Con la implementación de esta técnica se conoció la administración de los gestores de acuerdo con las políticas definidas y configuraciones establecidas en las empresas (Anexo 1). Para Hernández y Carrera (2014), la entrevista tiene como fin la mejora del conocimiento, la cual se construye a partir de una interacción conversacional cara a cara entre el entrevistador y el entrevistado.

Observación

Se utilizó la observación como técnica para validar o comprobar cada una de las respuestas indicadas en la lista de chequeo, la ficha de observación se puede observar en el Anexo 22. Guillermo y Covarrubias (2012) definen a la observación como la forma más fácil de captar lo que ocurre en el mundo real.

Prueba

La implementación de esta técnica permitió la validación de algunas preguntas de la lista de chequeo, a las cuales eran necesaria aplicarles métodos para poder comprobar si las entidades cumplían con los requisitos, para ello se utilizó la herramienta sqlmap Anexo 17.

> Según Damele y Stampar (2016), sqlmap es una herramienta para pruebas de penetración "penetration testing" de software libre que automatiza el proceso de detección y explotación de fallos mediante inyección de SQL además de tomar el control de servidores de bases de datos. Contiene un poderoso motor de detección, así como muchas de las funcionalidades esenciales para el "pentester" y una amplia gama de opciones desde la recopilación de información para identificar el objetivo conocido como "fingerprinting" mediante la extracción de información de la base de datos, hasta el acceso al sistema de archivos subyacente para ejecutar comandos en el sistema operativo a través de conexiones alternativas conocidas como "Out-of-band"

Características del sqlmap:

- Soporte completo para los sistemas de administración de bases de datos MySQL, Oracle, PostgreSQL, Microsoft SQL Server, Microsoft Access, IBM DB2, SQLite, Firebird, Sybase, SAP MaxDB, HSQLDB y Informix.

- Soporte para conectarse directamente a la base de datos sin pasar por una inyección SQL, proporcionando credenciales DBMS, dirección IP, puerto y nombre de la base de datos.

- Soporte para enumerar usuarios, hashes de contraseñas, privilegios, roles, bases de datos, tablas y columnas.

- Reconocimiento automático de los formatos hash de contraseñas y soporte para descifrarlos usando un ataque basado en diccionario.

3.3. DIAGNÓSTICO

Para poder evaluar los resultados obtenidos con la lista de chequeo se debe conocer sobre cada una de las preguntas de la misma. En el dominio "Control de Acceso" de la ISO 27002 existen controles que indican lo que debería tener la empresa o institución para cumplir. Se considera al dominio fundamental para evaluar las bases de datos buscando la seguridad de la información a partir de controlar el acceso a los datos.

Para poder identificar de mejor manera a las instituciones involucradas en el estudio se les asigno letras de la siguiente manera:

- A = Pontificia Universidad Católica Sede Esmeraldas

- B = Gobierno Autónomo Descentralizado de la Prefectura de Esmeraldas

La institución A maneja los gestores de base de datos SQL Server estándar y MySQL, la institución B SQL Server express y MySQL.

Para realizar la evaluación de cada una de las preguntas de la lista de chequeo, se revisaron los modelos de madurez más significativos de acuerdo al artículo "Modelos de madurez y su idoneidad para aplicar en pequeñas y medianas empresas" y se determinó a partir del requerimiento de la lista de chequeo, considerando la existencia de un nivel 0 y que las etiquetas deben ajustarse a la posibles respuestas en la lista de chequeo, se dio como resultado la elección del modelo de madurez CMMI, el cual era el modelo idóneo para la evaluación. El CMMI "es el estándar de calidad más utilizado a nivel internacional por las organizaciones desarrolladoras de software, aunque su uso no se limita solamente a este tipo de organización"(Pérez-Mergarejo, Pérez-Vergara, y Rodríguez-Ruíz, 2014).

Tabla 1. Nivel de madurez CMMI. Fuente: (Pérez-Mergarejo et al., 2014)

Nivel	**Niveles de madurez**
0	No tiene
1	Inicial
2	Administrado
3	Definido
4	Administrado cuantitativamente
5	En optimización

Luego de implementar la lista de chequeo a las instituciones A y B se obtuvo como resultado lo siguiente.

Tabla 2. Diagnóstico de la lista de chequeo. Fuente: Autor

	A	B	Detalles
¿Cuenta con una política de control de acceso basada en los requisitos de negocio y de seguridad de la información?	0	0	Los administradores de los gestores de bases de datos de las instituciones A y B, mencionaron que no cuentan con una política formal, pero tienen claro que es importante para las instituciones contar con políticas que permitan el mejoramiento de las actividades.
¿Cuentan con políticas de almacenamiento de base de datos?	2	2	En la institución A realiza el respaldo de sus bases de datos a todos los días a una determinada hora como se muestra en la Anexo 2, así mismo la institución B también realiza el respaldo de sus bases de datos, pero de dos maneras como se visualiza en la Anexo 3: a) Semanal, b) Mensual, esta además es guardada en disco duro externo.
¿El acceso a las redes y servicios en red lo realizan solo los usuarios autorizados?	3	3	Para el acceso y los servicios de red en la institución A utilizan Active Directory (Directorio de administración), en el cual se realiza todo en cuanto a controles de acceso, eso se puede visualizar en la Anexo 4, en cambio la institución B manejan una aplicación la cual permite asignar los accesos a los usuarios como se muestra en la Anexo 5.

¿Cuentan con un procedimiento de asignación de derechos de acceso en el que contemple el registro y baja de usuarios?	3	3	Las instituciones A y B cuentan con un proceso el cual permite el registro y baja de usuario con se contempla en la Anexo 6, 7 respectivamente.
¿Cuentan con un control en la asignación y uso de privilegios de acceso?	5	5	Las instituciones A y B cuentan con una aplicación en el cual se realiza la asignación de los privilegios de acceso a los usuarios con se visualiza en la Anexo 8, 9 respectivamente.
¿Cuentan con un proceso formal de gestión de la información secreta de autenticación de los usuarios?	4	4	En la institución A manejan una regla que indica que los usuarios sean creados con el primer nombre y el primer apellido y la contraseña debe que ser una combinación entre letras, números y caracteres especiales, se puede visualizar en la Anexo 10, a diferencia de la institución B que manejan una regla en la cual indica que los usuarios deben ser creados con la primera letra del nombre y el apellido, y en cuento a contraseña manejan dos escenarios para sistemas que están dentro de la intranet en la cual la contraseña es segura y otros sistemas que no se encuentra en la intranet que la clave puede ser muy débil, se puede visualizar en la Anexo 11.
¿Realizan revisiones de los derechos de acceso de usuario?	3	3	En las instituciones A y B se realiza la revisión de los derechos de usuarios solo cuando los usuarios piden realizar cambios en las contraseñas como se muestra en la Anexo 12 y 13 respectivamente.

¿Realizan reasignación o retirada de los derechos de acceso de usuario cuando un empleado finaliza sus actividades de la empresa?	2	5	En esta situación se muestra una gran diferencia en las entidades, es importante mencionar que las dos instituciones cuentan con un sistema que permite la reasignación o retirar de acceso, pero en una de ellas interviene un factor que impide que este proceso sea óptimo. En la institución A interviene recursos humanos, este departamento es el que se encargada de gestionar los reportes de las modificaciones que se puedan presentar en con cualquier usuario, este departamento de recursos humanos demora en comunicar sobre el cambio de algún usuario, lo dicho se pude visualizar en las Anexo 8. Un caso distinto es la institución B, el sistema que ellos manejan, así como permite la asignación del acceso, este mismo sistema automáticamente lo cancela, esto se da por el hecho que cuando se realiza el proceso de asignación de acceso se ingresa la fecha de inicio y fin para el usuario como se visualiza en la Anexo 9.
¿Se realiza controles en el uso de la información secreta de autenticación por parte del administrador de base de datos?	5	5	En las dos instituciones solo los administradores cuentan con las claves de los gestores de bases de datos que utilizan.
¿Cuentan con alguna restricción en el acceso a la información y a las funciones de las aplicaciones?	3	1	Parte de los sistemas web de las instituciones A y B cuentan con el protocolo de seguridad htpps. La institución A cuenta con restricciones y con controles en cuanto a los mensajes de error que

