ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría En Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE UN ESQUEMA DE SEGURIDAD PARA CONTROLAR EL ACCESO NO AUTORIZADO AL AMBIENTE DE PRODUCCIÓN EN ENTIDAD FINANCIERA"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

VANESSA ELIZABETH MALDONADO MENDIETA

GUAYAQUIL-ECUADOR

AÑO: 2015

AGRADECIMIENTO

Agradezco a Dios por brindarme su sabiduría y salud para la culminación de este proyecto, a mi familia por incentivarme cada día a salir adelante.

.

Gracias a cada uno de los profesores por compartir sus enseñanzas y así haber aportado para la finalización de esta etapa profesional.

DEDICATORIA

Dedico este trabajo a mis padres, por ser los pilares fundamentales en mi vida, por su apoyo incondicional para cumplir cada una de mis objetivos.

TRIBUNAL DE SUSTENTACIÓN

MGS KARINA ASTUDILLO

PROFESOR DELEGADO

POR LA SUBDECANA DE LA FIEC

ING JUAN CARLOS GARCÍA

PROFESOR DELEGADO

POR LA SUBDECANA DE LA FIEC

RESUMEN

Este proyecto tiene como objetivo implementar un esquema de seguridad para controlar el acceso de funcionarios de Entidad Financiera no autorizados a información confidencial de los clientes en ambiente de producción.

En el capítulo 1 se abordará la problemática en un inadecuado control de acceso a la base de datos en ambiente de producción, así como también sus posibles soluciones.

En el capítulo 2 se expondrá conceptos generales de la herramienta a implementar, beneficios, monitoreo a la Base de la Base de Datos en tiempo real, funcionamiento de políticas, bloqueo de transacciones, alertas y el procedimiento de gestión de eventos presentados en el monitoreo.

En el capítulo 3 se analizará los resultados obtenidos al implementar la herramienta IBM InfoSphere Guardium.

Al finalizar este proyecto se emitirán las conclusiones y recomendaciones.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

DDL	Data Definition Language
DML	Data Manipulation Language
GIM	Guardium Installation Manager
S – GATE	Real-time blocking software
S – TAP	Lightweight software probes that monitor both network and local database protocols

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La mayoría de los datos sensibles en una entidad financiera se encuentran almacenados en sistemas gestores de bases de datos comerciales tales como Oracle, Microsoft SQL Server, DB2, entre otros, y atacar una base de datos es uno de los objetivos favoritos para los delincuentes informáticos.

Por tal motivo las Entidades Financieras necesitan contar con mecanismos que garanticen la disponibilidad de la información y el acceso seguro a información confidencial de sus clientes en ambiente de producción.

El presente proyecto pretende ser una guía para identificar las debilidades existentes en el inadecuado control de acceso a la información confidencial, con el fin de fortalecerlo y de esta manera evitar que funcionarios tengan demasiados privilegios a la Base de Datos que le permita ejecutar transacciones en todo un proceso de la institución sin controles y ni autorizaciones.

Mantener una herramienta de monitoreo para el control de acceso a la Base de datos en tiempo real, es una solución que permite prevenir la fuga de información, asegurar el control de datos y reducir el costo para cumplir con las regulaciones.

El problema que este proyecto resuelve es relevante para cualquier entidad financiera que mantenga herramientas de monitoreo de sus bases de datos, ya que a menudo se confía demasiado en las personas y no permite analizar las amenazas de seguridad que pueden causar.

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

En una entidad Financiera se maneja gran cantidad de información misma que puede estar organizada en varios gestores de Base de Datos como: Oracle, SQL, DB2, etc, existe un porcentaje alto de información confidencial e información sensible que puede ser accedida por múltiples caminos tanto por usuarios internos (administradores de Base de Datos, Desarrolladores de las Aplicaciones) como usuarios externos (proveedores, outsourcing, clientes), por lo que la Entidad debe garantizar que la información esté disponible sólo para las personas autorizadas.

El problema cuando se implementa un control para el acceso a la base de datos en ambiente de producción se da en el proceso inapropiado de segregación de funciones, ya que ningún funcionario debe de tener demasiado acceso a un sistema que le permita ejecutar transacciones en todo un proceso de la institución sin controles y autorizaciones. Permitir este tipo de acceso representa un riesgo muy real para la entidad y manejar este riesgo de manera pragmática y eficaz es más difícil de lo que parece.

1.2 SOLUCIÓN PROPUESTA

Las Entidades Financieras deben garantizar la seguridad y calidad de la información confidencial de sus clientes, por tal motivo deben de implementar medidas y elementos de seguridad para evitar que funcionarios no autorizados ingresen a los repositorios de la información y se generen eventos fraudulentos, que podría causar un daño (material o inmaterial), la pérdida o la modificación errónea, sea causado intencionalmente o simplemente por negligencia humana, de algún dato en una cuenta bancaria, puede resultar en pérdidas económicas u otras consecuencias negativas para la entidad.

Por lo anteriormente expuesto se hace necesario implementar un adecuado control para impedir que funcionarios no autorizados accedan a información confidencial de los clientes en ambiente de producción, a continuación se describen las acciones a realizar:

- Implementar una plataforma de seguridad empresarial para evitar actividades no autorizadas o sospechosas por parte de personas con privilegios de acceso a información confidencial y hackers potenciales.
- Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas.
- Monitoreo continuó en tiempo real basado en políticas, de todas las actividades de tráfico de datos, incluyendo las de usuarios privilegiados.
- Bloquear el acceso a información considerada como confidencial.
- Registrar, Revisar y Gestionar los eventos presentados durante el monitoreo de accesos a la base de datos del ambiente de producción.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 IMPLEMENTACIÓN DEL ESQUEMA DE SEGURIDAD PARA EVITAR ACTIVIDADES NO AUTORIZADAS

2.1.1 IBM INFOSPHERE GUARDIUM

El contenido de las Bases de Datos en una Entidad Financiera es vital y confidencial se almacenan información sensible de los clientes como son: Nombres, Apellidos, Direcciones, Números de Cuenta, Números de Tarjeta, Registros Financieros, etc. El problema que se da en las organizaciones hoy en día son:

- Aumento de ataques, robos internos y externos de datos.
- Aumento del fraude por el robo de datos sensibles.

