CHILQUINTA servicios	**CHILQUINTA SERVICIOS** **GERENCIA DE TECNOLOGÍA**		
Identificación: CS GT SGTI PO 22	Fecha Creación: 10-12-2024	Fecha Modificación: N/A	Versión: 0

PROCEDIMIENTO OPERATIVO

CONFIGURACIÓN Y REVISIÓN PERIÓDICA DE PARÁMETROS DE AUDITORÍA EN LA BASE DE DATOS DE OPEN SMARTFLEX (OSF)

CONFIGURATION AND PERIODIC REVIEW OF AUDIT PARAMETERS IN THE OPEN SMARTFLEX DATABASE (OSF)

Revisado por: Alfredo Martinez Fecha: 10-12-2024	Aprobado por: Wei Zhonghua Fecha: 10-12-2024

1. OBJETIVO

El objetivo de este procedimiento es definir y establecer una metodología para la configuración, monitoreo, y revisión periódica de los parámetros de auditoría en la base de datos Oracle del sistema Open SmartFlex (OSF). Esto busca reforzar la seguridad del sistema y garantizar la trazabilidad de las actividades realizadas por los usuarios con privilegios elevados, como SYS y SYSDBA, minimizando el riesgo de accesos no autorizados y posibles impactos en la información crítica de la Entidad.

2. ALCANCE

Este procedimiento aplica a todos los administradores de bases de datos (DBA) responsables de la configuración y monitoreo de la base de datos Oracle del sistema OSF.

3. DEFINICIONES Y ABREVIACIONES

DBA: Administrador de Base de Datos.

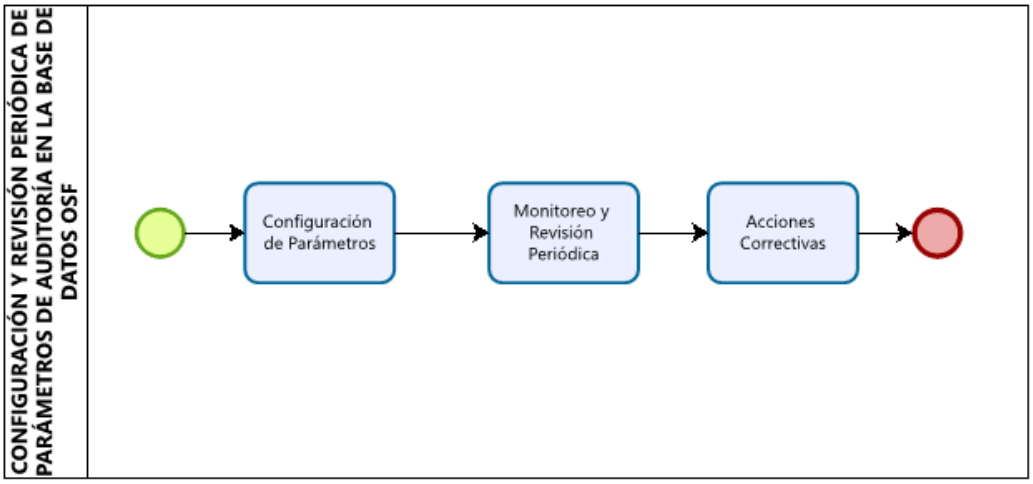
SIEM: Sistema de Gestión de Información y Eventos de Seguridad.

CSOC: Centro de Operaciones de Ciberseguridad.

4. RESPONSABILIDAD Y AUTORIDAD

CARGO	DESCRIPCIÓN (Ejecución de labores/Revisiones y/o aprobaciones)
Administrador de la Base de Datos (DBA):	Responsable de la configuración inicial de los parámetros de auditoría, así como del monitoreo y revisión periódica.
Jefe de Sistema e Infraestructura:	Responsable de la supervisión de la implementación del procedimiento y la evaluación de los informes de auditoría.
Ingeniero de Ciberseguridad:	Responsable de la configuración, monitoreo y respuesta a alertas en el Sistema de Gestión de Información y Eventos de Seguridad (SIEM).

5. DIAGRAMA DE FLUJO



6. CONTENIDO

6.1. Configuración de Parámetros de Auditoría

6.1.1. Parámetro: `audit_sys_operations`

- Valor Recomendado: TRUE
- Descripción: Habilita la auditoría de todas las operaciones realizadas por los usuarios SYS, SYSDBA y SYSOPER, que están exentos de la auditoría estándar.
- Acción: Configurar este parámetro a TRUE para asegurar la auditoría completa de las actividades de los usuarios con privilegios elevados.

6.1.2. Parámetro: `audit_syslog_level`

- Valor Recomendado: LOCAL0.WARNING
- Descripción: Permite la escritura del registro de auditoría en el Syslog del sistema operativo para su retención y reenvío a un sistema de gestión de registros.
- Acción: Configurar este parámetro según los valores recomendados para facilitar la retención y análisis de registros en sistemas centralizados de gestión de logs.