			impiden el acceso a terceros como se visualiza en la Anexo 14. A diferencia de la institución B que no cuentan con un buen control como se visualiza en la Anexo 15.
¿Existe un procedimiento seguro de inicio de sesión?	4	2	En la institución A tiene un inicio de sesión seguro como se visualiza en la Anexo 16. A diferencia de la institución B que si se pudo ingresar como se visualiza en la Anexo 15.
¿Existe control registros de auditoria donde se evidencie las acciones de los usuarios?	2	5	En la institución A el administrador menciono que ellos cuentan con el gestor de base de datos SQL Server el mismo que genera archivos logs, los cuales llevan el registro de cada movimiento que pueda existir, pero no cuentan con una aplicación que les permita revisar dichos archivos, también indico que hace unos años atrás se contaba con la licencia de la herramienta Apex SQL la cual permitía leer los archivos logs. En cambio, la institución B si cuenta con una aplicación la cual permite determinar quién y cuándo realizo algún movimiento como se ve en la Anexo 13.
¿Existe instalación de actualización del gestor de base de datos?	5	5	En las instituciones A y B, las actualizaciones se realizan automáticamente, por el hecho de utilizar como gestor de base de datos SQL SERVER.

4. EJECUCIÓN DE LA PRUEBA

La herramienta SqlMap fue utilizada para obtener información de los gestores de bases de datos de las instituciones involucradas mediante inyecciones Sql. Se busco servicios web vulnerables de las instituciones, principalmente se identificaron páginas que no tenían el protocolo de seguridad https y tenían extensión php.

4.1. Ejecución de la prueba en la institución A

En el análisis de los servicios web de la institución A se identificó que las paginas tenían protocolos de seguridad https, también se verificó que las páginas de inicio de sesión contaban con los controles de aplicación impidiendo el acceso a terceros no autorizados.

De acuerdo con el Anexo 14, se demuestra que la aplicación posee un control interno de manejo de errores para validar cadenas de SQL Injection por lo cual la página presentada no proporcionó información que permita identificar el gestor de base de datos u otra información de programación interna.

De igual forma se procedió a realizar el análisis con la herramienta SqlMap lo cual demostró que no se pudo vulnerar la página mediante SQL Injection como se visualiza en la imagen 1.

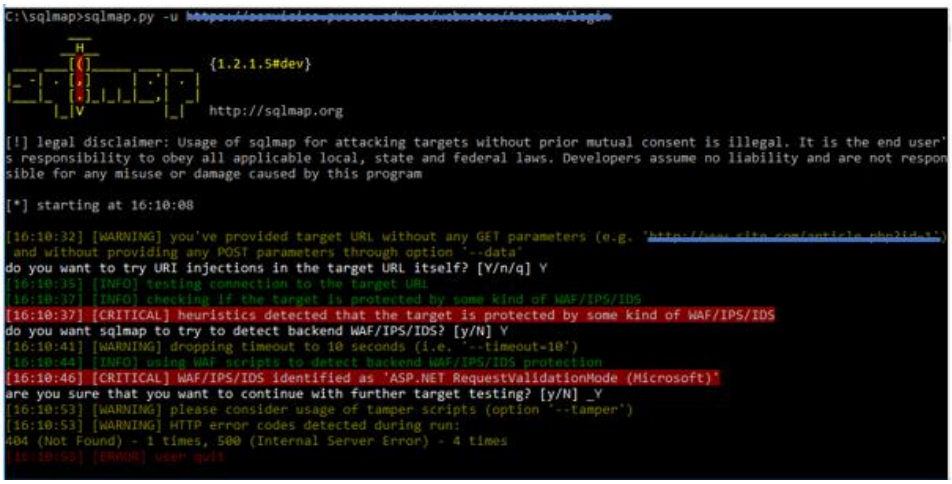


Imagen 1. Ejecución de la prueba a la institución A. Fuente: Autor

4.2. Ejecución de la prueba en la institución B

Al realizar el análisis la institución B se encontró una página vulnerable, la cual no contaba con el control de seguridad https, también se comprobó que la página de inicio de sesión no contaba con los controles de identificación permitiendo el acceso no autorizado.

Después del análisis a la página se procedió a buscar una url vulnerable la cual se la colocó en la herramienta SqlMap como se muestra en la imagen 1, esto con el fin de conocer si es posible atacar a través de la variable utilizada en la url, mediante técnicas de SQL Injection incluidas en el sistema SqlMap.

Como resultado se obtuvo el nombre de las bases de datos que se utiliza en la institución como se visualiza en el Anexo 20, obteniendo un total de 15 bases de datos como se ve en el Anexo 18.

Se selecciono una base de datos y se procedió a obtener el listado de las tablas a través de la introducción de comandos en la herramienta SqlMap (Anexo 21), teniendo como resultado un total de 30 tablas como se observa en el Anexo 19. Por motivo de confidencialidad no se puede colocar el nombre de las bases y de las tablas.

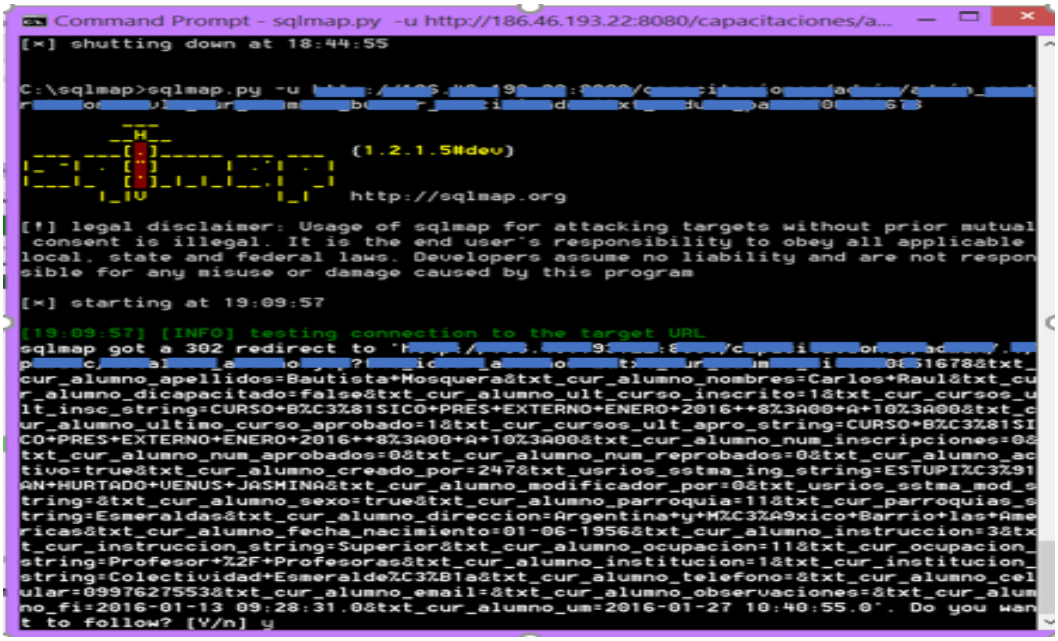


Imagen 2. Ejecución de la prueba a la institución B. Fuente: Autor

5. RESULTADOS

Se realizó el agrupamiento por objetivos de control de cada pregunta, con la finalidad de realizar un diagrama radial de cada una de las instituciones, con el propósito de observar de mejor manera las debilidades de las dos instituciones involucradas en el estudio.

Los cuatro objetivos de control ayudaron a realizar los diagramas radiales que se muestran a continuación.