- Multas y sanciones por no cumplir con los entes reguladores.

La solución de IBM InfoSphere Guardium abarca toda la seguridad de base de datos y ciclo de vida de cumplimiento con una consola web unificada, almacenamiento de información administrativa y sistema de automatización de flujo de trabajo [1]. Como se muestra a continuación.

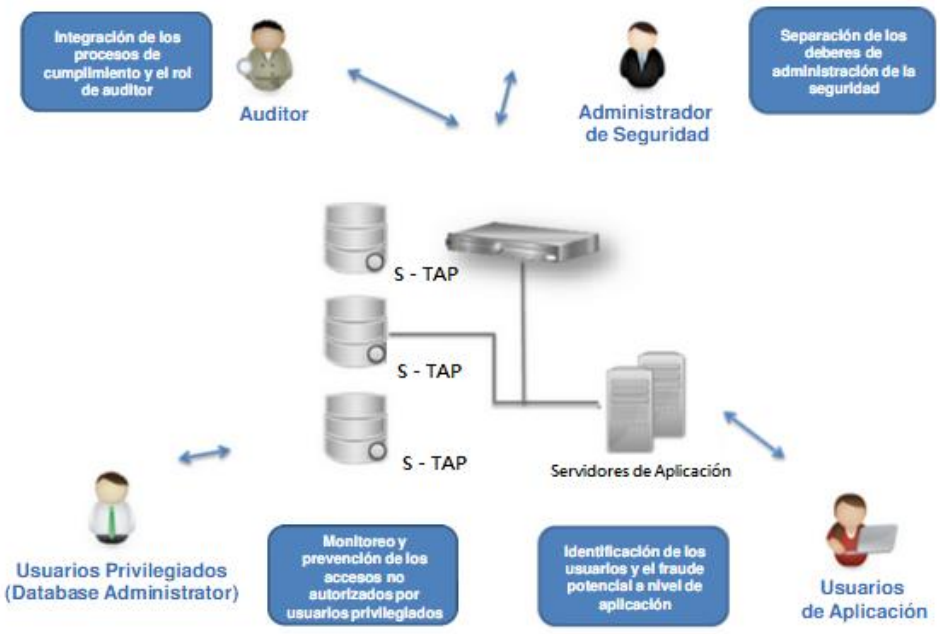

Figura 2.1 Complejidad de Usuarios y Amenazas

Lo que le permite a las organizaciones:

Prevenir peligros internos

- Identificar accesos y cambios no autorizados.
- Prevenir fuga de información.

Prevenir peligros Externos

- Prevenir robo
- Bloqueo de datos y tablas críticas

Monitorización

- Usuarios privilegiados
- Base de datos y tablas críticas

Cumplimiento Regulaciones

- Simplificar y automatizar el proceso de auditoria

Reducción de costos

Análisis de Vulnerabilidades y gestión de incidentes sobre las bases de datos.

2.1.2 BENEFICIOS DE IBM INFOSPHERE GUARDIUM

a) Arquitectura no-invasiva

- Fuera de la Base de Datos

- Impacto mínimo en rendimiento (2-3%)
- Sin cambios al DBMS o aplicativos

b) Solución multi-plataforma.

c) 100% visibilidad incluyendo accesos locales de DBAs.

d) Refuerza toda la segregación de roles y funciones entre los auditores y los administradores de la Base de datos.

e) No depende de los logs nativos del DBMS que pueden ser borrados por atacantes o personal interno.

f) Granular, políticas en tiempo real y auditoría. [2]

- *Identificación*: Quién, que, cuando, dónde, y cómo de cada transacción.
    - *Quién*: usuario de la base de datos, usuario del aplicativo, usuario del SO
    - *Qué*: Base de datos, nombre del campo, objeto sensible.
    - Cuando: Periodo de tiempo, horas laborables, hora no laborables.
    - *Dónde*: IP Cliente, IP Servidor.
    - *Cómo*: Acceso, extrusión de data, excepción de SQL/login.
- Acción: Aplicar reglas
    - Loguear

- Alertar
- Control de acceso

Identificación + Acción = Regla -> Política de seguridad con máximo detalle.[3]

g) Informes automatizados de cumplimiento,

- Trazabilidad y escalado (SOX, PCI, NIST, etc.)[2]

2.1.3 MONITORIZACIÓN DE BASES DE DATOS EN TIEMPO REAL

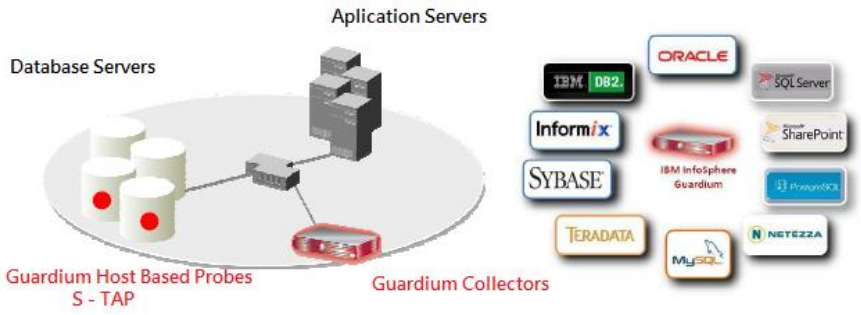

Figura 2.2 Monitorización de Bases de Datos en Tiempo Real

Monitoreo de seguridad se refiere al análisis continuo de las transacciones de bases de datos. InfoSphere Guardium monitorea las transacciones de bases de datos de todos los usuarios utilizando dispositivos de software de monitoreo (S-TAPs) como medidores, pero también se integra con otras soluciones e infraestructuras de seguridad de IBM.

