ISSN: 2594-0937

REVISTA ELECTRÓNICA MENSUAL

Debates sobre Innovación

DICIEMBRE 2019

VOLUMEN 3
NÚMERO 1

XVIII Congreso Latino Iberoamericano de Gestión Tecnológica
ALTEC 2019 Medellín

UNIVERSIDAD AUTÓNOMA METROPOLITANA
Casa abierta al tiempo
Unidad Xochimilco

MEGI
MAESTRÍA EN ECONOMÍA, GESTIÓN Y POLÍTICAS DE INNOVACIÓN

LALICS
LATIN AMERICAN NETWORK FOR ECONOMICS OF LEARNING, INNOVATION AND COMPETENCE BUILDING SYSTEMS

Asistente Virtual en el Sistema de Gestión Seguridad de la Información para Gestor de Base de Datos ORACLE

Jeanneth Alvarado Abarca
Universidad Nacional, Académica, Costa Rica
holajanet@gmail.com

Josué Naranjo Cordero
Universidad Nacional, Académico, Costa Rica
jnaranjo@una.cr

Pablo Chaves Murillo
Universidad Nacional, Académico, Costa Rica
pchaves11@gmail.com

Resumen

El riesgo nunca es totalmente eliminable, por lo que es necesario definir una estrategia de aceptación de riesgo y especificar los niveles de riesgo aceptable. Lo primordial de la metodología es que los resultados obtenidos sean comparables y repetibles para evitar grados de subjetividad que falseen la valoración de los riesgos. Una estrategia de evaluación de riesgos en una organización puede efectuarse siguiendo la norma internacional ISO 27000, mediante el modelo de Planificar-Hacer-Verificar-Actuar, los cuales se aplican para estructurar todos los procesos de la norma. La solución propuesta en este trabajo brinda soporte al SGSI mediante un Sistema de Información, siguiendo el modelo PDCA de la Norma ISO 27001. Con tres simples pasos: Guardar una consulta SQL, ejecutar automáticamente la consulta mediante parámetros que definan la ejecución y enviar correos electrónicos con los resultados a las direcciones que el sistema seleccione.

Palabras clave
Riesgo, ISO, 27000, 27001

1 Introducción

Las organizaciones cada día dependen más de los sistemas informáticos, la mayoría de las empresas dependen de sistemas de información que gestionan los datos, es decir, la información más valiosa que tiene la compañía. Resguardar dicha información aumenta el espectro de riesgos a la que se ve expuesta: atacantes informáticos, robo, destrucción, filtración o extorsión por información confidencial son algunos ejemplos de los riesgos a los que se expone la información.

La forma más sencilla de dar respuesta a las necesidades de información para la toma de decisiones con relación a la gestión del riesgo es mediante el desarrollo de aplicaciones o adquiriendo una herramienta capaz de facilitar y realizar de forma automatizada algunas de las tareas de proceso de análisis y gestión de riesgos, especialmente aquellas que manualmente san más costosas.

Ante el crecimiento exponencial que tienen los servicios informáticos y el océano de datos que se generan día a día en las organizaciones, minimiza la capacidad de los funcionarios de control interno, auditoría o seguridad de la información de realizar controles manuales de forma eficiente y oportuna. De manera que, si la organización está siendo objetivo de un ataque informático

malicioso o hay una fuga de información confidencial, la detección por medio de los mecanismos manuales no es la óptima.
Ante esta situación surge la necesidad de crear herramientas informáticas que automaticen los procesos de control y monitoreo de la seguridad, brindando soporte a los sistemas de gestión de seguridad informática.

2 Objetivos

Objetivo general

Brindar soporte al SGSI mediante el modelo PDCA seguido en la Norma ISO 27001 y al cumplimiento de los Principios de Auditoría establecido en la Norma ISO 19011 mediante un Sistema de Información para el Seguimiento de Transacciones.

Objetivos específicos

- Planificar procesos realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados, utilizando comparaciones con datos parametrizables de acuerdo con lo establecido por la auditoría interna.
- Implantar consultas que se ejecuten de forma automática sobre una base de datos definida para propósitos de auditoría.
- Enviar alertas por medio de correo electrónico a los funcionarios encargados de realizar las evaluaciones correspondientes de acuerdo con las transacciones analizadas con el objetivo revisar y evaluar el desempeño.
- Generar reportes que ayuden a generar acciones correctivas y preventivas, cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

3 Marco Teórico

Auditoría

Desde el enfoque que nos dirigimos en este trabajo, debemos retomar algunos conceptos importantes para dar un soporte teórico a esta propuesta.
Auditoría, según textos encontrados en la ISO 19011:2011, es un proceso sistemático, independiente y documentado para recolectar las evidencias y evaluarlas con el propósito de que se cumplan los criterios de la auditoría.
Según la definición de Ron Weber, El proceso de recolectar y evaluar evidencia para determinar si un sistema informático protege los activos, mantiene la integridad de los datos, alcanza los objetivos de la organización de manera eficaz y consume recursos eficientemente.
La Auditoría Informática reúne las características anteriores agregando el enfoque que se le debe dar a los sistemas informáticos, manteniendo la integridad de los datos y llevando a cabo los fines de la organización con la utilidad eficaz de los recursos.
Además, podemos distinguir distintas clases de auditorías, dependiendo de las personas que la ejecuten. Tenemos Auditorías Externas cuando los auditores son personas ajenas a la organización contratadas por la misma organización o bien ordenadas por medios judiciales. Tenemos las Auditorías Internas, que en nuestro caso son las que nos interesa, porque se realizan por las personas dentro de la organización que tienen acceso y medios para establecer los procesos que garanticen los objetivos de la auditoría.

¿Qué es SGSI?

SGSI es el nombre en siglas para referirse a un Sistema de Gestión de la Seguridad de la Información. La seguridad de la información conlleva la preservación y conservación de tres de

sus atributos que serían: confidencialidad, integridad y disponibilidad, adicionalmente se debe tener en cuenta la trazabilidad y la autenticidad de la información, así como de los sistemas implicados en su tratamiento, dentro de una organización.
Para asegurar que la seguridad de la información sea gestionada de manera adecuada se debe asegurar los aspectos relevantes:

- Confidencialidad: La información no debe ser accedida por quien no tenga la autorización. No debe confundirse con privacidad que es solamente un grado de confidencialidad
- Integridad: la información debe ser exacta y completa. No debe tener alteraciones no autorizadas
- Disponibilidad: la información debe estar disponible para su acceso y utilización

El estándar ISO 27001, sistema de gestión de la seguridad de la información, establece los requisitos para la gestión del SGSI y su auditoría.
La familia de la ISO 27000

- 27001- Requerimientos del SGSI
- 27002- Buenas prácticas en seguridad
- 27003- Gestión del riesgo en el SGSI
- 27004- Métricas y mediciones del SGSI
- 27005- Guía de implementación del SGSI
- 27006 en adelante- Diferentes temas de la seguridad de información.

La norma ISO 27001 describe los requisitos de un sistema de gestión de la seguridad de la información. Es la base del proceso de auditoría y certificación de los sistemas de seguridad de información de las organizaciones.

Integración de los Sistemas de Gestión
Los Sistemas de Gestión, son integrables entre sí, ya que contemplan partes comunes que se pueden realizar y documentar a la vez, lo que facilita su implementación.

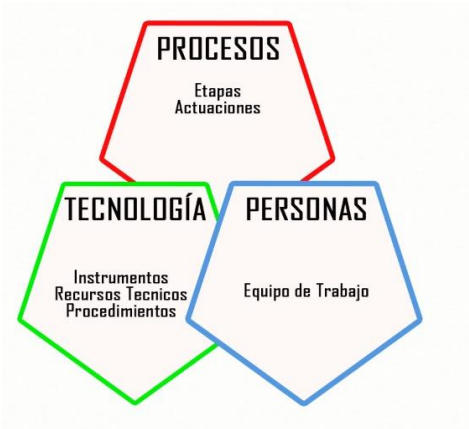


Figura 1, Integración de Sistemas de Gestión. (Elaboración propia)

Sistemas gestores de bases de datos (SGBD)

Los sistemas gestores de bases de datos son sistemas informáticos especializados en gestionar grandes cantidades de información, proporcionar fiabilidad de la información almacenada, proveer mecanismos para la manipulación de la información, y definir estructuras para almacenar los datos. (A. Silberschatz, H. Korth, S. Sudarshan, 2002).