6.2. Monitoreo y Revisión

6.2.1. Integración con SIEM

- Envío de Logs al SIEM: Los logs generados por las auditorías y otros eventos de seguridad relevantes son enviados automáticamente al SIEM de la empresa para su análisis y monitoreo continuo.

- Configuración de Reglas de Alerta en el SIEM: Se establecen reglas de alerta específicas en el SIEM para identificar y responder a posibles incidentes de seguridad con base en los datos de auditoría.
- Reporte de Anomalías: El servicio de CSOC reporta las anomalías tan pronto sean identificadas con base en las reglas definidas.

6.2.2. Actividades de Monitoreo

- Validación de las Anomalías: El ingeniero de ciberseguridad debe analizar los reportes de anomalías del CSOC y solicitar antecedentes al DBA y/o Jefe de Sistemas e Infraestructura hasta que la anomalía sea entendida.

6.2.3. Acciones Correctivas

- Reconfiguración Inmediata: Se deben restablecer los parámetros de auditoría a los valores recomendados de forma inmediata.
- Investigación de Incidentes: Se lleva a cabo una investigación para determinar la causa de los cambios no autorizados o las anomalías y se implementarán medidas para prevenir su recurrencia.

6.3. Reglas de Alerta en el SIEM

Las siguientes reglas de alerta se configuran en el SIEM para detectar actividades inusuales o potencialmente maliciosas en la base de datos Oracle:

6.3.1. Acceso No Autorizado a Usuarios SYS o SYSDBA

- Descripción: Generar una alerta cuando un usuario no autorizado intente acceder o ejecute comandos bajo los privilegios SYS o SYSDBA.
- Condición: Más de 3 intentos de inicio de sesión fallidos o cambios de privilegios en usuarios que no pertenecen al grupo de SYSDBA.
- Nivel de Alerta: Crítico

6.3.2. Cambios en la Configuración de Parámetros de Auditoría

- Descripción: Generar una alerta si se detectan cambios en los parámetros `audit_sys_operations` o `audit_syslog_level`.
- Condición: Cualquier modificación de los valores configurados para estos parámetros.
- Nivel de Alerta: Alto

6.4. Comentarios y/o Consultas

Consultas o inquietudes, respecto del presente procedimiento pueden ser tratadas con su jefatura directa o con los siguientes responsables:

Contacto
1. Administrador de Base de Datos
2. Ingeniero de Ciberseguridad
3. Jefe de Sistemas e Infraestructura

7. NORMATIVA VIGENTE

No Aplica.

8. REFERENCIAS

No Aplica.

9. ASUNTOS ÉTICOS

Consultas o inquietudes relacionadas con temas éticos pueden ser realizadas al encargado de cumplimiento (Gerente Legal) al fono: 322452289.

10. HISTORIAL DE CAMBIOS

Nº Versión	Fecha Vigencia	Comentario	Elaborado por	Revisado por	Aprobado por
0	***10-12-2024***	Creación del documento	Alfredo Martinez	Alfredo Martinez	Wei Zhonghua

11. ANEXOS Y REGISTROS

Registros: Los registros digitales se almacenarán según se indique en la planilla de gestión de configuración del área de Sistemas e Infraestructura.

CHILQUINTA servicios	**CHILQUINTA SERVICES** **TECHNOLOGY MANAGEMENT**

Identification:	**Creation Date:**	**Date Modified:**	**Version:**
CS GT SGTI PO 22	10-12-2024	N/A	0

OPERATIONAL PROCEDURE

CONFIGURATION AND PERIODIC REVIEW OF AUDIT PARAMETERS IN THE OPEN SMARTFLEX DATABASE (OSF)

CONFIGURACIÓN Y REVISIÓN PERIÓDICA DE PARÁMETROS DE AUDITORÍA EN LA BASE DE DATOS DE OPEN SMARTFLEX (OSF)

Reviewed by:	Approved by:
Alfredo Martinez Date: 10-12-2024	Wei Zhonghua Date: 10-12-2024

1. OBJECTIVE

The objective of this procedure is to define and establish a methodology for the configuration, monitoring, and periodic review of audit parameters in the Oracle database of the Open SmartFlex system (OSF). This seeks to strengthen system security and ensure the traceability of activities performed by users with high privileges, such as SYS and SYSDBA, minimizing the risk of unauthorized access and possible impacts on the critical information of the Entity.

2. SCOPE

This procedure applies to all database administrators (DBAs) responsible for configuring and monitoring the Oracle database in the OSF system.

3. DEFINITIONS AND ABBREVIATIONS

DBA: Database Administrator.