Se coloca un S-TAP en todos los agrupamientos y se envía una copia de todas las transacciones de las bases de datos a InfoSphere Guardium **Collector**.

El Collector es un aparato o dispositivo para registrar, guardar, auditar y analizar las auditorías de las transacciones de las bases de datos en cuanto a las violaciones a la seguridad.

Las acciones generadas por el sistema reflejan el **Motor de Políticas** de InfoSphere Guardium que provee las políticas para el cumplimiento de seguridad que se usan para identificar las violaciones a la seguridad.

Un **Aggregator** de InfoSphere Guardium es el dispositivo que consolida los análisis de colectores múltiples para generar reportes de seguridad a nivel empresarial. De esta forma, las organizaciones obtienen los beneficios de las advertencias preliminares sobre las violaciones a la seguridad. InfoSphere Guardium monitorea meticulosamente las transacciones para detectar el uso no autorizado, entidades no escrupulosas, violaciones a los datos y otros ataques y amenazas a la seguridad [4].

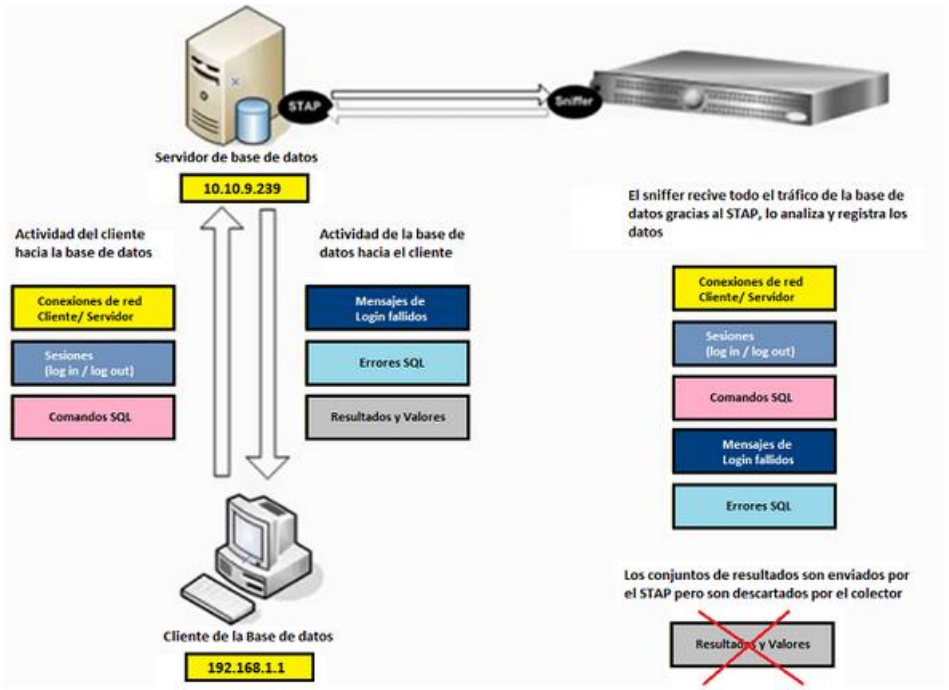

Figura 2.3 Comportamiento por default del Agente S - TAP

Veamos el tráfico entre el cliente de la base de datos y el servidor de la base de datos como un tráfico bidireccional. El cliente realiza un acceso a la base de datos y podemos identificar el término acceso en varias partes del funcionamiento de Guardium, como lo son las reglas de acceso en las políticas, reportes, etc.

Existen 3 peticiones que el cliente realiza:

1. *A nivel de red*: cuando realizamos una conexión hacia la base de datos, ésta incluye la IP del cliente, usuario de base de datos, programa fuente que realiza la conexión.
2. *Sesión (log in/ log out)*: cada vez que el cliente realice una nueva conexión a la base de datos es una nueva sesión
3. *Comandos SQL*: selects, inserts, deletes, etc. Todo lo que el cliente está ejecutando hacia la base de datos.

Después de que el cliente realiza una conexión a la base de datos, ésta le responde y enviará mensajes de vuelta hacia el cliente los cuales son:

1. *Logins fallidos*: el servidor responde que el cliente no puede realizar una conexión cuando hay algún parámetro incorrecto.
2. *Errores SQL*: cuando realizas una consulta a una tabla que no existe, el servidor regresa un mensaje indicando que la tabla no existe, o bien cuando hay un error de sintaxis y se escribe incorrectamente una sentencia.

3. *Resultados y Valores*: cuando se ejecuta por ejemplo una consulta y nos devuelve mil filas, los resultados y valores de esa consulta.

Toda la información viaja desde el S-TAP hacia el colector Guardium el cual, si no existe una política instalada, o bien, se instaló una política "allow all"(política que contiene cero reglas) almacenará la información antes mencionada EXCEPTO los Resultados y Valores, el agente S-TAP los envía al colector pero éste último, simplemente los descarta, para ahorrar espacio en disco duro [5].

2.1.4 FUNCIONAMIENTO DE LAS POLÍTICAS CON IBM INFOSPHERE GUARDIUM

Las políticas nos ayudan a cambiar el comportamiento de que es lo que almacena en el colector de Guardium, las políticas se componen de una serie de reglas y acciones que al ser instaladas, modificarán el comportamiento por default, estas reglas residen en el lado del colector.

Cada vez que se realiza un cambio en alguna política instalada en Guardium (por ejemplo, se modifica un usuario que reside dentro de un grupo) se tiene que reinstalar la política.