Oracle

Oracle Corporation es una de las mayores compañías de software del mundo. Sus productos van desde bases de datos (Oracle) hasta sistemas de gestión. Cuenta, además, con herramientas propias de desarrollo para realizar potentes aplicaciones, como Oracle Designer, o JDeveloper. Oracle surge a finales de los 70 bajo el nombre de Relational Software a partir de un estudio de George Koch sobre los sistemas gestores de base de datos que Computer World definió como uno de los más completos jamás escritos sobre la materia. Este artículo incluía una comparativa de productos que erigía a Relational Software como el más completo desde el punto de vista técnico. Esto se debía a que usaba la filosofía de las bases de datos relacionales, algo que en ese tiempo era desconocido.

(Mejia, 2009)

Oracle tiene su sede en la localidad californiana de Redwood City, Estados Unidos. La tecnología Oracle se encuentra prácticamente en todas las industrias del mundo y en las oficinas de 98 de las 100 empresas Fortune 100. Oracle es el proveedor mundial líder de software para administración de información, muy por delante de la segunda empresa de su segmento.(Mejia, 2009).

Arquitectura de un sistema de bases de datos.

La arquitectura de un sistema de bases de datos está influenciada por el sistema informático en el que se ejecuta, en particular por aspectos como la conexión en red, el paralelismo y la distribución. (A. Silberschatz, H. Korth, S. Sudarshan, 2002).

La distribución de datos a través de las distintas sedes o departamentos de una organización permite que estos datos residen donde han sido generados o donde son más necesarios, pero continúan siendo accesibles desde otros lugares o departamentos diferentes. (A. Silberschatz, H. Korth, S. Sudarshan, 2002).

Sistemas de Bases de Datos Auditables

La auditoría informática es una situación creciente y con nuevos retos, se debe considerar la recolección de pistas de auditoría, que son vitales para la tarea del auditor, no se conocen soluciones integrales que sean capaces de interactuar con cualquier gestor de bases de datos y que les permita definir el mundo de cambios a auditar. Eso hace que los auditores deban seleccionar diferentes soluciones dependiendo de la infraestructura de datos del modelo auditado. Es importante mencionar los componentes auditables de una base de datos: los esquemas, las tablas, las restricciones; estos componentes son objeto del desarrollo de este trabajo.

4 Diseño Metodológico.

Mediante el círculo de Deming, o conocido como PDCA (plan-do-check-act) se sigue una metodología recomendada para la implementación de este trabajo.

Después de implementado el software que aporta el generador de las consultas y alertas a la auditoría interna, se establecen pasos sencillos para fortalecer la seguridad en la información de las organizaciones de manera continua, disminuyendo faltas, mejorando eficacia y eficiencia, previniendo riesgos y resolviendo problemas. El método Deming está dividido en 4 etapas en un

solo ciclo, de manera que al finalizar se reinicia de nuevo y así sistemáticamente, pero con la salvedad que las actividades son mejoradas a medida que se revisan y son revalidadas, por medio de la misma metodología.
De manera que, siguiendo los pasos del ciclo, vamos a implementar los procesos a seguir para ingresar alertas al software propuesto en este trabajo:

1. Se hacen reuniones con el equipo de autoría interna de la organización, siendo necesario que un técnico o desarrollador sea parte del equipo y cuente con conocimiento amplio de los esquemas y contenidos de la Base de Datos de la entidad. De esta reunión surgen revisiones que pueden ser planteadas por medio de consultas de datos.
2. Se realizan las consultas, se ingresan al software con todos los datos y parámetros que se definieron en la reunión de equipo. Muy importante es tomar en cuenta que los resultados de estas consultas representan los hallazgos de la auditoría interna, de manera que los destinatarios de los correos que contienen los hallazgos deben de ser bien analizados y aprobados. Se recomienda que se realicen pruebas iniciales con destinatarios del mismo departamento de la auditoría interna, luego de que se repita el ciclo metodológico.
3. El paso de chequeo es cuando son revisadas las alertas que han sido enviadas por la herramienta por medio de los correos, este paso puede ser una etapa del ciclo que sea analizada por algunos miembros de la auditoría interna, eso dependerá de lo que se establece en el paso de planeamiento.
4. Como último paso, cuando se termina el ciclo, se analizan los resultados de todas las consultas ejecutadas y que han generado alertas, se pueden clasificar como hallazgos de auditoría o bien como recomendaciones internas para la modificación o implementación permanente de revisiones, en algunos casos podrían eliminarse consultas si así se considera prudente.

Este tipo de metodología o ciclo puede aplicarse a varios principios como acciones, que pueden ser correctivas, preventivas y de mejoramiento. En este caso, la metodología cumple con todas las acciones mencionadas porque en un SGSI aplicado por un departamento de auditoría interna, las búsquedas y revisiones son de todos estos tipos y pueden ser implementadas como consultas en una Base de Datos.

5 Propuesta del sistema de apoyo a la auditoría

El sistema de Información para el Seguimiento de Transacciones es una herramienta para ser utilizada por un funcionario de la Auditoría Interna con conocimientos específicos en consultas de base de datos, la generación de consultas y la revisión de las alertas estarán a cargo del departamento de Auditoría Interna.
El sistema realiza consultas a la base de datos, utilizando el esquema general de datos, mediante un proceso almacenado que se ejecute de forma automatizada, preferiblemente en horas no laborales porque beneficia la eficiencia de las consultas al no estar activas las distintas transacciones de la organización.
Esta herramienta aporta un proceso que apoya el SGSI, especialmente mediante el modelo Planear-Hacer-Revisar-Verificar, porque permite crear consultas directamente en los datos de la organización, los resultados de las consultas representan alertas a la auditoría interna que procura la seguridad de la información de la organización. Los rastreos de datos y procesos sospechosos pueden ubicarse en los datos del sistema de Base de Datos y también en los datos transaccionales de la empresa.
Para la implementación del software, se proponen consultas predefinidas y modificables que

apoyen directamente la Auditoría en la seguridad de la información.
A continuación, se listan consultas que tienen implicación directa con la seguridad de la información:

Usuarios con perfil por defecto

En Oracle se crean usuarios y se les asigna un perfil (PROFILE) el cual es asignado de acuerdo con los privilegios que se le definen a cada nuevo usuario. Existen casos donde no es asignado un perfil, lo cual permite que el usuario tenga un perfil por defecto (DEFAULT), esto representa un alto riesgo porque el usuario tendrá muchos privilegios y no debe ser permitido, de manera que se genera una alerta que muestra todos los usuarios su PROFILE sea DEFAULT.

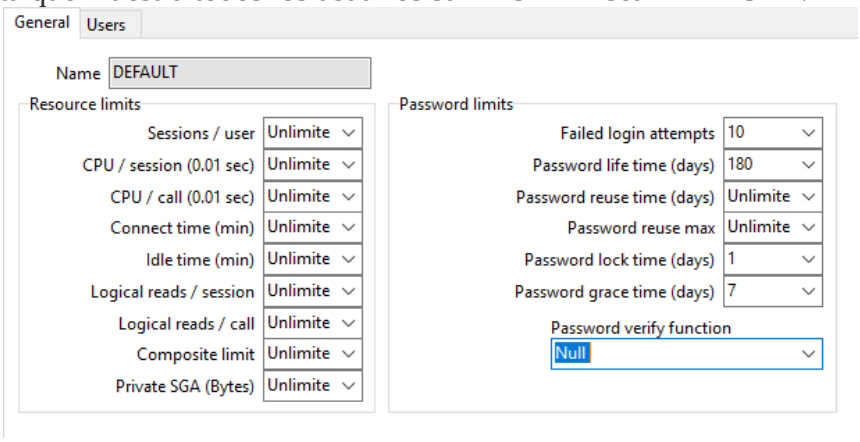


Figura 2, Permisos de un usuario DEFAULT. (Elaboración propia)

