ESTANDAR DE SEGURIDAD – DOCUMENTO LINEA BASE ORACLE

CONTROL DE VERSIONES

Elaborado por:	Alvaro De las Salas Rubio	**No. de Versión:**	1
Revisado por:		**Fecha de revisión:**	
Aprobado por:		**Fecha de aprobación:**	

Historia de Modificaciones

No. de Versión	Fecha de Versión	Autor	Revisado por	Aprobado por	Descripción
1.0	Febrero 27, 2023	Alvaro De las Salas Rubio			

DESCRIPCIÓN GENERAL

1.Introducción

Este documento es una guía para la configuración de seguridad, es inherente que el consultor responsable de implementar los cambios sea responsable de validarlos y tomar medidas correctivas.

2.Objetivo

La idea fundamental del documento es establecer controles de seguridad que serán aplicados en los activos de las diferentes compañías que contraten los servicios de SETI, el cual adopta estos controles de seguridad para proteger la información para el cumplimiento de las normas y alcanzar los objetivos del negocio.

3.Motor al que aplica

Estos controles de seguridad serán aplicados a los activos que se muestran en la siguiente tabla.

Aplicabilidad Hardening		
Activo	**Modelo**	**Versión**
Base de datos	Oracle	9i, 10g, 11g, 12c y 19c

4.LINEA BASE DE SEGURIDAD

4.1. Instalación y Parches

ITEM	Vulnerabilidad	Descripción	Remediación	Impacto
4.1.1	Actualización de Oracle	La versión de instalación y los parches de Oracle deben ser los más recientes que sean compatibles con las necesidades operativas de la organización.	Para evaluar esta recomendación, utilice el siguiente comando de ejemplo según corresponda a su entorno. Unix/Linux: opatch lsinventory | grep -e "^.*\s*.*$" Windows: opatch lsinventory | find "" Descargue y aplique los últimos parches críticos trimestrales	Alto
4.1.2	Asegurar que todas las contraseñas predeterminadas sean cambiadas	Las contraseñas predeterminadas deben considerarse "bien conocidas" por los atacantes. En consecuencia, si se mantienen las contraseñas predeterminadas, cualquier atacante con acceso a la base de datos puede autenticarse como usuario con esa contraseña predeterminada.	Para remediar esta configuración, puede ejecutar cualquier de la siguiente instrucción SQL. • Emita manualmente la siguiente instrucción SQL para cada NOMBRE DE USUARIO devuelto en el procedimiento de auditoría: PASSWORD <username> • Ejecute el siguiente script SQL para asignar una contraseña generada aleatoriamente a cada cuenta usando una contraseña predeterminada: begin for r_user in (select username from dba_users_with_defpwd	Alto

			where username not like '%XS$NULL%') loop DBMS_OUTPUT.PUT_LINE('Password for user '||r_user.username||' will be changed.'); execute immediate 'alter user "'||r_user.username||'" identified by "'|| DBMS_RANDOM.string('a',16)||'"account lock password expire'; end loop; end;	

4.2. Configuración Oracle

ITEM	Vulnerabilidad	Descripción	Remediación	Impacto
4.2.1	Configuración remota del listener	El ajuste del SECURE_CONTROL_<listener> determina el tipo de conexión de control el servidor de Oracle requiere para la configuración remota del listener	Para auditar esta recomendación, siga los siguientes pasos: Abrir el archivo: $ORACLE_HOME/network/admin/listener.ora file (o en Windows %ORACLE_HOME%\network\admin\listener.ora) Asegúrese de que cada listener se defina como una directiva asociada SECURE_CONTROL_<listener_name>. Por Ejemplo: LISTENER1 = (DESCRIPTION= (ADDRESS=(PROTOCOL=TCP) (HOST=sales-server)(PORT=1521)) (ADDRESS=(PROTOCOL=IPC) (KEY=REGISTER))	Alto

			(ADDRESS=(PROTOCOL=TCPS)(HOST=sales-server)(PORT=1522))) **SECURE_CONTROL_LISTENER1=TCPS**	
4.2.2	Asegurar que 'extproc' no esté presente en 'listener.ora'	extproc debe eliminarse de listener.ora para mitigar el riesgo de que la instancia de Oracle pueda invocar las librerías del sistema operativo.	Para auditar esta recomendación, ejecute los siguientes comandos de shell según corresponda para su entorno Linux/Windows. Linux: grep -i extproc $ORACLE_HOME/network/admin/listener.ora Windows: find /I "extproc" %ORACLE_HOME%\network\admin\listener.ora Asegúrese de que extproc no exista. Elimine extproc del archivo listener.ora.	Alto
4.2.3	Asegurar 'ADMIN_RESTRICTIONS_<listener_name>'	La configuración admin_restrictions_<listener_name> en el archivo listener.ora puede requerir que se rechace cualquier intento de alteración en tiempo real de los parámetros en el listener a través del archivo de comando set, a menos que el archivo listener.ora se modifique manualmente y luego lo reinicie un usuario privilegiado.	Para auditar esta recomendación, ejecute los siguientes comandos de shell según corresponda para su entorno Linux/Windows. Linux: grep -i admin_restrictions $ORACLE_HOME/network/admin/listener.ora Windows: find /I "admin_restrictions" %ORACLE_HOME%|\network\admin\listener.ora	Alto