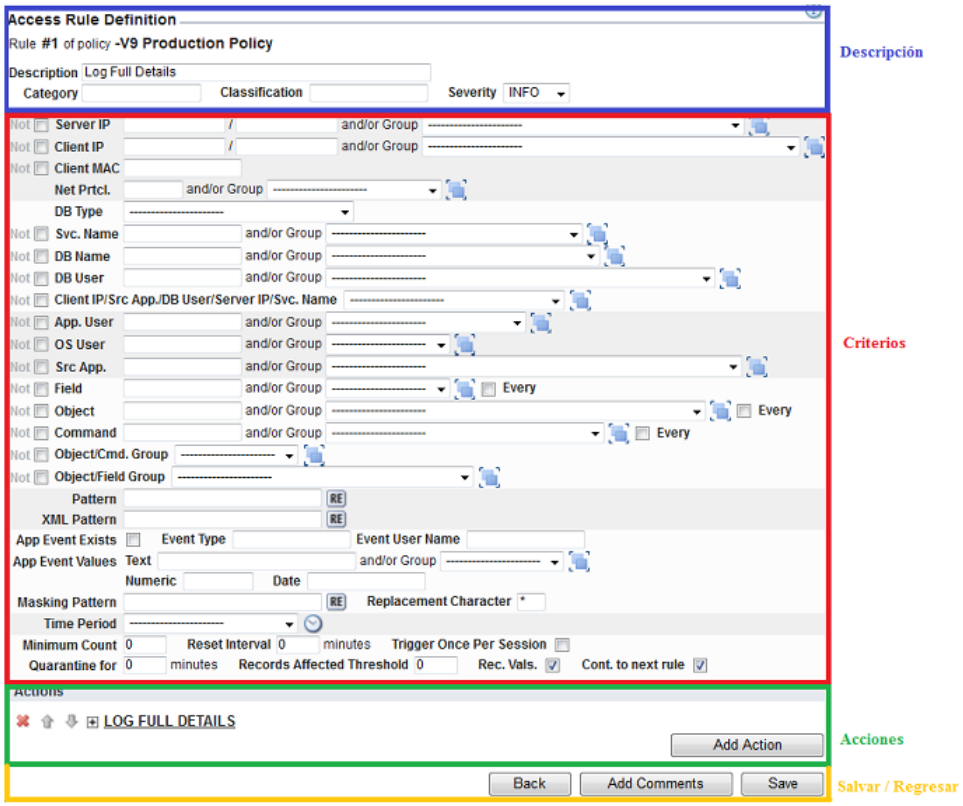

Figura 2.4. Política, composición de una regla de acceso

Una regla de acceso se compone de los siguientes elementos:

- *Descripción*: el nombre y la severidad que se otorgará a la regla.

- *Criterios*: es lo que causa que la regla sea disparada, por ejemplo, un comando que sea ejecutado por un usuario que provenga de una aplicación específica va a disparar una acción; a mano izquierda se especifica un campo de manera individual, mientras que a la derecha podemos utilizar grupos.

La regla se disparará cuando alguien modifique un objeto que puede ser llamado credit, crédito, crediticio, credencial, etc.

- *Acciones*: lo que va a suceder cuando la regla sea disparada.
- *Salvar / Regresar*: guardar cambios de la regla.[5]

2.1.4.1 POLÍTICAS IMPLEMENTADAS EN ENTIDAD FINANCIERA CON INFOSPHERE GUARDIUM

Se han identificado a los siguientes grupos de usuarios que accederán a la base de datos en ambiente de producción

Tipo	Descripción
Usuarios de Aplicaciones	Usuarios dueño de paquetes y objetos
Usuarios propios de la base de datos	Usuarios como sys o system
Usuarios Administradores de la Base de Datos	Usuarios del Área de Tecnología – Producción
Usuarios del Área de Seguridad	Usuarios del Área de Seguridad
Usuarios Desarrolladores	Usuarios del Área de Tecnología – Desarrollo, Desarrolladores con acceso limitado
Usuarios Operadores	Usuarios del Área de Tecnología – Producción Centro de Cómputo función Operadores.
Usuarios Stand By	Usuarios que cumplen la función de revisar novedades presentadas en producción en horarios no laborables, fin de semana y día feriados.
Usuarios Gestión de Cambios – Técnicos	Usuarios que realizan la función de Pases de Versión en el Ambiente de Producción.

Tabla 2.1 Grupos de usuarios que accederán a la base de datos en ambiente de producción

Los usuarios antes descritos accederán a producción desde direcciones IP´s ya definidas, en base a esto se configuró las siguientes reglas:

Acceso - Usuarios de Aplicaciones:

Son aquellos que únicamente deben acceder a la base de datos desde direcciones IP´s de servidores de capa intermedia y son los siguientes:

- De conexión
- Dueños de Paquetes
- Dueño de Objetos

Acciones: Si un usuario de aplicación intenta acceder a la base de datos desde otras direcciones IP´s o se intenta acceder con otros usuarios desde las direcciones IP´s de los servidores de la capa intermedia, se registrará el incidente y se generarán las respectivas alarmas.

Acceso - Usuarios propios de la base de datos

Usuarios propios de la base de datos únicamente deben acceder desde las direcciones IP´s del grupo de Administradores o desde la dirección IP propia del servidor de Base de Datos.

- Usuarios propios de la Base de Datos Oracle: SYS, SYSTEM, DBSNMP, WKSYS.

Direcciones IP´s Administradores	192.168.239.234, 192.168.239.232, 192.168.239.233 , 192.168.239.242, 192.168.241.149, 192.168.239.116
Direcciones IP´s Servidor de la Base de Datos.	192.168.254.1

Tabla 2.2 Usuarios propios de la Base de Datos

Acciones: Si un usuario propio de la Base de datos Oracle, intenta acceder desde otra dirección IP se registrará el incidente y se generarán la respectivas alarmas.

Acceso - Usuarios Administradores de la Base de Datos

Los usuarios Administradores únicamente deben acceder desde sus direcciones IP´s asignadas o desde la dirección IP propia del servidor de Base de Datos.

Usuario Administrador	Direcciones IP´s asignadas
FGALLO	192.168.239.232, 192.168.239.242. 192.168.241.149
SUSINA	192.168.239.233
CFRANCO	192.168.239.116
FBANCHO	192.168.239.234

Tabla 2.3 Usuarios Administradores de la Base de Datos

Acciones: Si un usuario Administrador intenta acceder desde otras direcciones IP. O si desde la dirección IP asignada a un Administrador se intenta acceder con un usuario distinto al asignado (y que no sea usuario propio de la base) se registrará el incidente y se generaran alarmas.