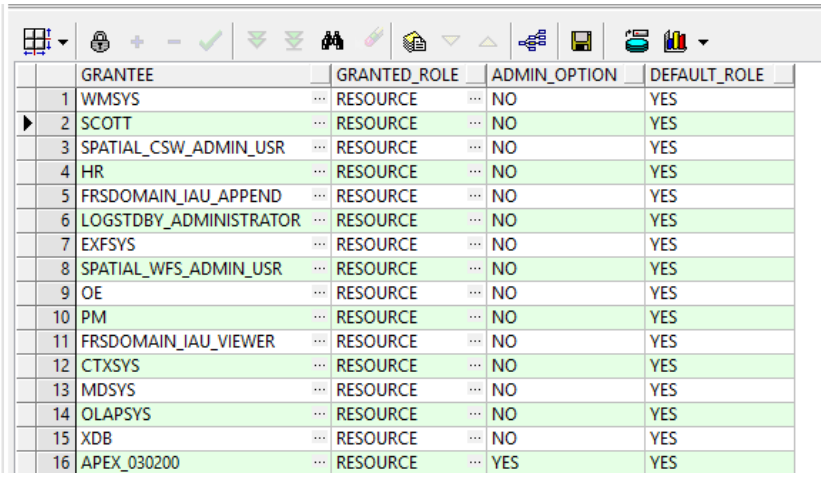
Consulta de usuarios con perfil DEFAULT:

- select t.* from dba_users t where profile='DEFAULT';

Esquemas existentes en la Base de Datos

Un esquema en Oracle se define con la asignación del privilegio “Resource”.
Una consulta importante para la auditoría interna es conocer la lista de esquema existentes de manera periódica, para hacer comparaciones del crecimiento o cambios de los esquemas de la base de datos.
Consulta de lista de ESQUEMAS EXISTENTES:

- select * from dba_role_privs where GRANTED_ROLE='RESOURCE';



	GRANTEE	GRANTED_ROLE	ADMIN_OPTION	DEFAULT_ROLE
1	WMSYS	RESOURCE	NO	YES
2	SCOTT	RESOURCE	NO	YES
3	SPATIAL_CSW_ADMIN_USR	RESOURCE	NO	YES
4	HR	RESOURCE	NO	YES
5	FRSDOMAIN_IAU_APPEND	RESOURCE	NO	YES
6	LOGSTDBY_ADMINISTRATOR	RESOURCE	NO	YES
7	EXFSYS	RESOURCE	NO	YES
8	SPATIAL_WFS_ADMIN_USR	RESOURCE	NO	YES
9	OE	RESOURCE	NO	YES
10	PM	RESOURCE	NO	YES
11	FRSDOMAIN_IAU_VIEWER	RESOURCE	NO	YES
12	CTXSYS	RESOURCE	NO	YES
13	MDSYS	RESOURCE	NO	YES
14	OLAPSYS	RESOURCE	NO	YES
15	XDB	RESOURCE	NO	YES
16	APEX_030200	RESOURCE	YES	YES

Figura 3, Esquema con privilegios. (Elaboración propia)

Asignar cuota a los usuarios por tablespace

A cada usuario se le debe asignar una cuota de espacio para cada tablespace, esto permite que los usuarios con privilegios puedan crear los objetos en las tablespace asignados, también se limita el espacio para almacenar los objetos que el usuario pueda crear.

Cuando este valor de cuota no esta siendo asignado, se genera una alerta a la Auditoría para que se realice una revisión.

Ejemplo de una consulta con cuotas asignadas:

```
CREATE USER jward
 IDENTIFIED BY password
 DEFAULT TABLESPACE data_ts
 QUOTA 100M ON test_ts
 QUOTA 500K ON data_ts
 TEMPORARY TABLESPACE temp_ts
 PROFILE clerk
 CONTAINER = CURRENT;
```

Figura 4, Quotas. (Elaboración propia)

Seguridad de profile / Perfiles sin restricciones

Una consulta a la tabla de perfiles puede devolver información importante para la auditoría, es una alerta importante, cuando existen perfiles que tengan alguna opción ilimitada.

Consulta de lista de perfiles con opciones ILIMITADAS:

- select distinct t.profile from Dba_Profiles t where LIMIT='UNLIMITED';

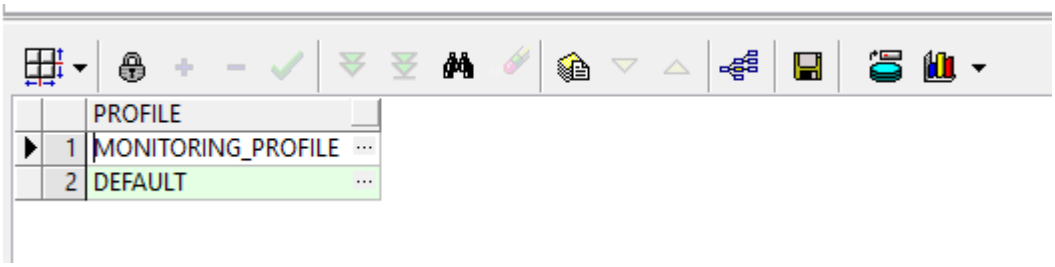


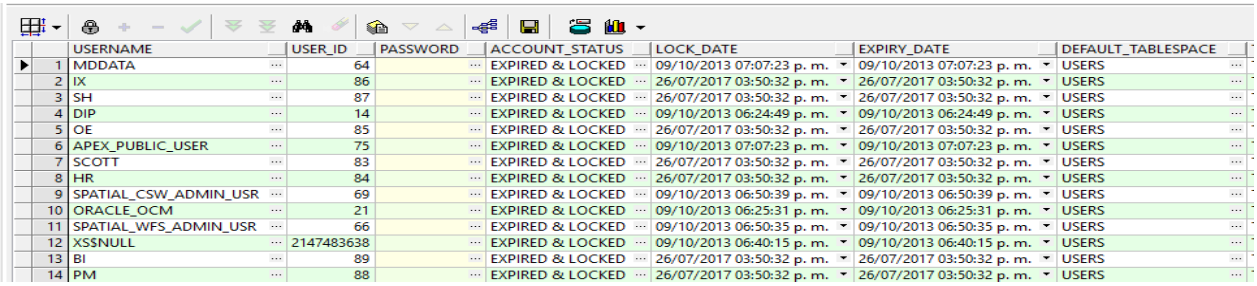
Figura 5, Lista perfiles con opciones ilimitadas. (Elaboración propia)

Usuarios bloqueados

Una consulta importante para auditar la seguridad de la base de datos es verificar periódicamente los usuarios que se encuentran bloqueados.

Consulta de lista de usuarios bloqueados:

- select t.* from dba_users t where DEFAULT_TABLESPACE='USERS' and ACCOUNT_STATUS!='OPEN';



	USERNAME	USER_ID	PASSWORD	ACCOUNT_STATUS	LOCK_DATE	EXPIRY_DATE	DEFAULT_TABLESPACE
1	MDDATA	64		EXPIRED & LOCKED	09/10/2013 07:07:23 p. m.	09/10/2013 07:07:23 p. m.	USERS
2	IX	86		EXPIRED & LOCKED	26/07/2017 03:50:32 p. m.	26/07/2017 03:50:32 p. m.	USERS
3	SH	87		EXPIRED & LOCKED	26/07/2017 03:50:32 p. m.	26/07/2017 03:50:32 p. m.	USERS
4	DIP	14		EXPIRED & LOCKED	09/10/2013 06:24:49 p. m.	09/10/2013 06:24:49 p. m.	USERS
5	OE	85		EXPIRED & LOCKED	26/07/2017 03:50:32 p. m.	26/07/2017 03:50:32 p. m.	USERS
6	APEX_PUBLIC_USER	75		EXPIRED & LOCKED	09/10/2013 07:07:23 p. m.	09/10/2013 07:07:23 p. m.	USERS
7	SCOTT	83		EXPIRED & LOCKED	26/07/2017 03:50:32 p. m.	26/07/2017 03:50:32 p. m.	USERS
8	HR	84		EXPIRED & LOCKED	26/07/2017 03:50:32 p. m.	26/07/2017 03:50:32 p. m.	USERS
9	SPATIAL_CSW_ADMIN_USR	69		EXPIRED & LOCKED	09/10/2013 06:50:39 p. m.	09/10/2013 06:50:39 p. m.	USERS
10	ORACLE_OCM	21		EXPIRED & LOCKED	09/10/2013 06:25:31 p. m.	09/10/2013 06:25:31 p. m.	USERS
11	SPATIAL_WFS_ADMIN_USR	66		EXPIRED & LOCKED	09/10/2013 06:50:35 p. m.	09/10/2013 06:50:35 p. m.	USERS
12	XS$NULL	2147483638		EXPIRED & LOCKED	09/10/2013 06:40:15 p. m.	09/10/2013 06:40:15 p. m.	USERS
13	BI	89		EXPIRED & LOCKED	26/07/2017 03:50:32 p. m.	26/07/2017 03:50:32 p. m.	USERS
14	PM	88		EXPIRED & LOCKED	26/07/2017 03:50:32 p. m.	26/07/2017 03:50:32 p. m.	USERS

Figura 6, Lista de usuarios bloqueados. (Elaboración propia)

Modificación de datos sin usuario

En Oracle existen usuarios y esquemas, los dos funcionan para ingresar a la base de datos con un nombre y una contraseña. La diferencia es que el esquema puede crear objetos (tablas, procedimientos, paquetes, vistas, disparadores, funciones) y el usuario solo puede utilizarlos.