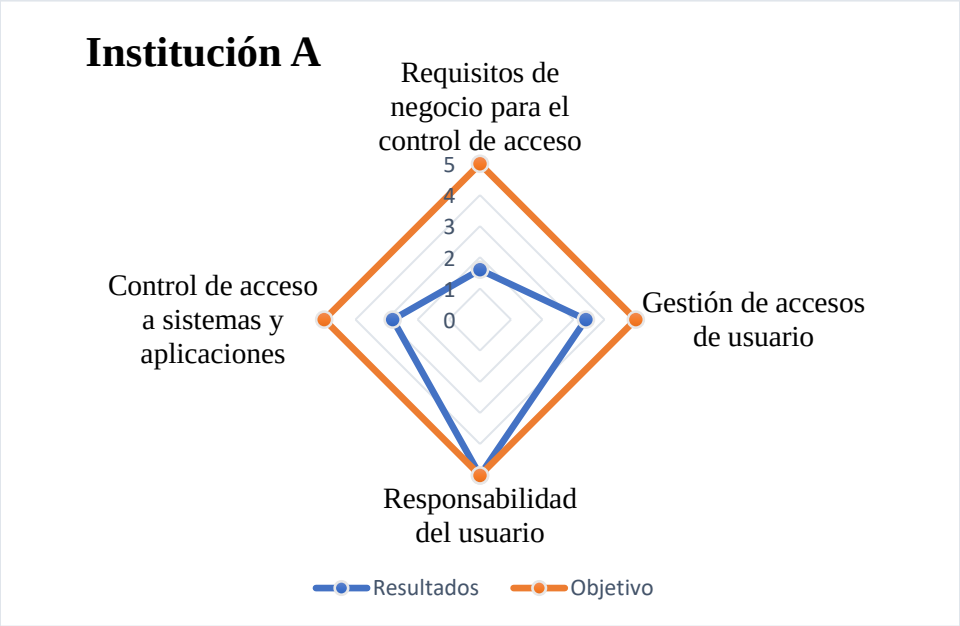


Diagrama 1. Diagrama Radial de la institución A. Fuente: Autor

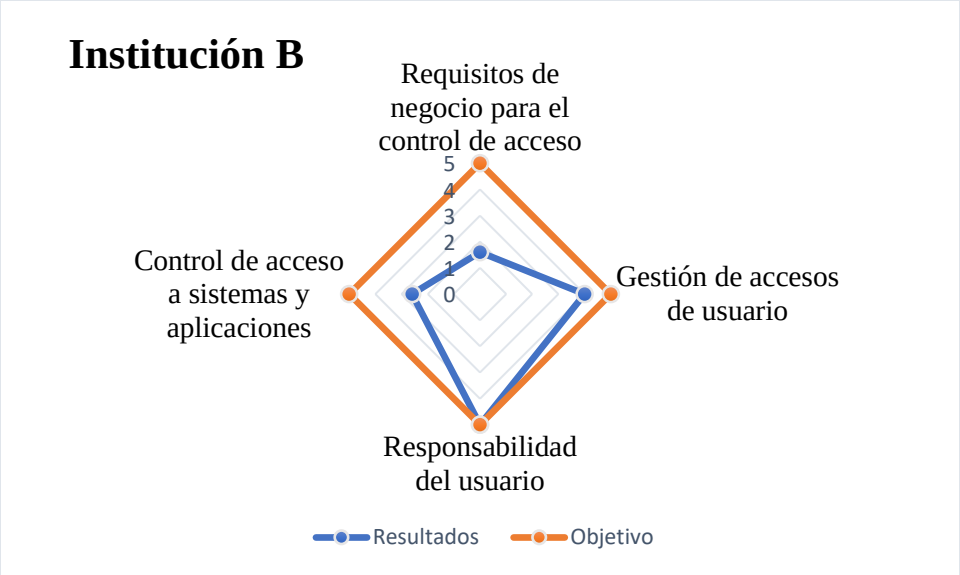


Diagrama 2. Diagrama Radial de la institución B. Fuente: Autor

Con los resultados obtenidos de los diagramas radiales se evidencio que las instituciones cuentan con debilidades en cuanto a Requisitos de negocio para el control de acceso, Gestión de accesos a usuario y Control de acceso a sistemas y aplicaciones. De manera más precisa las instituciones tienen vulnerabilidades como: falta de documentación en cuanto a políticas de acceso y de almacenamiento de datos, procedimientos inadecuados en cuanto al registro y baja de usuarios, falta de revisión de los privilegios de usuarios, entre otros.

En las dos instituciones A y B el objetivo de control "Responsabilidad de los usuarios" consiguió el mayor nivel de acuerdo con el modelo de madurez CMMI con un valor de 5. Mientras que el objetivo de control "Requisitos de negocio para el control de acceso" adquirió el menor nivel con el valor de 1.6 para las dos.

A las dos instituciones A y B se les realizaron las mismas pruebas para tratar de obtener información sensible referente a ellas. Se examinó cada uno de los servicios web que las

instituciones tienen, con la finalidad de buscar aplicaciones vulnerables, en lo cual resultó la institución B más vulnerable.

Por lo general las aplicaciones que las instituciones creen que son menos importantes, llegan a ser el blanco principal para los atacantes. Unas de las aplicaciones de la institución B que no contaba con el protocolo de seguridad https fue la que se pudo vulnerar, logrando llegar hasta la visualización de las bases de datos y tablas de dicha institución como se muestra en la Anexo 18 y 19 respectivamente.

6. PROPUESTA DE INTERVENCION

Para identificar y mitigar las vulnerabilidades se propone implementar en las instituciones o empresas la lista de chequeo que permitirá conocer las vulnerabilidades existentes, y aplicar los controles que pertenecen a los cuatros objetivos de control del dominio “Control de Acceso” de la ISO 27002.

A continuación, se detalla cuáles son los requisitos que deben cumplir las empresas para alcanzar el objetivo de tener sus gestores de bases de datos seguros

Tabla 3. Objetivos de control. Fuente: Autor

OBJETIVO DE CONTROL ISO 27002	PREGUNTA ASOCIADA A POSIBLE VULNERABILIDADES EN BASE DE DATOS	RECOMENDACIÓN
Requisitos de negocio para el control de acceso	¿Cuenta con una política de control de acceso basada en los requisitos de negocio y de seguridad de la información?	Se debería establecer, documentar y revisar una política de control de acceso basada en los requisitos de negocio y de seguridad de la información.
Requisitos de negocio para el control de acceso	¿Cuentan con políticas de almacenamiento de base de datos?	Se debería establecer, documentar y revisar una política almacenamiento de base de datos.
Requisitos de negocio para el control de acceso	¿El acceso a las redes y servicios en red lo realizan solo los usuarios autorizados?	Proporcionar a los usuarios el acceso a las redes y servicios en red para cuyo uso hayan sido específicamente autorizados. Por ejemplo, MySQL en su página oficial recomienda algunas pautas de seguridad las cuales son: • Restringir el acceso a usuarios normales a la tabla user de la base de datos mysql excepto el usuario root. • Conocer el sistema de control de acceso, las instrucciones GRANT y REVOKE se usan para control el acceso a la base de datos.

		• Comprobar que no se puede ingresar a la base de datos como root sin la petición de la contraseña. Por defecto, la cuenta root vienen sin contraseña, lo cual se debe modificar. • Usar la declaración SHOW GRANTS, para verificar que cuentas tiene acceso a qué. Luego usar la declaración REVOKE para eliminar los privilegios que no son necesarios. • No almacenar contraseñas en texto plano. • No elegir contraseñas de diccionario. • Invierta en un firewall, esto lo protege de al menos el 50% de todos los tipos de exploits en cualquier software. Coloque MySQL detrás del firewall o en una zona desmilitarizada (DMZ). Para verificar y controlar el acceso Sql Server utiliza Sql Server Audit, el cual permite realizar auditoría en la base de datos creando una descripción de auditoría de base de datos, permitiendo conocer que usuario realiza modificaciones, esto solo es posible en SQL Server Enterprise y Develope.