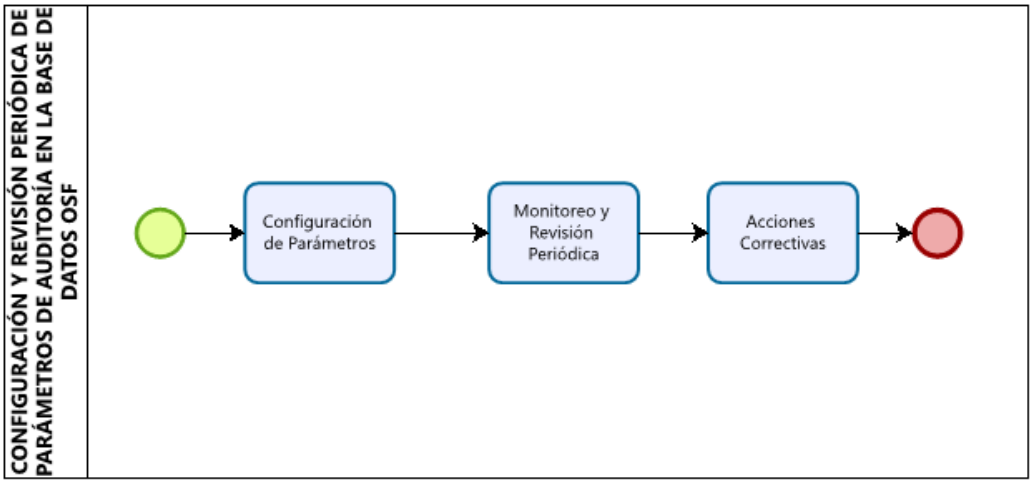
SIEM: Information Management System and Security Events.

CSOC: Cybersecurity Operations Center.

4. RESPONSIBILITY AND AUTHORITY

POSITION	DESCRIPTION (Execution of tasks/Reviews and/or approvals)
Database Administrator (DBA):	Responsible for the initial configuration of audit parameters, as well as monitoring and periodic review.
Head of System and Infrastructure:	Responsible for overseeing the implementation of the procedure and the evaluation of audit reports.
Cybersecurity Engineer:	Responsible for the configuration, monitoring and response to alerts in the Information Management System and Security Events (SIEM).

5. FLOWCHART



6. CONTENT

6.1. Configuring Audit Parameters

6.1.1. Parameter: `audit_sys_operations`

- Recommended Value: TRUE
- Description: Enables auditing of all operations performed by SYS, SYSDBA, and SYSOPER users, which are exempt from standard auditing.
- Action: Set this parameter to TRUE to ensure that activities of users with elevated privileges are fully audited.

6.1.2. Parameter: `audit_syslog_level`

- Recommended Value: LOCAL0.WARNING
- Description: Allows the audit log to be written to the operating system syslog for retention and forwarding to a records management system.
- Action: Configure this parameter to the recommended values to facilitate retention and analysis of logs in centralized log management systems.

6.2. Monitoring and Review

6.2.1. Integration with SIEM

- Logs sent to SIEM: Logs generated by audits and other relevant security events are automatically sent to the company's SIEM for continuous analysis and monitoring.
- Configuring Alert Rules in SIEM: Specific alert rules are established in SIEM to identify and respond to potential security incidents based on audit data.
- Anomaly Reporting: The CSOC service reports the anomalies as soon as they are identified based on the defined rules.

6.2.2. Monitoring Activities

- Validation of Anomalies: The cybersecurity engineer must analyze the CSOC anomaly reports and request background information from the DBA and/or Head of Systems and Infrastructure until the anomaly is understood.

6.2.3. Corrective Actions

- Immediate Reconfiguration: Audit parameters must be restored to recommended values immediately.
- Incident Investigation: An investigation is conducted to determine the cause of the unauthorized changes or anomalies and measures will be implemented to prevent their recurrence.

6.3. Alert Rules in SIEM

The following alert rules are configured in the SIEM to detect unusual or potentially malicious activities in the Oracle database:

6.3.1. Unauthorized Access to SYS or SYSDBA Users

- Description: Generate an alert when an unauthorized user attempts to access or execute commands under SYS or SYSDBA privileges.
- Condition: More than 3 failed login attempts or privilege changes on users that do not belong to the SYSDBA group.
- Alert Level: Critical

6.3.2. Changes to Audit Parameter Settings

- Description: Generate an alert if changes are detected in the 'audit_sys_operations' or 'audit_syslog_level' parameters.
- Condition: Any modification of the values configured for these parameters.
- Alert Level: High

6.4. Comments and/or Inquiries

Questions or concerns regarding this procedure can be addressed with your direct leadership or with the following responsible:

Contact
1. Database Administrator
2. Cybersecurity Engineer
3. Head of Systems and Infrastructure

7. CURRENT LEGISLATION

Does Not Apply.

8. REFERENCES

Does Not Apply.

9. ETHICAL ISSUES

Inquiries or concerns related to ethical issues can be made to the compliance officer (Legal Manager) at the phone number: 322452289.

10. CHANGE HISTORY

Version No	Effective Date	Comment	Prepared by	Reviewed by	Approved by
0	***10-12-2024***	Creating the document	Alfredo Martinez	Alfredo Martinez	Wei Zhonghua

11. ANNEXES AND RECORDS

Records: The digital records will be stored as indicated in the configuration management form of the Systems and Infrastructure area.