			Asegúrese de que admin_restrictions_<listener_name> esté ON para todos los listeners.	
4.2.4	Asegurar TNS listener	La configuración SECURE_REGISTER_<listener_name> especifica los protocolos utilizados para conectarse al agente de TNS listener. Cada configuración debe tener un valor de TCPS o IPC según las necesidades de su protocolo.	Para auditar esta recomendación, ejecute los siguientes comandos de shell según corresponda para su entorno Linux/Windows. Linux: grep -i SECURE_REGISTER $ORACLE_HOME/network/admin/listener.ora Windows: find /I "SECURE_REGISTER" %ORACLE_HOME%\network\admin\listener.ora Asegúrese de que SECURE_REGISTER_<listener_name> esté configurado en TCPS o IPC. Use un editor de texto vi para configurar SECURE_REGISTER_<listener_name>=TCPS o SECURE_REGISTER_<listener_name>=IPC para cada listener encontrado en $ORACLE_HOME/network/admin/listener.ora.	Alto
4.2.5	Asegurar operaciones de usuario SYSDBA	La configuración AUDIT_SYS_OPERATIONS proporciona la auditoría de todas las actividades de los usuarios realizadas en las cuentas SYSOPER y SYSDBA.	La configuración debe establecerse en TRUE. Para evaluar esta recomendación, ejecute la siguiente instrucción SQL:	Medio

			SELECT UPPER(VALUE) FROM V$SYSTEM_PARAMETER WHERE UPPER(NAME) = 'AUDIT_SYS_OPERATIONS'; Para remediar esta configuración, ejecute la siguiente instrucción SQL y reinicie la instancia. ALTER SYSTEM SET AUDIT_SYS_OPERATIONS = TRUE SCOPE=SPFILE;	
4.2.6	Asegurar AUDIT_TRAIL	La configuración de audit_trail determina si las funciones básicas de auditoría de Oracle están habilitadas o no. Se puede configurar en "Sistema operativo" (OS); BD,EXTEND; o XML, EXTENDID.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL: SELECT UPPER(VALUE) FROM V$SYSTEM_PARAMETER WHERE UPPER(NAME)='AUDIT_TRAIL'; ALTER SYSTEM SET AUDIT_TRAIL = DB, EXTENDED SCOPE = SPFILE; ALTER SYSTEM SET AUDIT_TRAIL = OS SCOPE = SPFILE; ALTER SYSTEM SET AUDIT_TRAIL = XML SCOPE = SPFILE; Asegure que el valor es configurado a OS o DB,EXTEND o XML,EXTEND	Medio
4.2.7	Asegurar GLOBAL_NAME	La configuración global_names requiere que el nombre de un enlace de base de datos coincida con el de la base de datos remota a la que se conectará. Esta configuración debe tener un valor TRUE.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL: SELECT UPPER(VALUE) FROM V$SYSTEM_PARAMETER WHERE UPPER(NAME)='GLOBAL_NAMES';	Alto

			Para remediar esta configuración, ejecuta la siguiente instrucción SQL: ALTER SYSTEM SET GLOBAL_NAMES = TRUE SCOPE = SPFILE;	
4.2.8	Asegurar LOCAL_LISTENER	LOCAL_LISTENER especifica un nombre de red que se resuelve en una dirección o lista de direcciones del listener locales de Oracle Net	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL: SELECT UPPER(VALUE) FROM V$SYSTEM_PARAMETER WHERE UPPER(NAME)='LOCAL_LISTENER'; Garantizar que el valor se establece en (DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=REGISTER))) Para remediar esta configuración ejecute la siguiente instrucción SQL: ALTER SYSTEM SET LOCAL_LISTENER='[DESCRIPTION]' SCOPE=BOTH; Cambiar [DESCRIPTION] con la descripción apropiada en el archivo listener.ora, donde la descripción establece el parámetro de protocolo con el IPC. ALTER SYSTEM SET LOCAL_LISTENER='(DESCRIPTION = (ADDRESS=(PROTOCOL = IPC) (KEY=REGISTER)))' SCOPE=BOTH;	Medio