Gestión de acceso de usuario	¿Cuentan con un procedimiento de asignación de derechos de acceso en el que contemple el registro y baja de usuarios?	Se debería implementar un procedimiento formal de registro y retirada de usuarios que haga posible la asignación de derechos de acceso. Tanto como en SQL Server y MySQL utilizan la declaración GRANT para asignar privilegios en las bases de datos.
Gestión de acceso de usuario	¿Cuentan con un control en la asignación y uso de privilegios de acceso?	Se debería restringir y controlar la asignación y uso de privilegios de acceso. Por ejemplo, en MySQL se puede Usar la declaración SHOW GRANTS para verificar qué cuentas tienen acceso a qué. Luego usar la declaración REVOKE para eliminar los privilegios que no son necesarios. De igual manera SQL Server utiliza la declaración REVOKE para revocar los privilegios.
Gestión de acceso de usuario	¿Cuentan con un proceso formal de gestión de la información secreta de autenticación de los usuarios?	La asignación de la información secreta de autenticación debe ser controlada mediante un proceso formal de gestión.
Gestión de acceso de usuario	¿Realizan revisiones de los derechos de acceso de usuario?	Los administradores deberían revisar los derechos de acceso de usuario en determinados tiempos.

Gestión de acceso de usuario	¿Realizan reasignación o retirada de los derechos de acceso de usuario cuando un empleado finaliza sus actividades de la empresa?	Se debería realizar la retira de los derechos de acceso para todos los empleados y terceras partes, a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato, o cambiado.
Responsabilidad del usuario	¿Se realiza controles en el uso de la información secreta de autenticación por parte del administrador de base de datos?	Se debería requerir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.
Control de acceso a sistemas y aplicaciones	¿Cuentan con alguna restricción en el acceso a la información y a las funciones de las aplicaciones?	Se debería restringir el acceso a la información y a las funciones de las aplicaciones, de acuerdo con la política de control de acceso definida. Por ejemplo en SQL Server se utiliza la función **sp_setapprole** la cual permite que una aplicación ejecute sus propios privilegios.
Control de acceso a sistemas y aplicaciones	¿Existe un procedimiento seguro de inicio de sesión?	Se debería controlar por medio de un procedimiento seguro de inicio de sesión al acceso a los sistemas y a las aplicaciones.

Control de acceso a sistemas y aplicaciones	¿Existe una gestión de contraseña que establezca contraseñas seguras y robustas?	Se debería contar con sistemas de gestión de contraseñas que sean interactivos y que aseguraren contraseñas robustas.
Control de acceso a sistemas y aplicaciones	¿Existe control registros de auditoria donde se evidencie las acciones de los usuarios?	Los registros de auditorías son datos que se almacenan en archivos de auditoría y describen un único evento. Donde cada uno se compone de tokens. Para implementar los controles de autoría se debería revisar y evaluar el control interno del entorno en que se desarrolla la base de datos, capacidad para examinar riesgos y controles, evaluar y recomendar mejoras, etc. Como punto importante, la información es un activo clave en toda organización, por ello, la labor de auditoría es de suma importancia.
Control de acceso a sistemas y aplicaciones	¿Existe instalación de actualización del gestor de base de datos?	Los procedimientos de actualización y recuperación, comunes y bien determinados, deberían ser capaces de conservar la integridad, seguridad y confidencialidad del conjunto de datos.

7. CONCLUSIONES

La falta de experiencia y conocimiento por parte de los administradores de base de datos sobre el manejo y configuración de los gestores es una de las vulnerabilidades más importante que puede presentar una empresa. Otras vulnerabilidades de los principales gestores de bases de datos son: Elevación de Privilegios, SQL Injection, DBMS (Data Base Management System) sin parches, autenticación débil y privilegios excesivos e inutilizados.

Para la identificación de vulnerabilidades en los principales gestores de bases de datos se elaboró una lista de chequeo basada en el dominio "Control de acceso" de la ISO 27002, en la cual se encuentran integrados 4 objetivos de control: Requisitos de negocio para el control de acceso, Gestión de accesos de usuario, Responsabilidad del usuario y Control de acceso a sistemas y aplicaciones.

Se ha implementado la lista de chequeo en dos instituciones, esta se realizó mediante el uso de la técnica de la entrevista juntamente con la observación, que permitió la verificación de la información obtenida en las preguntas de la lista de chequeo; sin embargo, para la verificación de algunas fue necesario aplicar pruebas.

8. RECOMENDACIONES

Es recomendable que las dos instituciones mencionadas en el estudio apliquen los controles establecidos en la propuesta debido a que ninguna mostró resultados óptimos en los objetivos de control, mismos que se encuentran basados en el dominio “Control de acceso” de la ISO 27002.

Las dos instituciones evaluadas no cumplen con los requisitos de negocio para el control de acceso, por lo que es indispensable gestionar políticas para el control del mismo y almacenamiento de base de datos, así como proporcionar accesos autorizados a las redes y servicios a los usuarios.

Es fundamental que las instituciones tengan un usuario con acceso a todas las funciones del gestor de base de datos definido como super administrador, sin embargo, las credenciales del mismo deben manejarse con una contraseña robusta y un nivel de encriptación alto.

Las empresas deberán invertir en capacitaciones y personal de primera línea para afrontar la falta de conocimiento y experiencia a la hora de administrar las bases de datos y evitar posibles vulnerabilidades.

REFERENCIA BIBLIOGRÁFICA

Azán, Y., Bravo, L., Rosales, W., Trujillo, D., Garcia, E., & Pimentel, A. (2014). Solución basada en el Razonamiento Basado en Casos para el apoyo a las auditorías informáticas a bases de datos. *Revista Cubana de Ciencias Informáticas*, *8*(2), 52–69. Retrieved from http://rcci.uci.cu

Damele, B., & Stampar, M. (2016). sqlmap: automatic SQL injection and database takeover tool. Retrieved February 7, 2018, from http://sqlmap.org/

Franck, J. J., & Romero, M. (2016). Auditoría De Las Bases De Datos De Gestión Superior Públicas De Manabí, 141. https://doi.org/http://repositorio.espam.edu.ec/handle/42000/300

Guillermo Campos y Covarrubias, N. E. L. M. (2012). La Observación, Un Método Para El Estudio De La Realidad. *Revista Xihmai*, *7*(13), 282. Retrieved from http://www.lasallep.edu.mx/xihmai/index.php/xihmai/article/view/203

Hernández Carrera, R. M. (2014). La Investigación Cualitativa a Tr Avés De Entrevistas: Su Análisis Mediante La Teoría Fundamentada. *Cuestiones Pedagógicas*, *23*, 187–210. Retrieved from https://idus.us.es/xmlui/bitstream/handle/11441/36261/La investigacion cualitativa a traves de entrevistas.pdf?sequence=1&isAllowed=y

ISO 27000. (2013). ControlesISO27002-2013, 27002. Retrieved from http://iso27000.es/download/ControlesISO27002-2013.pdf

Lopez, J. A., & Zuluaga, A. F. (2013). DESARROLLO DE UNA METODOLOGÍA PARA EL CONTROL DE RIESGOS PARA AUDITORIA DE BASE DE DATOS. Retrieved from http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4153/0058L864.pdf?sequence=1&isAllowed=y

MySQL. (n.d.). MySQL :: Security in MySQL :: 2.1 Security Guidelines. Retrieved February 1, 2018, from https://dev.mysql.com/doc/mysql-security-excerpt/5.7/en/security-guidelines.html

Pérez-Mergarejo, E., Pérez-Vergara, I., & Rodríguez-Ruíz, Y. (2014). Modelos de madurez y su

idoneidad para aplicar en pequeñas y medianas empresas. *Maturity Models and the Suitability of Its Application in Small and Medium Enterprises.*, *35*(2), 146–158. Retrieved from http://scielo.sld.cu/pdf/rii/v35n2/rii04214.pdf

Quiroz, S., & Macías, D. (2017). *Dominio de las Ciencias.* [publisher not identified]. Retrieved from https://docs.google.com/viewerng/viewer?url=https://www.dominiodelasciencias.com/ojs/index.php/es/article/viewFile/663/pdf

Quisbert, A. (2014). REVISTA PGI -INVESTIGACIÓN, CIENCIA Y TECNOLOGÍA Modelo de Sistemas Multi-Agentes para Percibir, Evaluar y Alertar Ex-Antes los Accesos no Autorizados a Repositorios de Base de Datos. Retrieved from http://www.revistasbolivianas.org.bo/pdf/rpgi/n1/n1_a24.pdf