Acceso - Usuarios del Área de Seguridad

Los usuarios del Área de Seguridad únicamente deben acceder desde sus direcciones IP´s asignadas.

Usuarios de Seguridad	Direcciones IP´s asignadas
MALVARE	198.162.231.57
MCASCAN	198.162.231.68
PSANCHE	198.162.231.62

Tabla 2.4 Usuarios del Área de Seguridad

Acciones: Si un usuario del Área de Seguridad intenta acceder desde otras direcciones IP´s, o si desde alguna dirección IP de esta Área intenta acceder con un usuario que no pertenece a dicha Área, se registrará el incidente y se generarán las respectivas alarmas.

Acceso - Usuarios Desarrolladores

Los Usuarios de Desarrolladores únicamente deben acceder desde las direcciones IP´s del grupo de Desarrollo.

- Direcciones IP´s de Desarrollo : Rango de IP´s desde 192.168.213.1 al 192.168.213.254

Acciones: Si un usuario Desarrollador intenta acceder desde otras direcciones IP´s, o si desde alguna dirección IP de este grupo se intenta acceder con un usuario que no pertenece a dicho grupo, se registrará el incidente y se generarán las respectivas alarmas.

Acceso - Usuarios Operadores

Los usuarios Operadores únicamente deben acceder desde las direcciones IP´s del grupo de Operadores.

- Usuarios de Centro de Cómputo (Operadores) : OPER_CP

Direcciones Ip de Usuarios de Centro	192.168.242.122, 192.168.241.152, 192.168.239.133, 192.168.241.72,

de Cómputo (Operadores)	192.168.241.116, 192.168.241.136,

Tabla 2.5 Usuarios de Centro de Cómputo

Acciones: Si un usuario del Centro de Cómputo (Operadores) intenta acceder desde otras direcciones IP´s, o si desde alguna dirección IP de grupo de Operadores se intenta acceder con un usuario que no pertenece a dicho grupo, se registrará el incidente y se generarán las respectivas alarmas.

Acceso - Usuario Stand By

Los usuarios Stand By únicamente deben acceder desde sus direcciones IP´s asignadas a la función de Stand By.

Direcciones Ip´s StandBy :	192.168.213.183, 192.168.213.194, 192.168.213.78, 192.168.213.107, 192.168.213.217, 192.168.213.118	192.168.213.122, 192.168.213.71, 192.168.213.158, 192.168.213.39, 192.168.213.91,

Tabla 2.6 Usuarios Stand By

Acciones: Si un usuario del Grupo de Stand By intenta acceder desde otras direcciones IP´s, o si desde alguna dirección IP de grupo de Stand By se intenta acceder con un usuario que no pertenece a dicho grupo, se registrará el incidente y se generarán las respectivas alarmas.

Acceso - Usuarios Gestión de Cambios - Técnicos

Los usuarios de Gestión de Cambios – Técnicos, únicamente deben acceder desde sus direcciones IP´s asignadas a su función.

- Usuarios Gestión de Cambios – Técnicos: ADMIN_GESTIONCAMBIOS.

Direcciones IP´s ADMIN_GESTIONCAMBIOS:	198.168.239.131, 198.168.239.133, 198.168.239.132

Tabla 2.7 Usuarios Gestión de Cambios

Acciones: Si un usuario del Grupo de Gestión de Cambios - Técnico intenta acceder desde otras direcciones IP´s, o si desde alguna dirección IP de grupo de administradores de Pases se intenta acceder con un usuario que no pertenece a dicho grupo, se registrará el incidente y se generarán las respectivas alarmas.

2.1.5 BLOQUEO DE TRANSACCIONES CON INFOSPHERE GUARDIUM

El proceso de prevención de accesos a la base de datos funciona de la siguiente manera:

1. Un usuario emite una petición SQL.

2. S-GATE, que es un componente de agente de S-TAP de Guardium, intercepta la solicitud y la envía al colector Guardium.
3. El colector Guardium procesa la petición contra las reglas de política configurada e instalada.
4. Si la solicitud contiene la acción no autorizada el aparato Guardium envía un veredicto 'terminar la sesión' al S-GATE.
5. El S-GATE termina la sesión del usuario y no envía el comando a la base de datos [6].

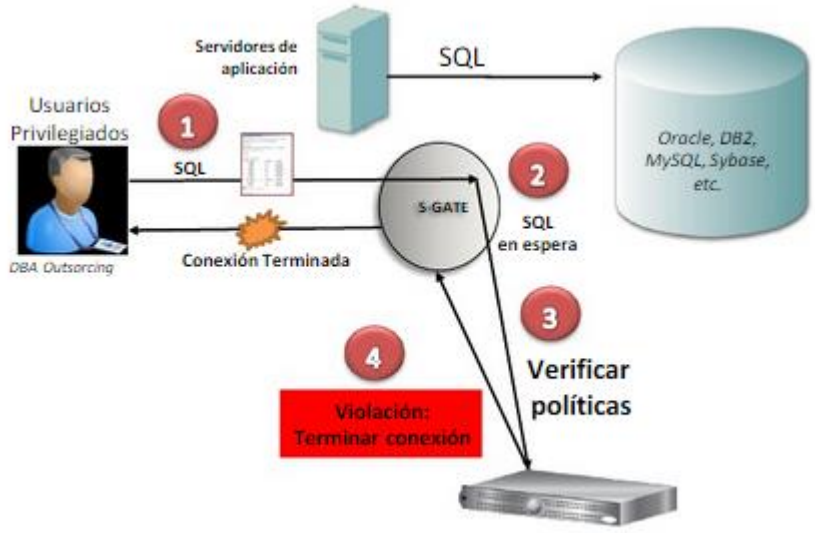

Figura 2.5 Bloqueo de Transacciones

2.1.5.1 BLOQUEO DE TRANSACCIONES DE ACCESO A INFORMACIÓN CONFIDENCIAL EN ENTIDAD FINANCIERA

La siguiente tabla indica las políticas de acceso a la información sensible configuradas para los diferentes grupos de usuarios autorizados.