Una buena recomendación es que debe existir la bitácora para las tablas principales de los sistemas, en caso de que exista, se debe verificar e incluir los datos del equipo, usuario, fecha, tabla, campos, valor nuevo, valor antiguo. Sobre esta tabla se puede verificar que las acciones sean realizadas por un usuario y no un esquema.

Adicional a las consultas predefinidas anteriores, también se hacen propuestas alternas para apoyar las normas ISO relacionadas con la seguridad de la información. Con estas propuestas pretendemos aportar ideas para conocer la capacidad del software y de este trabajo.

A continuación, se presentan acciones que pueden ser tratadas con el software, apoyadas en las normas ISO y con implicaciones en la seguridad de la información de las organizaciones:

- Monitoreo continuo de acuerdo con la ISO 27005 en su cláusula 12, donde estipula que las organizaciones deben asegurarse de que se supervise continuamente los nuevos activos que se incluyan en la gestión de riesgos, así como cualquier modificación que a estos se realice. Por lo tanto, las actividades de monitoreo de riesgos deben repetirse regularmente y las opciones seleccionadas para el tratamiento de riesgos deben revisarse periódicamente. Para este tipo de monitoreo se pueden generar consultas que puedan realizar las revisiones periódicamente, agregando así a la organización un tipo de auditoría en los riesgos posibles y cuando ocurran cambios importantes en los activos mencionados.
- Monitoreo continuo de acuerdo con ISO 27005 en su cláusula 9, donde se definen la modificación de los riesgos. Por medio de este software, se generan consultas que definan los controles necesarios para la aceptación y el monitoreo de los riesgos aceptados por la organización. Por ejemplo, debilidades técnicas, como la capacidad de administración (requisitos de soporte operativo) pueden impedir el uso de ciertos controles o inducir un error humano anulando el control, por ejemplo, en la creación de contraseñas robustas, por falta de capacitación adecuada los usuarios pueden escribir contraseñas débiles. Es un punto de control común en las revisiones de auditoría, que se debe hacer periódicamente, utilizando el software mencionado, este tipo de riesgo se minimiza o se elimina, ya que el monitoreo del control es permanente y los hallazgos se canalizan a la persona adecuada para su tratamiento y mejora.

Vamos a llamar ALERTAS a las ideas que generan las consultas que alimentan el sistema o ASISTENTE VIRTUAL.

El sistema realiza tres funciones específicas:

- **Guardar una consulta SQL**, para realizar esta función se utiliza una herramienta de consulta opcional, se crea la consulta SQL, se valida y luego se guarda el archivo tipo sql para que el sistema lo cargue y almacene.
- **Ejecutar automáticamente la consulta**, se realiza un proceso automático diario. Las consultas deben tener parámetros que definan la ejecución específica para cada consulta:
    - Un dato que defina si la consulta se encuentra activa.
    - La cantidad de días que definan la periodicidad de la consulta.
    - La fecha de la última vez que se realizó la consulta.
- **Enviar correos electrónicos,** de acuerdo con los resultados de las consultas, el sistema debe enviar correos a las direcciones que el sistema seleccione. Los destinatarios por puesto, cada puesto debe tener un funcionario a cargo y la dirección de correo electrónico. Cada correo enviado debe tener los siguientes datos:
    - Remitente:
    - Destinatario(s)
    - Asunto
    - Líneas para mensajes
    - Líneas de datos, estos dependen de cada consulta.

Generación de alerta por funcionarios externos a la Auditoría

Las consultas que se ingresen al asistente virtual pueden surgir de distintas fuentes, todas las ideas externas a la Auditoría Interna son aportes valiosos, la proyección es que el sistema sea alimentado por los mismos funcionarios que con las experiencias e ideas puedan generar alertas.
Para eso se crea un canal de comunicación entre los funcionarios y la Auditoría Interna. El medio es el correo interno y las alertas nacen de una consulta que debe ser enviada al funcionario a cargo.

Para este fin se solicitan los siguientes datos:

- **Consulta**: Un texto descriptivo de la solicitud, se debe especificar con detalles la lógica de la consulta, procurando utilizar los datos y/o parámetros del sistema.
- **Destinatarios**: Asignar el o los funcionarios a quienes deben llegar el correo de Alerta.
- **Asunto**: aquí se describe brevemente el interés principal de la consulta. Ejemplo: Usuario sin Autorización, Contraseña Débil, Consultas repetitivas, etc....
- **Mensaje de Alerta**: se describe más extenso y describiendo los parámetros, la idea que genera la consulta. Ejemplo: Se ha realizado un intento de ingreso al esquema XX con un usuario inválido.
- **Datos**: se detallan los datos que deben incluirse en el mensaje del correo. Ejemplo:
    - Fecha
    - Tabla, esquema o aplicación de BD.
    - Usuario
    - Intentos
- **Mensaje de pie**: Un texto con una indicación general. Ejemplo: Favor proceder a revisar el usuario xyz.

- **Periodicidad**: Es recomendable establecer una periodicidad en días para la ejecución de las consultas, pueden ejecutarse automáticamente una vez al día o cumpliendo con los períodos que se establezca.
- **Estado de la consulta**: Este parámetro establece si la consulta está activa o inactiva, es importante que los responsables de las consultas ingresadas al sistema reporten al encargado si la consulta pierde efectividad o importancia, de manera que se pueda inactivar la ejecución de dicha consulta, esto evita el envío de correos innecesarios y ayuda a mejorar el rendimiento del proceso automático de ejecución del programa.

6 La propuesta auditoría y seguridad

La propuesta ofrece una forma de realizar consultas y generar alertas que apoyen el SGSI, por este medio se pueden crear alertas que surgen de una eventualidad o de un control auditable, pero se mantienen en el tiempo y permanecen generando revisiones de auditoría aun cuando han pasado los momentos de la generación de la consulta.

Se pueden crear varios tipos de consultas a la base de datos, como una forma de ejecutar controles permanentes o eventos aislados. También se puede generar consultas que alerten a la auditoría interna de los movimientos de usuarios incluyendo el mismo DBA.

El aporte a la organización radica en la generación de controles y auditorías, puede ser de los negocios o transacciones derivadas, o bien de la seguridad establecida por la empresa para los movimientos de los datos almacenados en la base de datos.

Este trabajo no solo representa seguridad a niveles grandes de transacciones en donde es difícil tener el control de los movimientos de la información, sino también es un aporte para las pequeñas y medianas organizaciones que puede apoyarse en esta herramienta para generar y recibir alertas de las transacciones básicas y cotidianas como por ejemplo saldo de efectivo en una organización comercial o bien control de horarios en el departamento de Recursos Humanos.

Existen diferencias notables en una organización después de una implementación de este tipo de software, porque este software ofrece envío de alertas permanentes y automáticas, que después de ser generadas no van a tener que retomarse en futuras revisiones de auditorías, al contrario, la auditoría va a recibir alertas constantes por vía correo electrónico y esto va a mantener un buen sistema de seguridad, estas misma alertas que pudieron surgir de una consulta pasada y olvidada, eventualmente pueden generar nuevas pistas de auditoría al cambiar condiciones de la empresa, o básicamente mantener controles a través del tiempo sin que esto genere carga de trabajo repetido en un departamento de auditoría interna.

7 Diseño y Desarrollo

A continuación, se presenta la propuesta de diseño y desarrollo para el trabajo del software, una propuesta generada de acuerdo con las ideas de cumplir con un SGSI estándar para cualquier tipo y tamaño de organización, a la vez modificable y ajustable de acuerdo con las necesidades de la misma empresa y su herramienta de motor de base de datos.