Rubinos, A., & Nuevo, A. (2011). Seguridad en bases de datos Security Database. *Revista Cubana de Ciencias Informáticas (RCCI)*, *5*(Sistema de bases de datos), 16. Retrieved from http://rcci.uci.cu

Saraswat, D., & Tripathi, P. (2014). International Journal of Advanced Research in Computer Science and Software Engineering. *International Journal of Advanced Research in Computer Science and Software Engineering*, *4*(5), 442–458. Retrieved from http://ijarcsse.com/Before_August_2017/docs/papers/Volume_3/5_May2013/V3I5-0309.pdf

Villalobos Murillo, J. (2012). Principios Básicos de Seguridad en Bases de Datos | Revista .Seguridad. *13/01/2012*, 1–5. Retrieved from http://revista.seguridad.unam.mx/numero-12/principios-básicos-de-seguridad-en-bases-de-datos

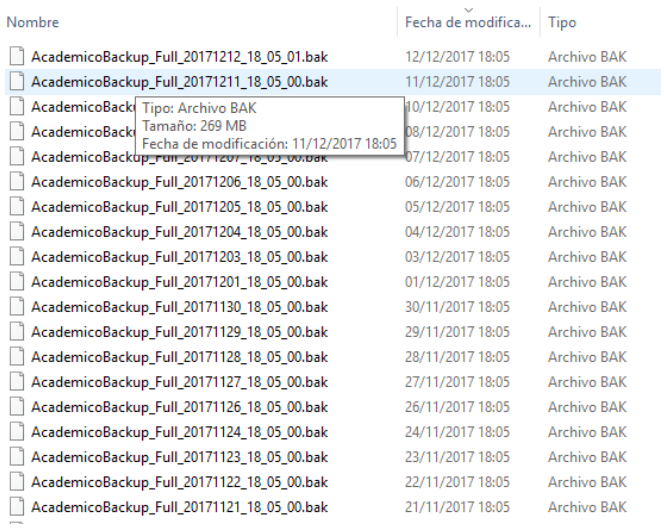
9. ANEXOS

Anexo 1. Lista de Chequeo (Control de Acceso). Fuente: ISO 27002 (2013)

	0	1	2	3	4	5
¿Cuenta con una política de control de acceso basada en los requisitos de negocio y de seguridad de la información?						
¿Cuentan con políticas de almacenamiento de base de datos?						
¿El acceso a las redes y servicios en red lo realizan solo los usuarios autorizados?						
¿Cuentan con un procedimiento de asignación de derechos de acceso en el que contemple el registro y baja de usuarios?						
¿Cuentan con un control en la asignación y uso de privilegios de acceso?						
¿Cuentan con un proceso formal de gestión de la información secreta de autenticación de los usuarios?						
¿Realizan revisiones de los derechos de acceso de usuario?						
¿Realizan reasignación o retirada de los derechos de acceso de usuario cuando un empleado finaliza sus actividades de la empresa?						
¿Se realiza controles en el uso de la información secreta de autenticación por parte del administrador de base de datos?						
¿Cuentan con alguna restricción en el acceso a la información y a las funciones de las aplicaciones?						

¿Existe un procedimiento seguro de inicio de sesión?						
¿Existe una gestión de contraseña que establezca contraseñas seguras y robustas?						
¿Existe control registros de auditoria donde se evidencie las acciones de los usuarios						
¿Existe instalación de actualización del gestor de base de datos?						

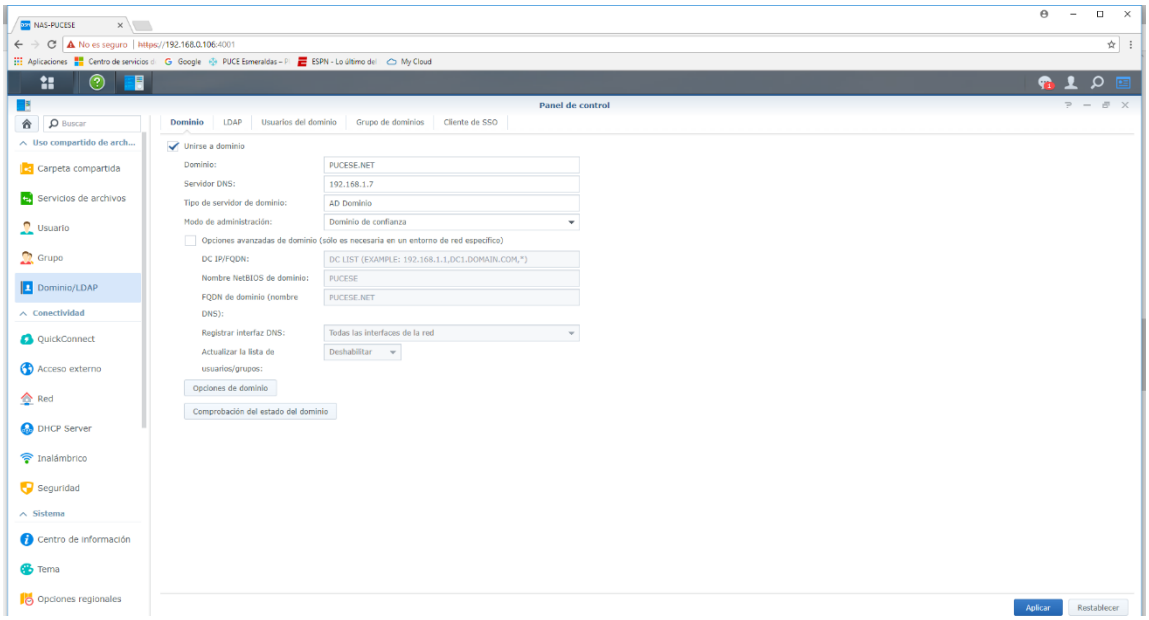
Anexo 2. Respaldo de base de datos de la institución A. Fuente: Autor



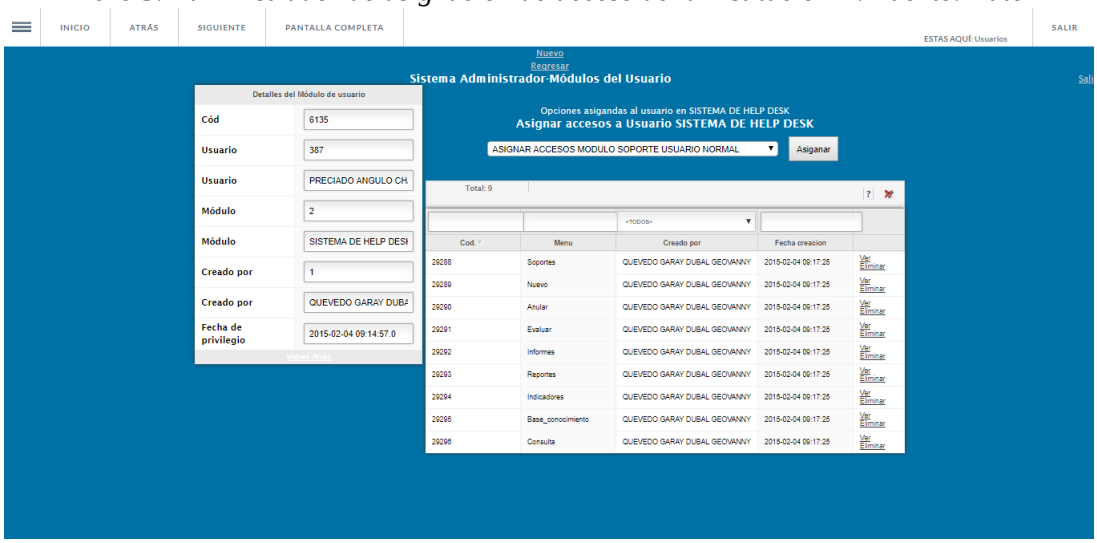
Anexo 3. Respaldo de base de datos de la institución B: Fuente: Autor

fecha_ing	fecha_um	id_estado	per_observacion_anulado	id_recepcionista_salida	id_recepcionista_entrada	fecha_anulado	tiempo
2014-08-22 11:16:49	2014-08-22 11:46:53	5	NULL	NULL	NULL	NULL	01:00:
2014-08-27 07:53:12	2015-02-25 14:26:51	2	NULL	NULL	NULL	NULL	04:00:
2014-08-27 07:54:07	2015-02-25 14:27:00	2	NULL	NULL	NULL	NULL	04:00:
2014-08-27 07:54:27	2015-02-25 14:27:09	2	NULL	NULL	NULL	NULL	04:00:
2014-08-29 15:52:58	2015-01-29 14:56:36	6	ANULAR	NULL	NULL	2015-01-29 14:56:36	00:10:
2014-08-29 15:52:58	2014-08-29 15:52:58	1	NULL	NULL	NULL	NULL	00:10:
2014-08-29 15:52:58	2015-02-20 15:23:08	2	NULL	NULL	NULL	NULL	00:10:

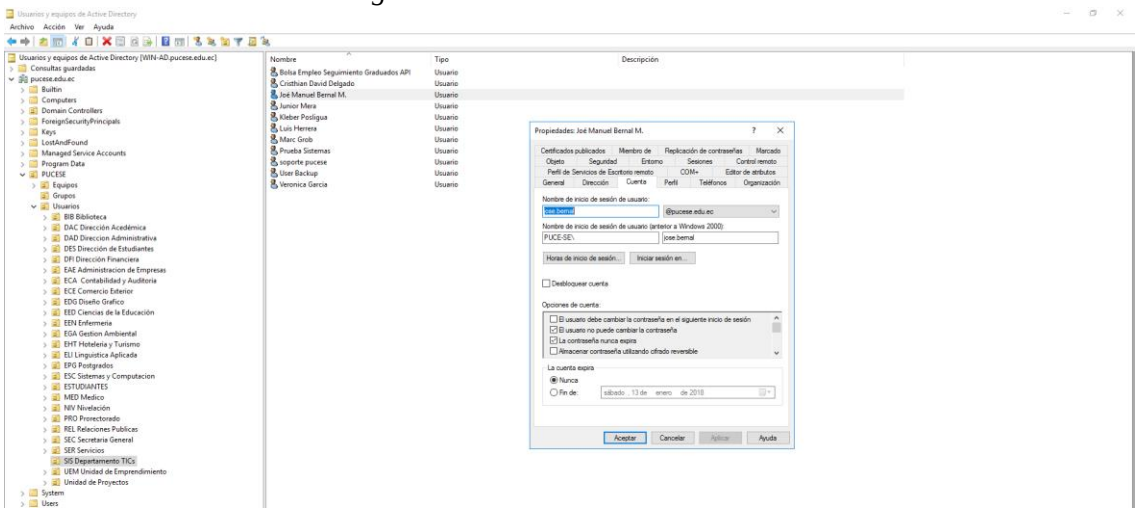
Anexo 4. Administrador de la institución A. Fuente: Autor



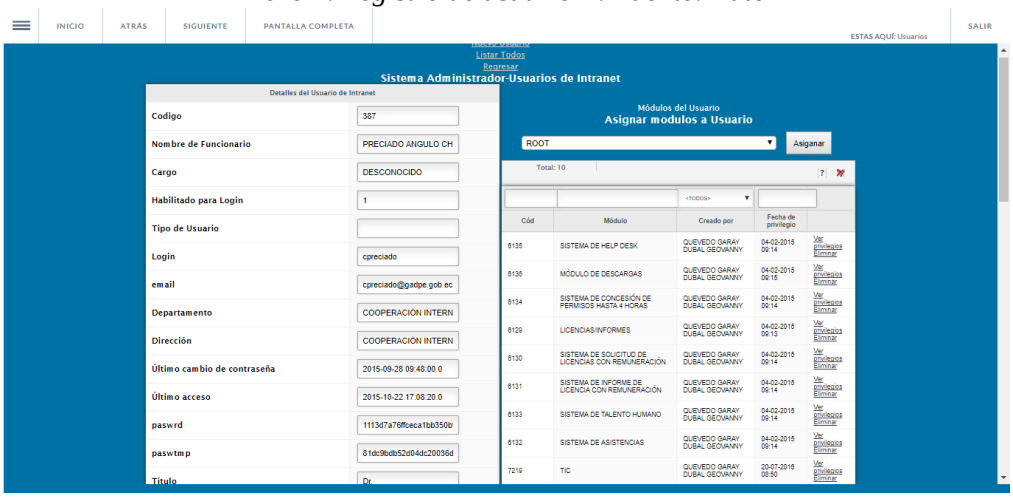
Anexo 5. Administrador de asignación de acceso de la institución B. Fuente: Autor



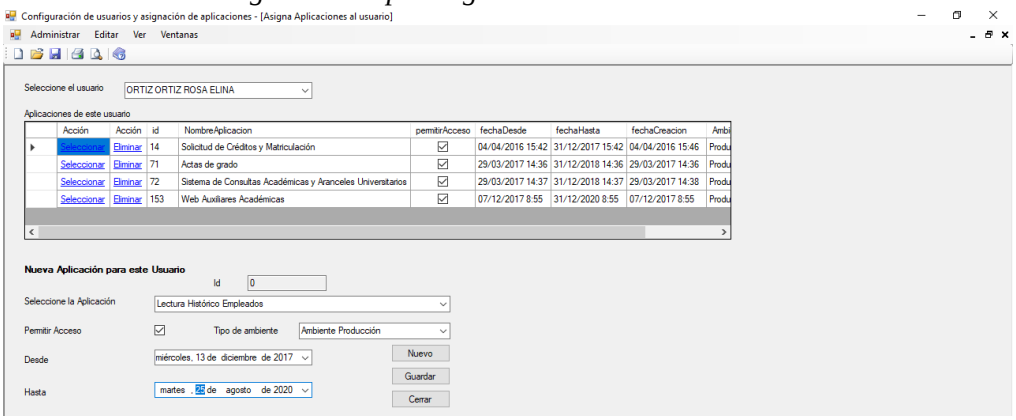
Anexo 6. Registro de usuario institución A. Fuente: Autor



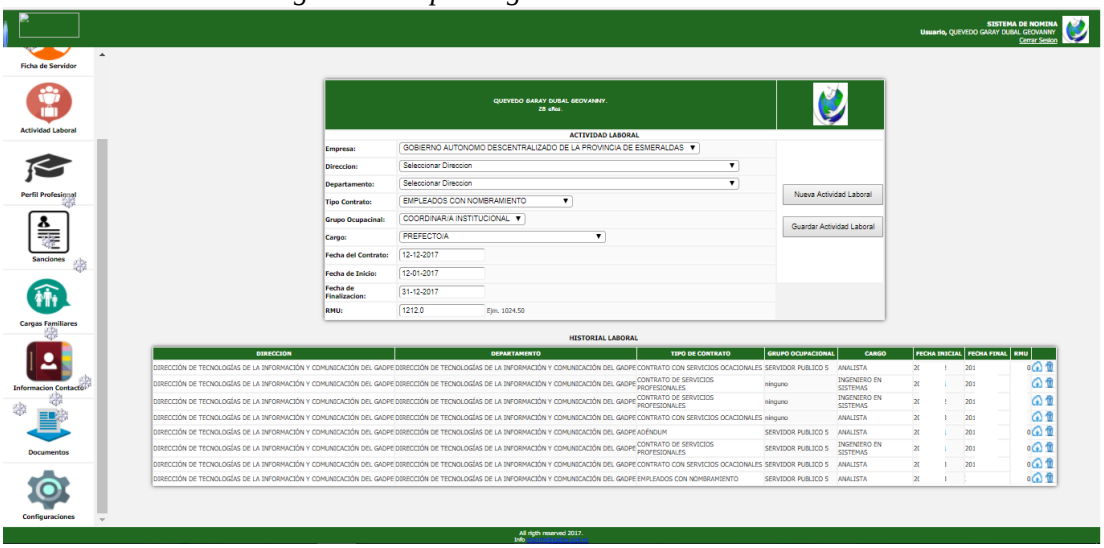
Anexo 7. Registro de usuario B. Fuente: Autor