	Sólo consulta		Sentencias DML		Sentencias DLL	
Tipo de Usuario	**No Sensible**	**Sensible**	**No Sensible**	**Sensible**	**No Sensible**	**Sensible**
Usuarios de Aplicaciones	SI	SI	SI	SI	SI	SI
Usuarios propios de la Base de Datos	SI	NO	SI	NO	SI	NO
Usuarios Administradores de la Base de Datos	SI	NO	SI	NO	SI	NO
Usuarios del Área de Seguridad	SI	NO	SI	NO	SI	NO
Usuarios Desarrolladores	SI	NO	NO	NO	NO	NO
Usuarios Operadores	SI	NO	SI	NO	SI	NO
Usuarios Stand By	SI	SI	SI	SI	NO	NO
Usuarios Gestión de Cambios	SI	NO	SI	SI	NO	NO

Tabla 2.8 Bloqueo de Transacciones

En caso de incumplirse con alguna de estas políticas se registrarán dicho incidente, se generarán las respectivas alarmas y se activarán un bloqueo del acceso. El bloqueo está configurado como de tipo abierto, esto es la base de datos atiende la petición mientras el agente S -TAP de Guardium evalúa el acceso, esto permite que haya el menor impacto en rendimiento para la base de datos.

2.1.6 ALERTAS IMPLEMENTADAS CON INFOSPHERE GUARDIUM EN ENTIDAD FINANCIERA

Se deberán generar alertas y registrar actividades por:

- Accesos desde direcciones IP’s no autorizadas, es decir que no pertenezcan a Servidores de Aplicación, Servidores OAS, Servidores de BD, Estaciones de Administradores de Base de Datos, Estaciones de personal de Gestión de Cambios, Estaciones de personal de Desarrollo, Estaciones de personal de Seguridad y Estaciones de Operadores.

- Accesos de usuarios no autorizados, es decir que no sean Usuarios de aplicación, Usuarios propios de Oracle, Usuarios Administradores de Base de Datos, personal de Gestión de Cambios, usuarios de Desarrollo para atención de requerimientos, personal de Seguridad y Operadores.

- Accesos de usuarios propios de Oracle (SYS, SYSTEM) desde direcciones IP's que no sean estaciones de Administradores de Base de Datos o Servidores de BD.

- Accesos de usuarios Administradores de Base de Datos, desde direcciones IP's que no pertenezcan a las Estaciones de Administradores de Base de Datos.

- Accesos de personal de Gestión de Cambios, desde direcciones IP’s que no pertenezcan a las Estaciones de personal de Gestión de Cambios.

- Accesos de usuarios de Desarrollo para atención de requerimientos, desde direcciones IP’s que no pertenezcan a estaciones de personal de Desarrollo.

- Accesos de personal de Seguridad, desde direcciones IP’s que no pertenezcan a estaciones de personal de Seguridad.

- Accesos de usuarios Operadores, desde direcciones IP’s que no pertenezcan a estaciones de Operadores.

- Accesos de usuarios de Aplicación desde direcciones IP’s que no pertenezcan a servidores de aplicación.

- Accesos de usuarios propios de Oracle y de Administradores de Base de Datos realizando consultas o ejecutando sentencias DML a tablas con información sensible de clientes. (Estas tablas se encuentran definidas en la herramienta).

- Accesos de usuarios de Seguridades y Operadores realizando consultas o ejecutando sentencias DML, o DDL a tablas con información sensible de clientes.

- Accesos de usuarios de Desarrollo para atención de requerimientos ejecutando sentencias DML, o DDL a tablas con información sensible de clientes.

- Accesos de usuarios de Gestión de Cambios realizando consultas o ejecutando sentencias DDL a tablas con información sensible de clientes.

2.1.7 EXCEPCIONES

- Accesos desde servidores de monitoreo, de base de datos con usuario de Oracle.

- Accesos desde estaciones de personal de Gestión de Cambios, con usuarios dueños de paquetería, ejecutando sentencias DML.

- Accesos desde estaciones de Administradores de bases de datos, con usuarios dueños de objetos, ejecutando sentencias DDL.

- Accesos desde estaciones de personal de Seguridad, ejecutando sentencias DML.

- Accesos desde estaciones de personal de Seguridad, realizando consultas o ejecutando sentencias DML a tablas con información sensible de clientes pero autorizadas para Seguridad por la operativa diaria.

2.2 PROCESO DE GESTIÓN DE ENVENTOS PRESENTADOS DURANTE EL MONITOREO DE ACCESO A LA BASE DE DATOS

2.2.1 PROCEDIMIENTO

1. El Oficial de Seguridad de la Información recibe automáticamente vía correo electrónico la alerta, desde la Herramienta de Monitoreo de Acceso a la Base de Datos.

2. El Oficial de Seguridad de la Información analiza el tipo de evento presentado de acuerdo a la prioridad del mismo.

3. En el caso se determine que es un Falso Positivo, el Oficial de Seguridad de la Información procede a archivar documentación auditable en la carpeta del área “Respuesta a Incidentes” por un periodo de doce meses; y registra en “*Bitácora de Gestión de Eventos de Monitoreo de Accesos*”. ***Ver Bitácora de Gestión de Eventos de Monitoreo de Accesos***

4. En el caso se determine que no es un Falso Positivo, el Oficial de Seguridad de la Información solicita vía correo electrónico al Jefe Inmediato del Usuario Comprometido, con Copia al Usuario Comprometido y al Gerente de Área del Usuario Comprometido el justificativo del incumplimiento de la regla.

5. El Jefe Inmediato del Usuario comprometido recibe vía correo electrónico solicitud del justificativo del incumplimiento de la regla, procediendo a enviar vía correo electrónico la justificación en caso existiera.