Esquema de la base de datos

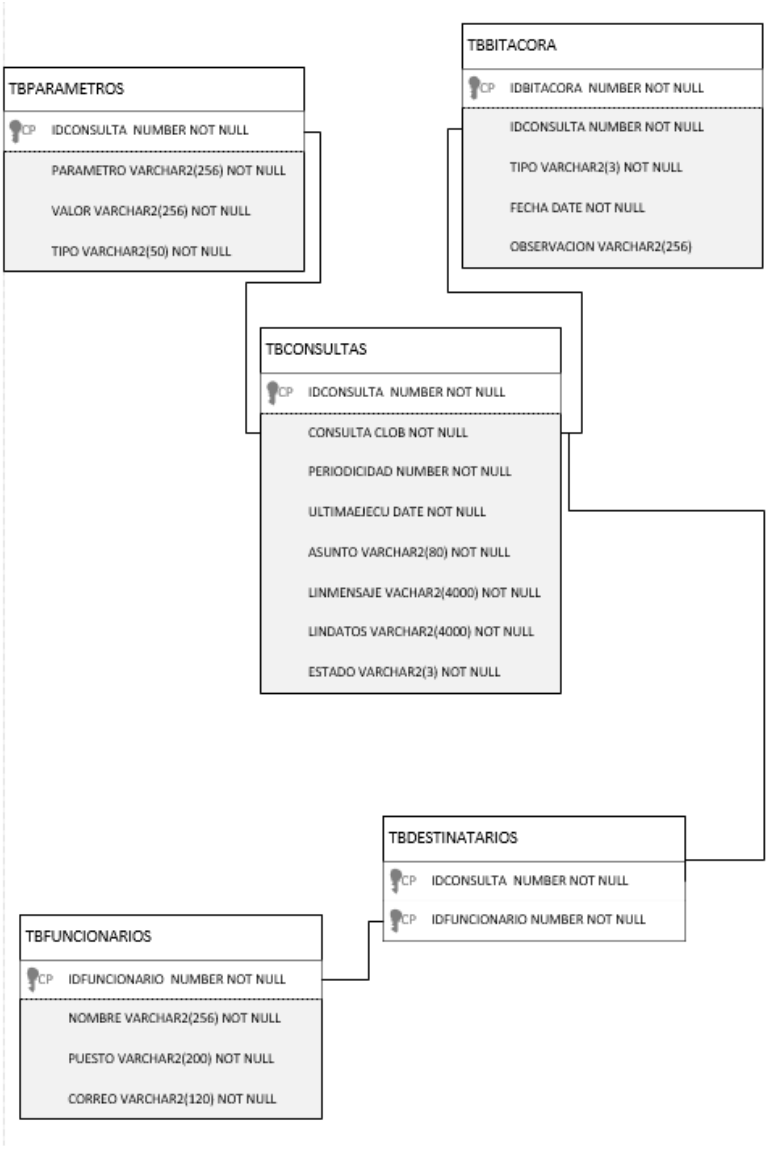


Figura 7, Esquemas de Base de Datos. (Elaboración propia)

Implementación y desarrollo

El desarrollo se dividió en dos segmentos principales, desarrollo de bases de datos y desarrollo de la aplicación.

Bases de Datos

- **Esquema de Bases de Datos**: A nivel de bases de datos, se procedió a crear el esquema TRACKER con las tablas indicadas en el diagrama.

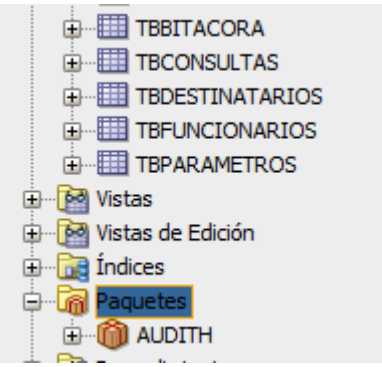


Figura 8, Esquemas creado en base de datos. (Elaboración propia)

- **Paquetes de Bases de Datos:** A nivel de paquetes de bases de datos, se procedió a crear a un paquete denominado "AUDITH" que posee todos los procedimientos almacenados necesarios para el funcionamiento del sistema.

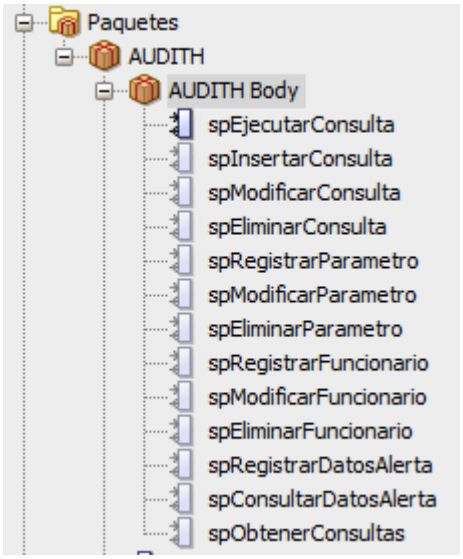


Figura 9, Paquete AUDITH. (Elaboración propia)

- **Tarea programa de la base de datos:** Se crea una tarea programada dentro de la base de datos que ejecute todos los días a la 1:00 a.m., y que ejecute el procedimiento almacenado spEjecutarConsulta.
- **Paquete DBMS_SQL:** Oracle provee el paquete DBMS_SQL cuya característica principal es la de permitir la ejecución dinámica de sentencias SQL con la sintaxis requerida, sustituyendo los parámetros de manera dinámica para evitar inyección SQL.

Aplicación

- **Arquitectura de la aplicación:** La arquitectura de la aplicación fue divida en 3 paquetes:
    - Un paquete de entidades: Donde se encuentran las clases que hacen referencia a las entidades de la base de datos.

- Un paquete de utilitarios: Donde se encuentran las clases que permiten la conexión a bases de datos y el envío de correos electrónicos.
- Un paquete de presentación: Donde se encuentran las pantallas que serán ejecutadas por la aplicación.

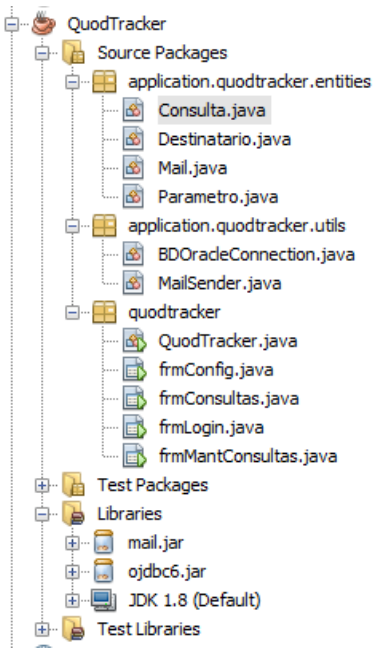


Figura 10, Paquete de la aplicación. (Elaboración propia)

- **Librería JavaMail.** Se utiliza una librería de java, JavaMail es distribuida como software libre para poder enviar los correos electrónicos. Con dicha librería se creó la clase MailSender.java que realiza la comunicación con la plataforma de correo electrónico y a su vez envía el mismo al destinatario indicado.

8 Aportes y Resultados

En esta sección se realizan las pruebas unitarias y se documentará las pruebas del software.

Caso práctico 1: Detección de ataque de fuerza bruta al usuario SYTEM de Oracle.

Teniendo presente que las cuentas por default de Oracle representan un objetivo clave para un atacante (M. Mushfiqur, 2014), se utilizará como caso de prueba la detección de un ataque de fuerza bruta al usuario SYSTEM de Oracle.

- **Registro de Consultas en la aplicación.** La consulta registrada detecta la cantidad de intentos fallidos por parte del usuario SYSTEM.