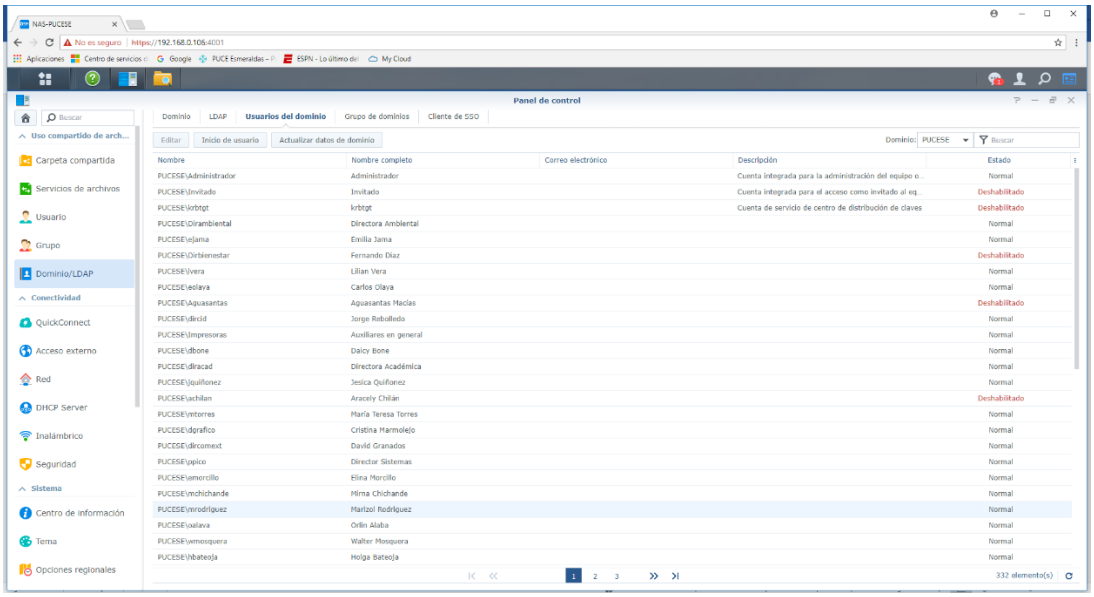
Anexo 8. Asignación de privilegios de la institución A. Fuente: Autor



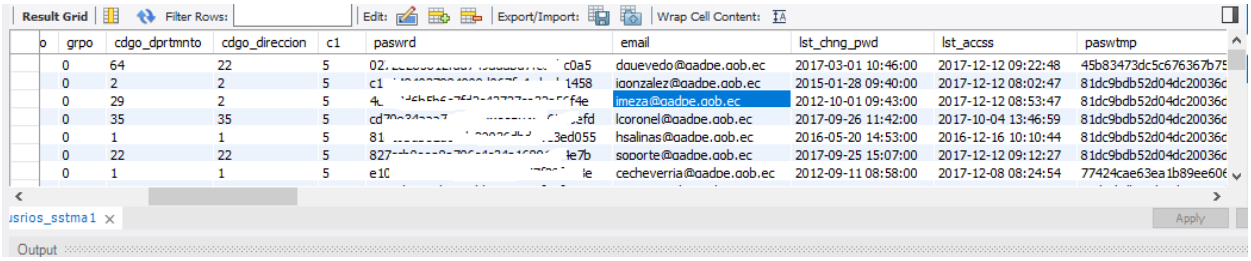
Anexo 9. Asignación de privilegios de la institución B. Fuente: Autor



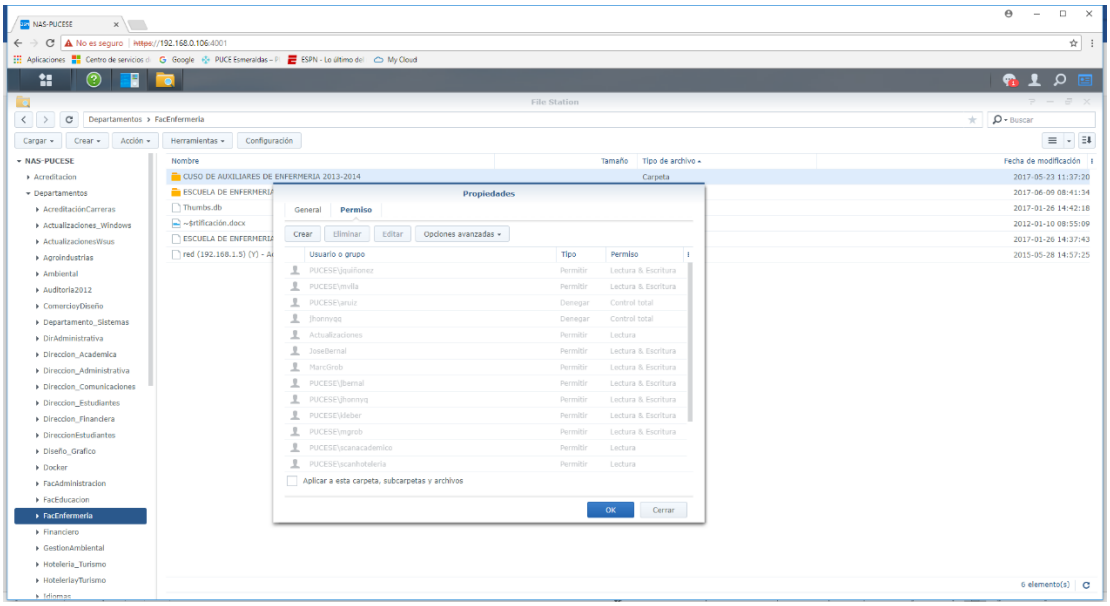
Anexo 10. Autenticación de usuario de la institución A. Fuente: Autor



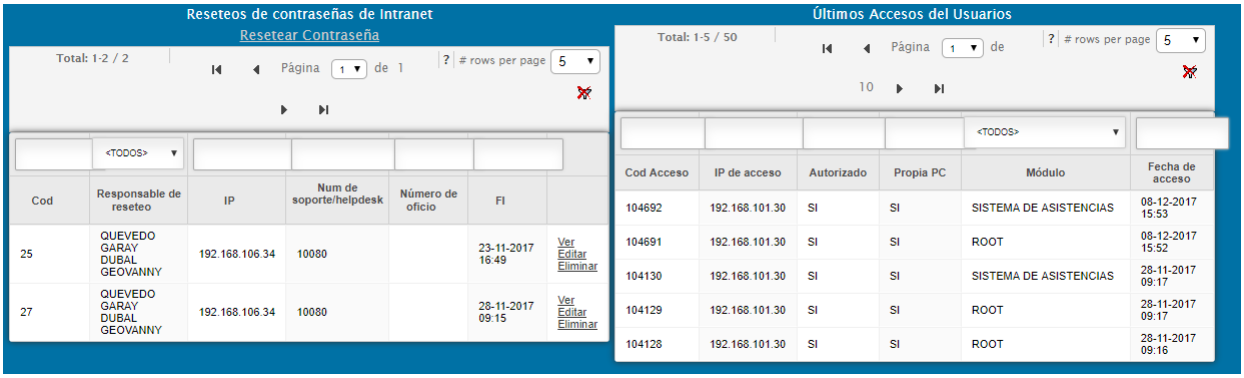
Anexo 11. Autenticación de usuario de la institución B. Fuente: Autor



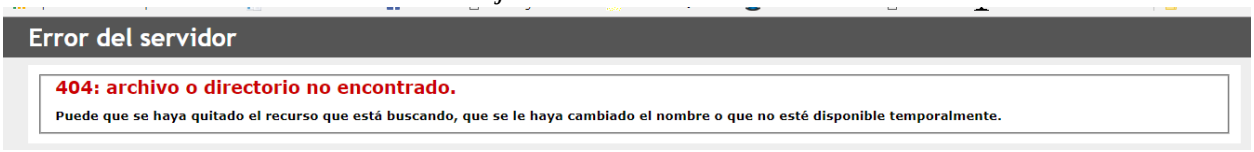
Anexo 12. Control de derechos de la institución A. Fuente: Autor.