6. El Oficial de Seguridad de la Información recibe vía correo electrónico la justificación del incumplimiento y analiza la misma.

7. Si la justificación es válida, el Oficial de Seguridad de la Información analiza la necesidad de regularizar el acceso, solicitando al Jefe Inmediato del Usuario comprometido que proceda con la ejecución del procedimiento de Configurar Reglas en Herramienta de Monitoreo de Acceso a la Base de Datos.

8. El Oficial de Seguridad de la Información si determina que es un incumplimiento o no se ha tenido respuesta en el tiempo

establecido en la política, realiza un informe del incumplimiento especificado detalles del mismo como: usuario, regla infringida y fecha, procediendo a enviarlo vía correo electrónico al Gerente de Seguridad de la Información.

9. El Gerente de Seguridad de la Información recibe vía correo electrónico el informe del incumplimiento, revisa el mismo y procede a su envío vía correo electrónico, al Jefe Inmediato del Usuario comprometido y Gerente de área del Usuario Comprometido, para que procedan a establecer las acciones disciplinarias que correspondan de acuerdo al reglamento interno.

10. El Oficial de Seguridad de la Información procede a archivar documentación auditable del incidente en la carpeta del área “respuestas a incidentes”, por un periodo de doce meses y registra en Bitácora de Gestión de Eventos de Monitoreo de Accesos.

2.2.2 POLÍTICAS

1. El tiempo para presentar la justificación de incumplimiento de reglas, de la herramienta de monitoreo de accesos a la base de datos, dependerá de la criticidad de la alerta reportada. Alta 1 día, Media 2 días y Baja 3 días.

2. La base de conocimientos de la herramienta de monitoreo de accesos a la base de datos deberá ser actualizada por el administrador del servicio cada tres meses.

FECHA	HORA	ID DEL EVENTO	USUARIO SO	USUARIO BD	REGLA QUE GENERÓ EVENTO	RESPONSABLE GESTIÓN	DESCRIPCIÓN DE GESTIÓN REALIZADA	FECHA FIN GESTIÓN
14/06/2015	8:43:58	219758584	CFRANCO	FB_PKG	Alerta Usuarios no autorizados	JORRALA	Usuario accedió para realizar tareas administrativas para esquema FB_OBJ	14/06/2015

Figura 2.6 Bitácora de Gestión de eventos de monitoreo de accesos

CAPÍTULO 3

ANÁLISIS DE RESULTADOS

Los resultados obtenidos al implementar la herramienta Infosphere Guardium fueron los siguientes:

VISIBILIDAD

Tener una mejor identificación de los accesos a la base de datos: Quien, Qué, Cuándo, Dónde, y Cómo de cada transacción.

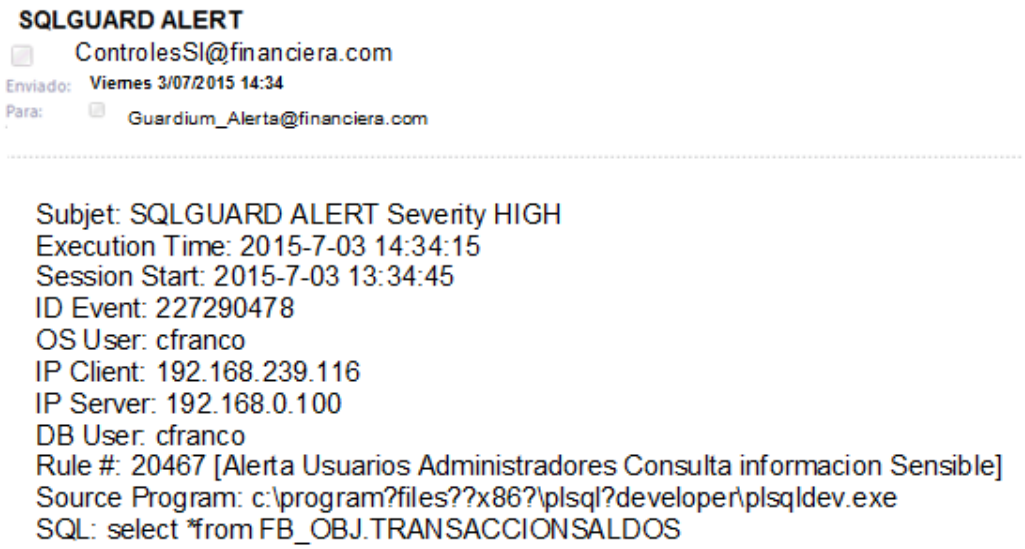

Figura: 3.1 Resultados Visibilidad

DETECCIÓN

Alertar en accesos no autorizados a la Base de Datos en Ambiente de Producción, basado en políticas y controles, mismo que nos ayuda a mitigar el potencial de acceso a datos confidenciales de los clientes.