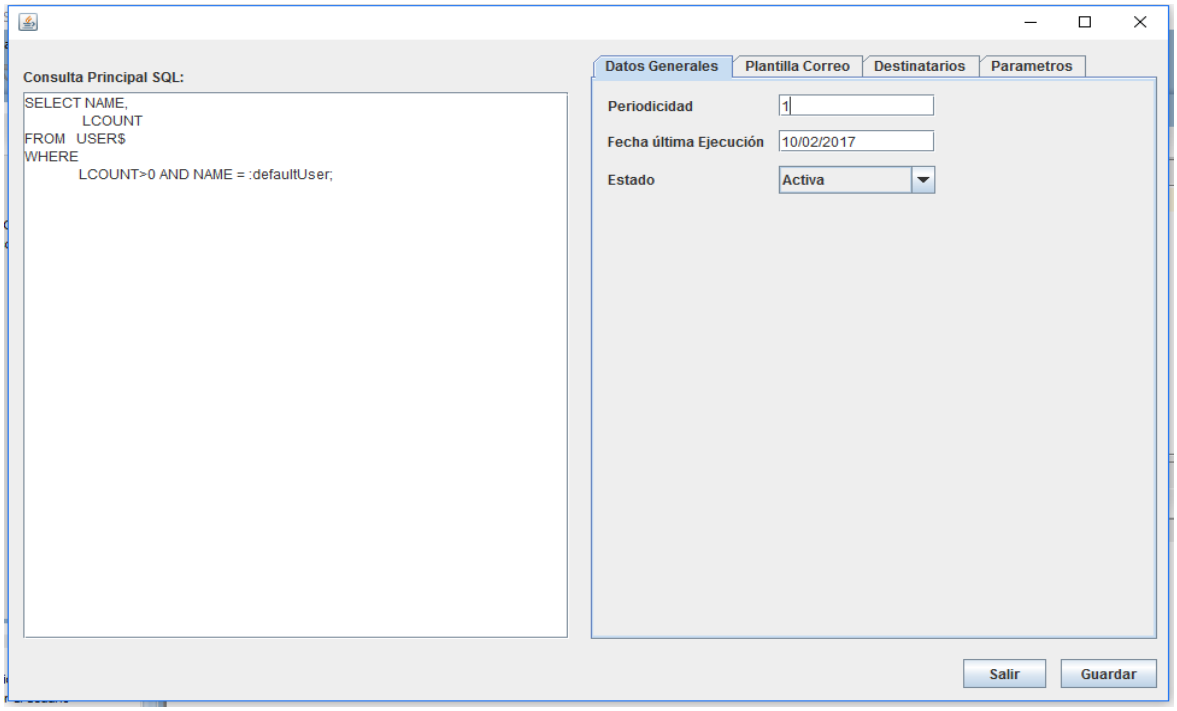


Figura 11, Registro de consulta y datos generales. (Elaboración propia)

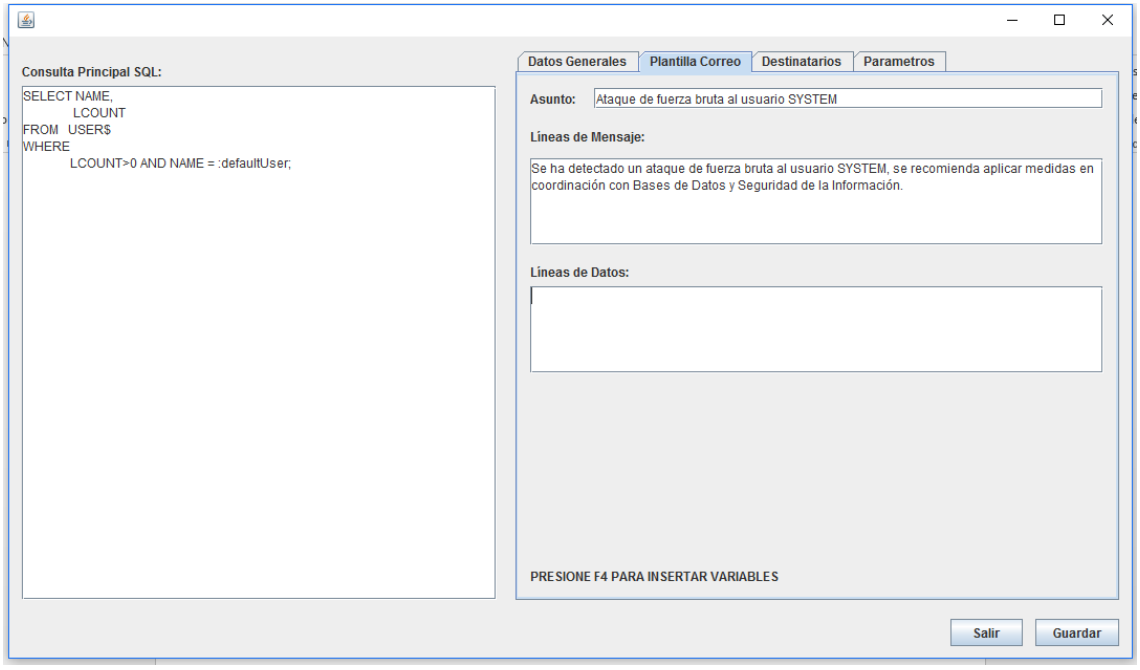


Figura 12, Registro de plantilla de correo asociada. (Elaboración propia)

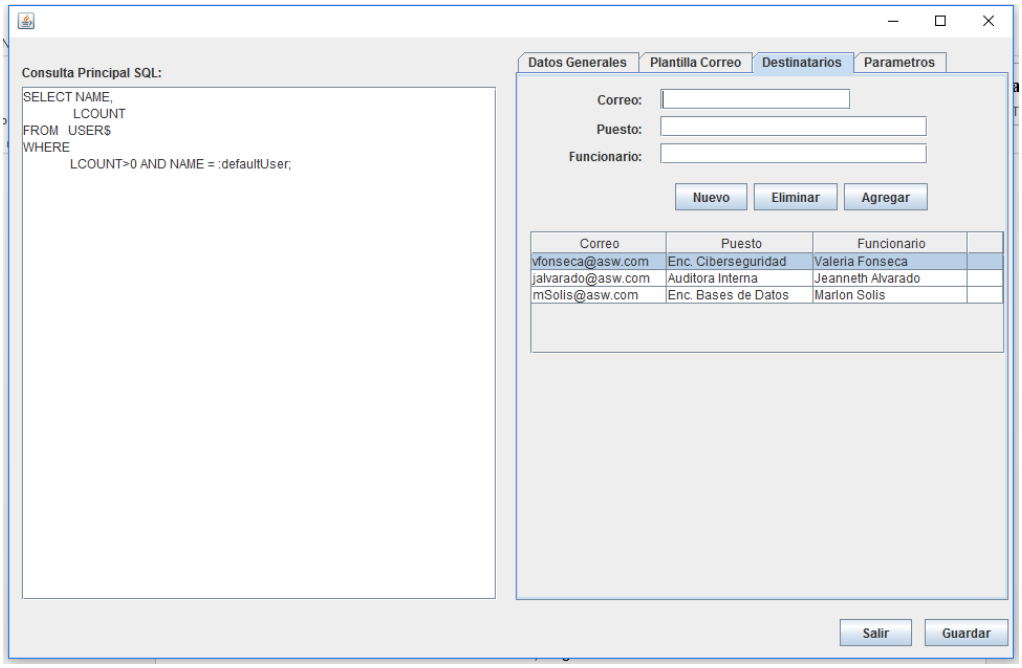


Figura 13, Registro de destinatarios. (Elaboración propia)

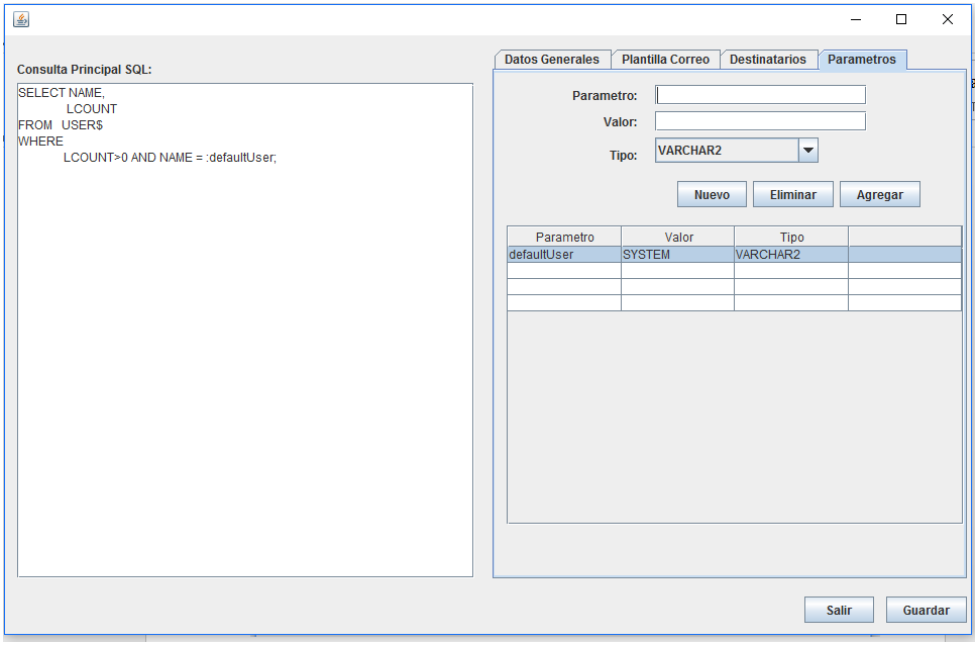


Figura 14, Registro de parámetros. (Elaboración propia)