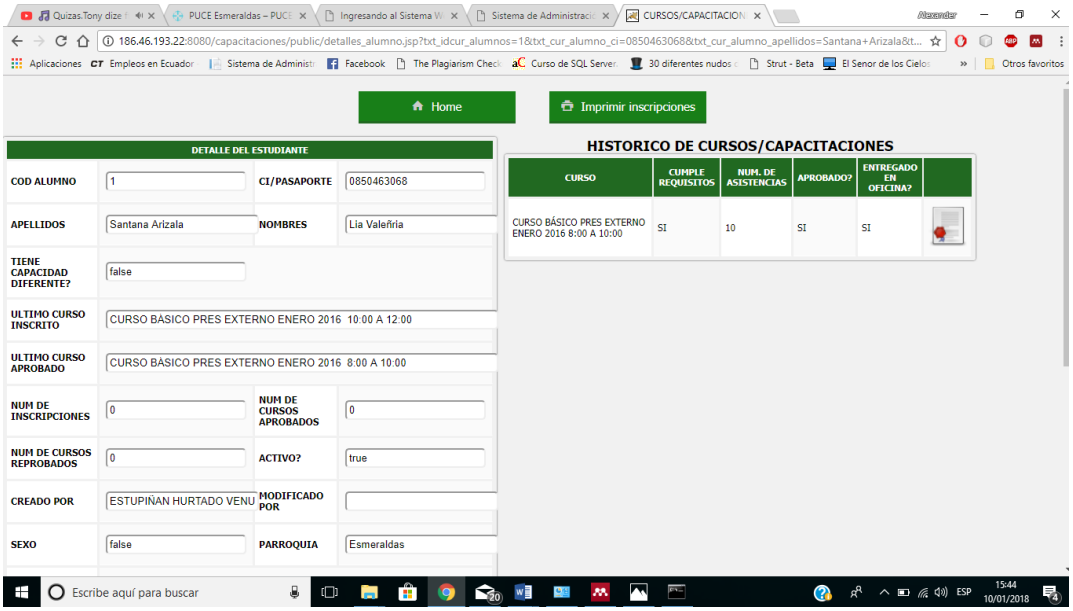
Anexo 13. Evidencia de la institución B. Fuente: Autor



Anexo 14. Mensaje de error institución A. Fuente: Autor

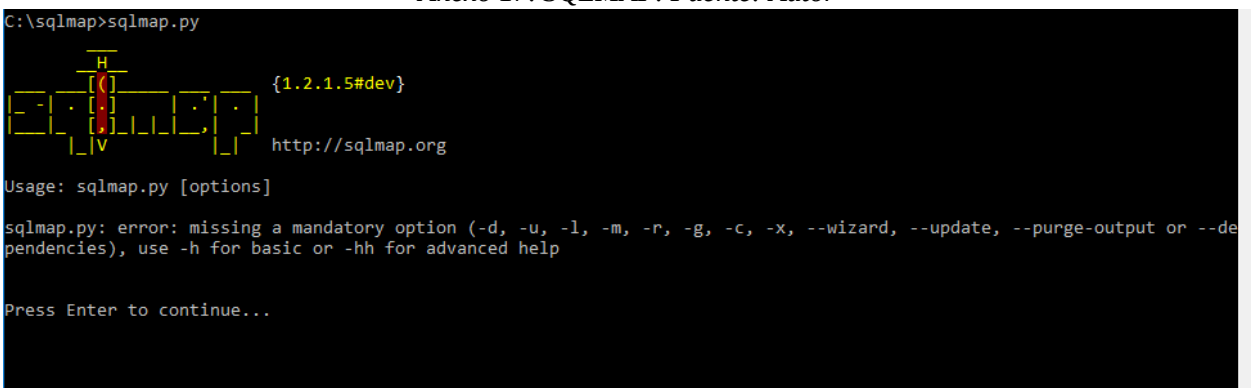


Anexo 15. Vulneración institución B. Fuente: Autor

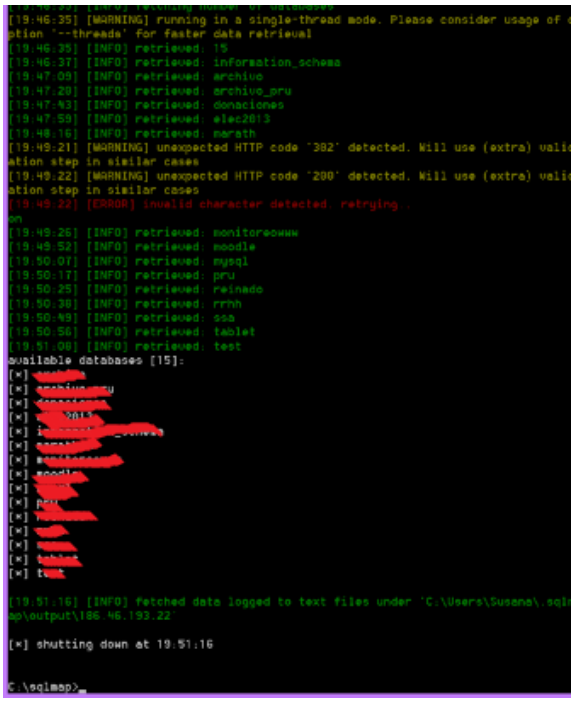


Anexo 16. Mensaje de error 2. Fuente: Autor

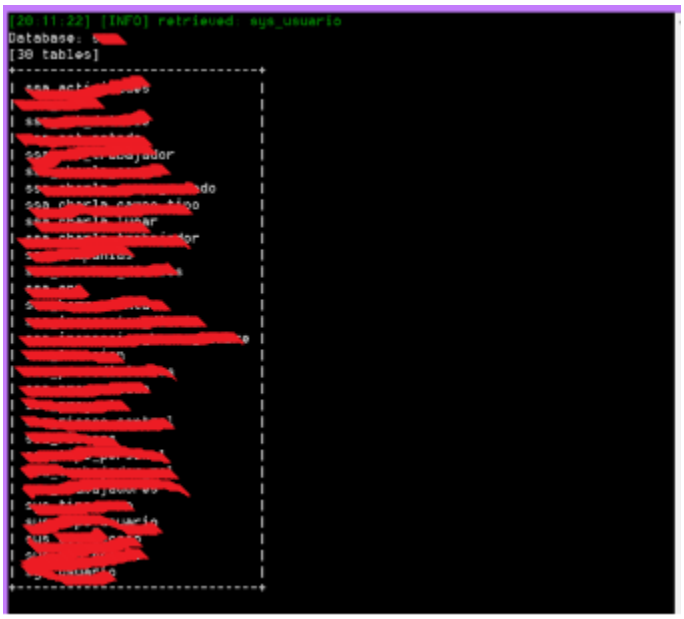
Anexo 17. SQLMAP. Fuente: Autor



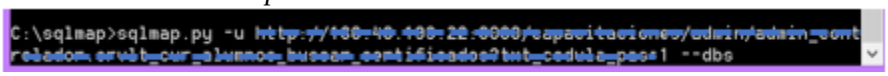
Anexo 18. Bases de datos de la institución B. Fuente: Autor



Anexo 19. Tablas de la institución B. Fuente: Autor



Anexo 20. Recuperación de las bases de datos. Fuente: Autor



Anexo 21. Recuperación de las Tablas. Fuente: Autor

Anexo 22. Ficha de Observación.

FICHA DE OBSERVACIÓN			
FICHA N°		**Fecha y Duración:**	
ELABORADO POR:			
LUGAR:			
LO OBSERVADO		**DETALLE**	

Anexo 23. Validación de la lista de chequeo. Fuente: Autor

Esmeraldas, 15 de febrero de 2018

CERTIFICACIÓN VALIDACIÓN DE INSTRUMENTOS

Quien suscribe, Msc. Kléber Posligua Flores, profesor de esta Sede Universitaria de la PUCE, certifica que revisó, valoró y aprobó los instrumentos del trabajo de Investigación del estudiante Alexander Caicedo Alcivar, consistentes en encuestas a instituciones del área de Sistemas de la ciudad de Esmeraldas.

El interesado puede dar al presente documento el uso que estime conveniente.

Atentamente,

Mgt. Kléber Posligua Flores

Docente PUCE