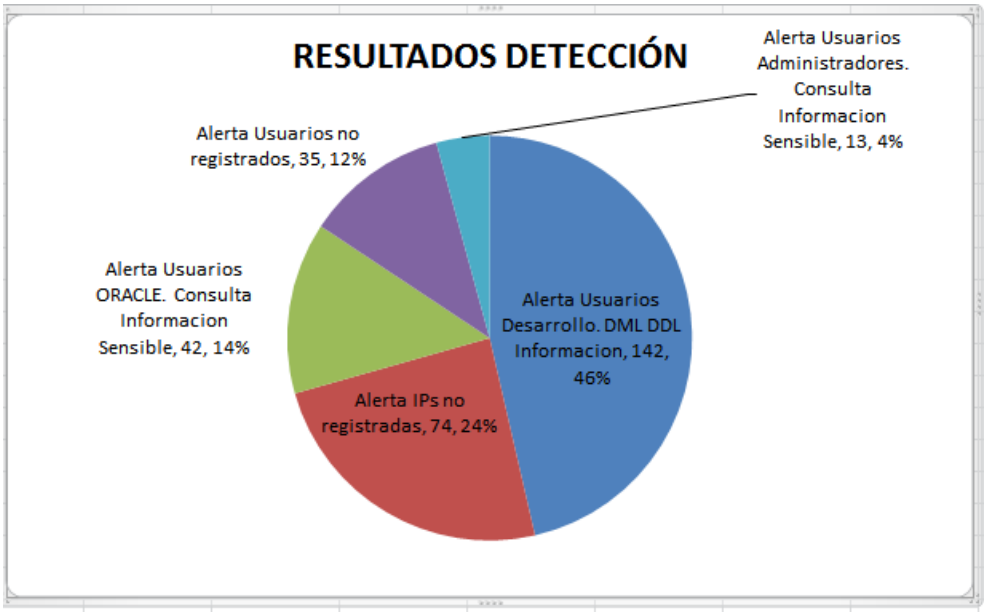

Figura 3.2 Resultados Detección

PREVENCIÓN

Con la detección de accesos no autorizados, nos permite mitigar búsquedas de información sensible de los clientes, modificación/eliminación de tablas críticas y creación de nuevas cuentas de usuarios y modificación de privilegios.

CONCLUSIONES

1. Se logró supervisar a los usuarios finales, sin realizar cambios en las bases de datos ni en las aplicaciones y sin afectar el rendimiento, con el fin de evitar actividades maliciosas que pongan en riesgo información sensible de los clientes.

2. Se identificó accesos a las bases de datos, lo cual permitirá realizar auditorías, informes, análisis forenses, análisis de vulnerabilidades, proteger los datos de operaciones indebidas que pongan en peligro su definición, existencia, integridad independiente de la persona que los acceda.

3. Se detectó accesos no autorizados, lo cual permite alertar ante posibles fraudes, hackeos que afecten la continuidad de la entidad financiera o su imagen.

4. Se logró centralizar controles y automatizarlos para simplificar los procesos, reducir costos de operación y mitigar los riesgos.

RECOMENDACIONES

1. Implementar una política de seguridad con el fin de concienciar a los empleados de la entidad financiera sobre la importancia de la información y servicios críticos que afecten las operaciones cotidianas de la institución.

2. Establecer un procedimiento de control para el ingreso del personal autorizado a los Data Center como medida de prevención ante amenazas a los recursos donde se almacena la información confidencial.

3. Mantenerse siempre informado de las vulnerabilidades, actualizaciones, parches y soluciones con el fin de minimizar los riesgos de ataques que afecten a la imagen y a los activos de la institución

BIBLIOGRAFÍA

[1]. IBM InfoSphere Guardium Cómo administrar toda la seguridad de base de datos y el ciclo de vida del cumplimiento, fecha de consulta julio 2015, http://www.ais.com.mx/alianzas/guardium/1_IBM_InfoSphere_Guardium.pdf

[2]. InfoSphere Guardium de IBM: Monitorización, Protección y Auditoría de Bases de Datos, https://www.youtube.com/watch?v=kKXS3McQ-VA, fecha de consulta julio 2015.

[3]. Seguridad y Auditoría para las bases de datos, http://www.telcoware.net/guardium-seguridad-y-auditoria-para-bases-de-datos/#.VbmkWvN_Oko, fecha de consulta julio 2015.

[4]. Cree un ambiente Hadoop seguro con IBM InfoSphere Guardium, http://www.ibm.com/developerworks/ssa/library/sesecurehadoopenvironment/ fecha de consulta julio 2015

[5]. IBM Infosphere Guardium Funcionamiento de las políticas, http://www.ibm.com/developerworks/ssa/data/library/IBMInfosphereGuardium_Funcionamiento_de_las_politicas/index.html, fecha de consulta julio 2015.

[6]. Conceptos y Mejores Prácticas para el control de accesos del agente STAP de IBM Infosphere Guardium, http://www.ibm.com/developerworks/ssa/security/library/Conceptos_y_Mejores_Pr%C3%A1cticas_para_el_control_de_accesos_del_agente_STAP_de_IBM_Infosphere_Guardium/index.html, fecha de consultad julio 2015.

APÉNDICE

INSTALACIÓN INFOSPHERE GUARDIUM

Requisitos previos para la instalación del Agente GIM (Guardium Installation Manager)

1. Mantener instalado en la base de datos el PERL V5.8.8
2. Mantener instalado JAVA 1.5.0.14

Acciones A Realizar Para Instalación Del Agente Gim en base de datos

1. Loguearse con los privilegios de usuario root.
2. Copiar archivo del instalador del módulo GIM en un directorio de la base de datos:
    - guard-bundle-GIM-9.0.0_r43212_v90_1-hpux-B.11.31-hpux-pa9000.gim.sh
3. Dar permisos de ejecución para el archivo antes descrito.
4. Crear un directorio en el servidor de base de datos donde se instalará el módulo GIM de GUARDIUM.

5. Ejecutar el siguiente script y remplazar las expresiones que se encuentren entre los símbolos “<>” en color rojo por lo solicitado en cada parte.

    - ./guard-bundle-GIM-9.0.0_r43212_v90_1-hpux-B.11.31-hpux-pa9000.gim.sh -- --dir **/<directorio de instalación del módulo GIM>** --sqlguardip 10.1.218.91 --tapip 10.1.218.126

6. Saldrá una pantalla donde se mostrara el acuerdo de licencia y después de aceptarlo nos indicará que el modulo ha sido instalado correctamente.

Acciones a realizar para la instalación del Módulo S –Tap en Base de Datos

La instalación de este módulo se la hará desde la interfaz web y luego de la instalación del agente GIM en el servidor de Base de Datos.

La instalación del STAP genera los pulsos hacia el servidor colector de Guardium.

Contingencia de la instalación del agente

En caso de reportarse alguna afectación se sugiere realizar los siguientes pasos para la inactivación del módulo GIM:

1. Loguearse con los privilegios de usuario root.
2. Abrir el archivo inittab y buscar las líneas que contengan “gim” y “gsrvr”.
3. Comentar las dos líneas antes encontradas y ejecutar como root el comando “init q”.