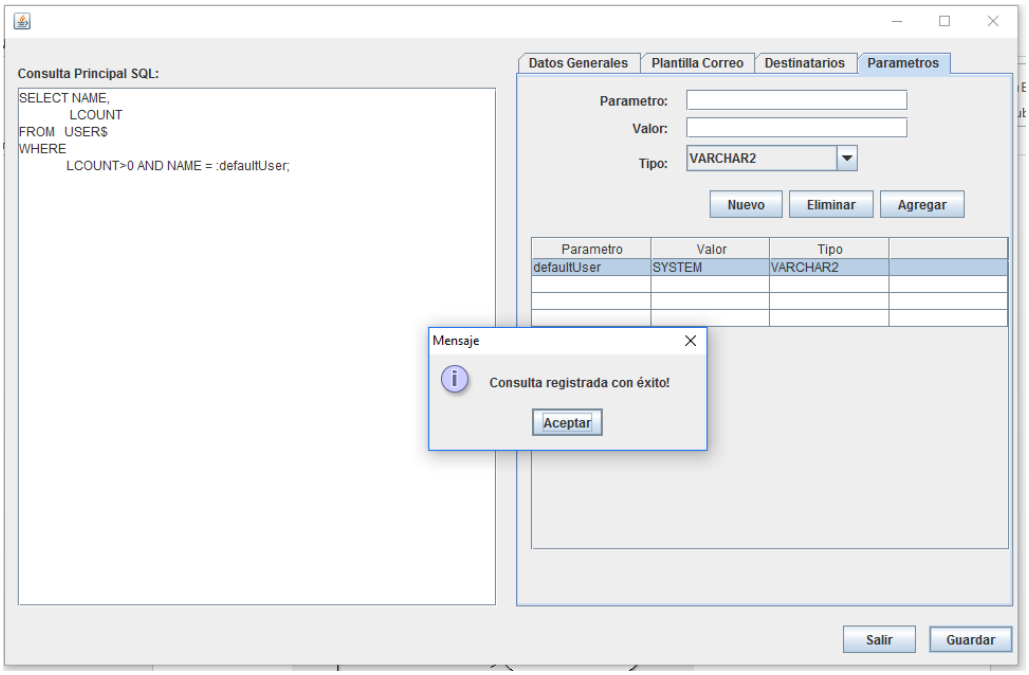


Figura 15, Registro exitosa de la consulta. (Elaboración propia)

- **Ejecución dinámica del paquete DBMS_SQL.**

```
Conectando a la base de datos SYSDB.
USUARIO: SYSTEM
Intentos de Login fallidos: 9
El proceso ha terminado.
Desconectando de la base de datos SYSDB.
```

Figura 16, Ejecución dinámica de la consulta. (Elaboración propia)

- **Alertas en el correo electrónico.**

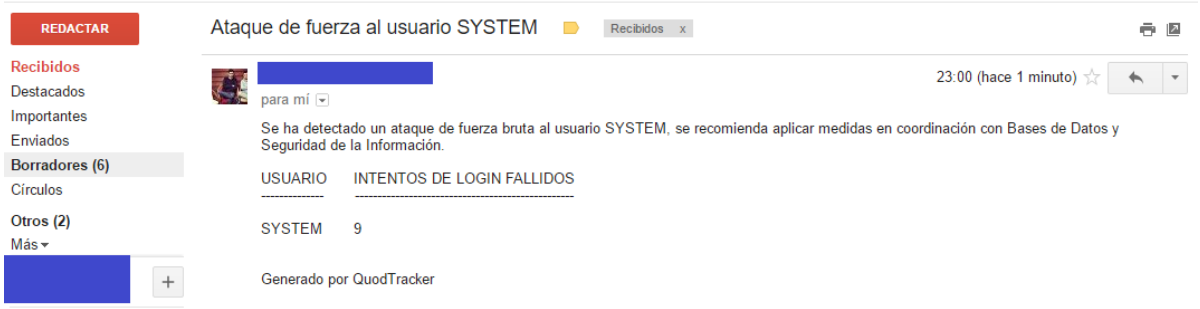


Figura 17, Alerta ataque de fuerza bruta al usuario SYSTEM. (Elaboración propia)

Caso práctico 2: Automatización de monitoreo de seguridad sobre cuentas privilegiadas.

La herramienta propuesta también logra automatizar el monitoreo de seguridad en las bases de datos, ya que el monitoreo dinámico es también un elemento esencial de la evaluación de vulnerabilidad y permite ir más allá de evaluaciones estáticas. (J. Villalobos, 2012).
Uno de los elementos esenciales que deben ser monitoreados son los usuarios privilegiados ya que muchos ataques más comunes se hacen con privilegios de usuario de alto nivel (J. Villalobos, 2012).
Para el ejemplo se pretende monitorear las últimas sentencias SQL ejecutadas por el Administrador de bases de datos con periodicidad diaria que involucren el eliminado de datos de las tablas.

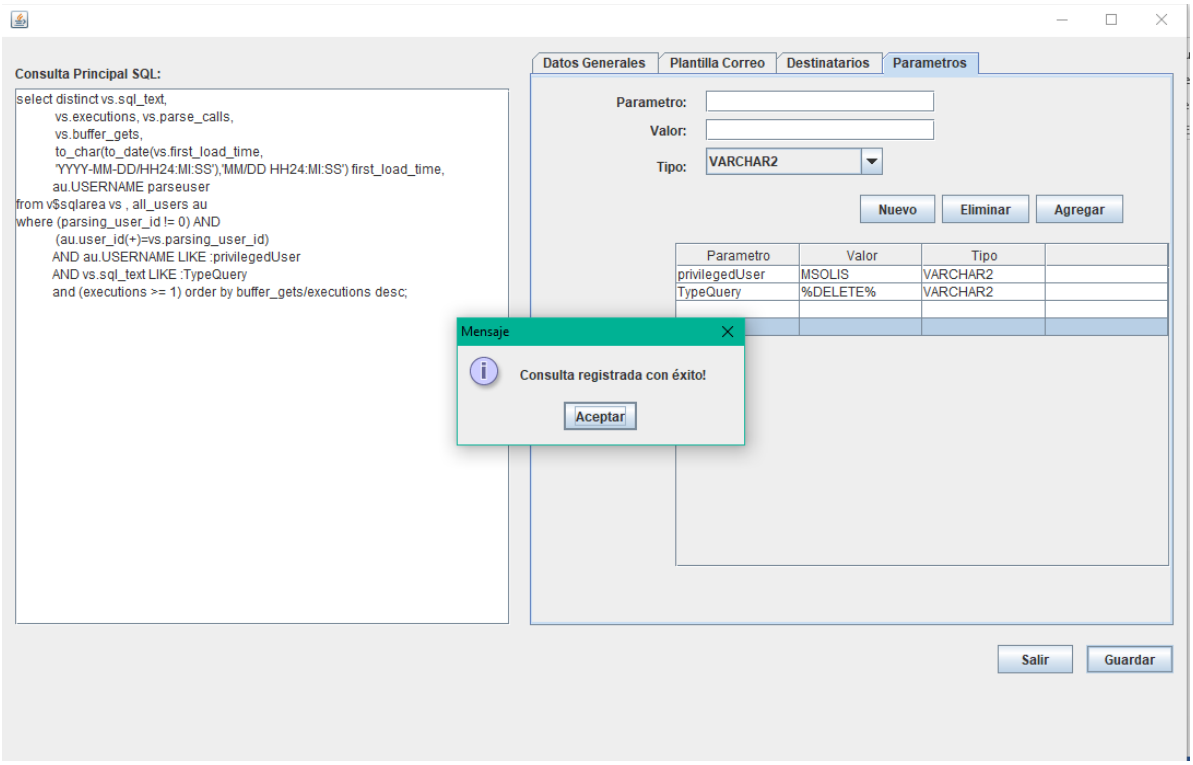


Figura 18, Registro de la consulta SQL para monitorias consultas de los DBA. (Elaboración propia)

A continuación, la consulta:

- select distinct vs.sql_text, vs.executions, vs.parse_calls, vs.buffer_gets, to_char(to_date(vs.first_load_time, 'YYYY-MM-DD/HH24:MI:SS'),'MM/DD HH24:MI:SS') first_load_time,au.USERNAME parseuser from v$sqlarea vs , all_users au where (parsing_user_id != 0) AND (au.user_id(+)=vs.parsing_user_id) AND au.USERNAME LIKE 'TRACKER' AND vs.sql_text LIKE '%DELETE%' and (executions >= 1) order by buffer_gets/executions desc;

Resultado de consulta:

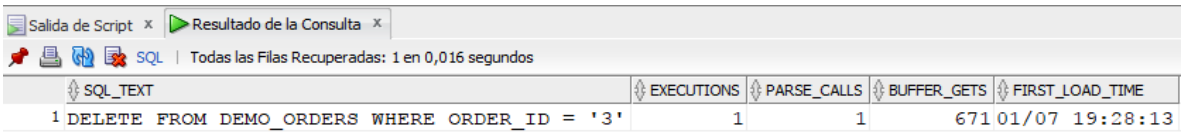


Figura 19, Resultado consulta SQL para monitorear consultas de los DBA. (Elaboración propia)

Correo de la alerta:

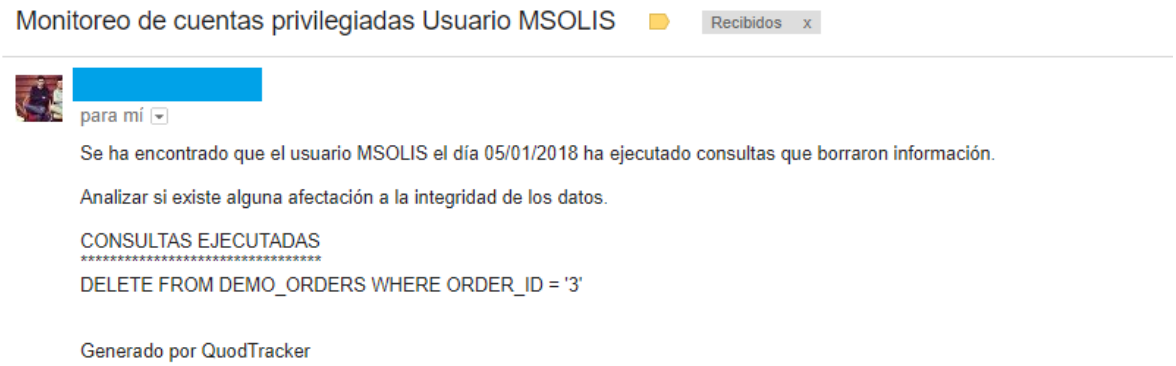


Figura 20, Alerta de consulta SQL para monitorear consultas de los DBA. (Elaboración propia)

9 Conclusiones y recomendaciones

- La aplicación desarrollada permite mantener un monitoreo programado completamente adaptado a las necesidades de la seguridad informática en las bases de datos de una organización, al permitir que la aplicación ejecute las consultas SQL y generando las alertas de comportamientos sospechosos, los cuales pueden representar el rastro de un ataque.
- Los sistemas de gestión de Seguridad Informática tendrían un soporte específico dentro de la base de datos, permitiendo que los especialistas en seguridad de la información se enfoquen en el desarrollo de las estrategias de recuperación y protección de la información teniendo como insumo de valor agregado las alertas generadas por la aplicación, aporte que tendría un desarrollo más lento si los procesos de detección se hicieran de manera manual.
- La eficiencia de la herramienta dependerá del enfoque de las consultas que sean desarrolladas y puestas en el control de generación de alertas, por lo que es muy valioso que la Auditoría Interna busque generar la conciencia de generar y actualizar constantemente las consultas de monitoreo, en este punto se ha recomendado utilizar el ciclo de Deming.
- Los datos generados por bitácoras del propio gestor de base de datos o bien generados por una aplicación, son almacenados y aportan valiosa información para la empresa, pero en la mayoría de las ocasiones no son conocidos ni consultados con regularidad, por lo que una

consulta automática con salidas por medio de correo electrónico aporta revisiones oportunas utilizando dichos datos.

- Esta herramienta aporta eficiencia implícita, porque los correos electrónicos de salida hacen que el departamento de auditoría interna tenga presente la utilidad de uso y de esta manera incentiva para ingresar más consultas.
- Las ideas de este trabajo se basaron en el gestor de base de datos Oracle por su poder y tamaño, procurando así que este software se magnificara en la auditoría macro, pero es importante mencionar que estas ideas y planteamientos pueden ser utilizadas en otros tipos de gestores sin mayores cambios, lo importante del trabajo presentado es generar ideas de auditoría poco exploradas y con gran aporte a la seguridad de la información de cualquier organización.
- La diferencia que podemos mencionar en una organización que cuente con este software y una que no, es que la auditoría interna de Tecnologías de la Información va a contar con revisiones periódicas sin que sean partes de una revisión programada que lleva tiempo y recursos. Esta generación de alertas se hace una primera vez y quedaran implementadas permanentemente, siendo modificables y mejorables con el tiempo y la experiencia generada. Las organizaciones cuentas con esta fuente de datos (Base de Datos) y no son explotadas por la auditoría para la seguridad de la información porque no cuentan con los medios idóneos, este trabajo da apoyo a esta labor.
- Se recomienda una versión avanzada de este software, de acuerdo con las experiencias obtenidas, se crean nuevas tablas de base de datos para almacenar los datos de los hallazgos, los cuales funcionan como parámetros para nuevas consultas. Por ejemplo, se guardan los datos de las listas obtenidas como el caso de los tamaños de los tablespaces, entonces se puede hacer la comparación con las nuevas listas y detectar crecimientos desmedidos.
- Actualmente una versión de este software se encuentra instalado en dos entidades una entidad financiera y una entidad gubernamental. El departamento de auditoría interna de la entidad financiera ha obtenido hallazgos importantes en las transacciones comerciales de la entidad, por ejemplo, en el cumplimiento de la ley de legitimación de capitales que está establecida por el gobierno de Costa Rica. Este no es un riesgo implícito de la seguridad informática, pero si ayuda para el cumplimiento de una ley por medio de los datos almacenados y los medios tecnológicos.

10 Referencias

AENOR. (Noviembre de 2014). *www.aenor.es.* Obtenido de http://www.aenor.es/aenor/normas/iso/buscadoriso.asp?modob=S#.WJjn-FPhDDc

Aguillón, E. (2012). *Universidad Nacional Autonoma de Mexico*. Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/criptografia/criptografia/index.php/1-panorama-general/12-historia-de-la-criptografia

Aguirre, J. (15 de 03 de 2012). *Crypt4you*. Obtenido de http://www.criptored.upm.es/crypt4you/temas/RSA/leccion1/leccion01.html

DeLuz, S. (16 de 11 de 2010). *Criptografía : Algoritmos de cifrado de clave asimétrica*. Obtenido de http://www.redeszone.net/2010/11/16/criptografia-algoritmos-de-cifrado-de-clave-asimetrica/

DeLuz, S. (4 de 11 de 2010). *Criptografía : Algoritmos de cifrado de clave simétrica*. Obtenido de http://www.redeszone.net/2010/11/04/criptografia-algoritmos-de-cifrado-de-clave-simetrica/

Mejia, A. (20 de 02 de 2009). *Historia de Oracle*. Obtenido de http://arbeymejia-historiaoracle.blogspot.com/2009/02/historia-de-oracle.html

Oracle. (2016). *Oracle*. Obtenido de https://www.oracle.com/es/products/database/enterprise-edition/overview/index.html

Segruidad Informatica . (14 de 09 de 2007). *Segruidad Informatica* . Obtenido de https://seguinfo.wordpress.com/2007/09/14/%C2%BFque-es-rsa/