4.2.9	Asegurar '07_DICTIONARY_ACCESSIBILITY'	Parámetro de inicialización de la base de datos que controla el acceso a los objetos en el esquema SYS. Originalmente estaba destinado a ayudar con las migraciones de Oracle7 a versiones más nuevas donde el acceso a los objetos del diccionario de datos está limitado de manera predeterminada.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL: SELECT UPPER(VALUE) FROM V$SYSTEM_PARAMETER WHERE UPPER(NAME)= '07_DICTIONARY_ACCESSIBILITY'; Para remediar esta configuración, ejecuta la siguiente instrucción SQL: ALTER SYSTEM SET 07_DICTIONARY_ACCESSIBILITY=FALSE SCOPE=SPFILE;	Medio
4.2.10	Asegurar '07_DICTIONARY_ACCESSIBILITY'	Parámetro de inicialización de la base de datos que controla el acceso a los objetos en el esquema SYS. Originalmente estaba destinado a ayudar con las migraciones de Oracle7 a versiones más nuevas donde el acceso a los objetos del diccionario de datos está limitado de manera predeterminada.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL: SELECT UPPER(VALUE) FROM V$SYSTEM_PARAMETER WHERE UPPER(NAME)= '07_DICTIONARY_ACCESSIBILITY'; Para remediar esta configuración, ejecuta la siguiente instrucción SQL: ALTER SYSTEM SET 07_DICTIONARY_ACCESSIBILITY=FALSE SCOPE=SPFILE;	Medio
4.2.11	Asegurar 'OS_ROLES'	La configuración os_roles permite que los grupos creados externamente se apliquen a la gestión de la base de datos.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL.	Alto

			SELECT UPPER(VALUE) FROM V$SYSTEM_PARAMETER WHERE UPPER(NAME)='OS_ROLES'; Asegúrese de que VALUE esté establecido en FALSE Para remediar esta configuración, ejecute la siguiente instrucción SQL. ALTER SYSTEM SET OS_ROLES = FALSE SCOPE = SPFILE;	
4.2.12	Asegurar 'REMOTE_LOGIN_PASSWORDFILE'	La configuración de remote_login_passwordfile especifica si Oracle verifica o no un archivo de contraseña durante el inicio de sesión y cuántas bases de datos pueden usar el archivo de contraseña.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL. SELECT UPPER(VALUE) FROM V$SYSTEM_PARAMETER WHERE UPPER(NAME)='REMOTE_LOGIN_PASSWORDFILE'; Asegúrese de que VALUE esté establecido en NONE Para remediar esta configuración, ejecute la siguiente instrucción SQL. ALTER SYSTEM SET REMOTE_LOGIN_PASSWORDFILE = 'NONE' SCOPE = SPFILE;	Alto
4.2.13	Asegurar 'REMOTE_OS_AUTHENT'	La configuración remote_os_authent determina si se permiten o no los 'roles' del sistema operativo con los privilegios de asistente	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL. SELECT UPPER(VALUE) FROM V$SYSTEM_PARAMETER WHERE	Alto

		para las conexiones de clientes remotos.	UPPER(NAME)='REMOTE_OS_AUTHENT'; Asegúrese de que VALUE este establecido en FALSE. Para remediar esta configuración, ejecute la siguiente instrucción SQL. ALTER SYSTEM SET REMOTE_OS_AUTHENT = FALSE SCOPE = SPFILE;	
4.2.14	Asegurar 'REMOTE_OS_ROLES'	La configuración remote_os_roles permite que los roles de SO de los usuarios remotos se apliquen a la administración de la base de datos.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL. SELECT UPPER(VALUE) FROM V$SYSTEM_PARAMETER WHERE UPPER(NAME)='REMOTE_OS_ROLES'; Asegúrese de que VALUE este establecido en FALSE. Para remediar esta configuración, ejecute la siguiente instrucción SQL. ALTER SYSTEM SET REMOTE_OS_ROLES = FALSE SCOPE = SPFILE;	Alto
4.2.15	Asegurar 'SEC_CASE_SENSITIVE_LOGON'	La información SEC_CASE_SENSITIVE_LOGON determina si se requiere distinguir entre mayúsculas y minúsculas para las contraseñas durante el inicio de sesión.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL. SELECT UPPER(VALUE) FROM V$SYSTEM_PARAMETER WHERE UPPER(NAME)='SEC_CASE_SENSITIVE_LOGON';	Alto

			Asegúrese de que VALUE este establecido en TRUE. Para remediar esta configuración, ejecute la siguiente instrucción SQL. ALTER SYSTEM SET SEC_CASE_SENSITIVE_LOGON = TRUE SCOPE = SPFILE;	
4.2.16	Asegurar 'SEC_MAX_FAILED_LOGIN_ATTEMPTS'	El parámetro SEC_MAX_FAILED_LOGIN_ATTEMPTS determina cuántos intentos fallidos de inicio de sesión se permiten antes de que Oracle cierre la conexión de inicio de sesión.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL. SELECT UPPER(VALUE) FROM V$SYSTEM_PARAMETER WHERE UPPER(NAME)='SEC_MAX_FAILED_LOGIN_ATTEMPTS'; Asegúrese de que VALUE este establecido en 3. Para remediar esta configuración, ejecute la siguiente instrucción SQL. ALTER SYSTEM SET SEC_MAX_FAILED_LOGIN_ATTEMPTS = 3 SCOPE = SPFILE;	Alto
4.2.17	Asegurar 'SEC_PROTOCOL_ERROR_FURTHER_ACTION'	La configuración SEC_PROTOCOL_ERROR_FURTHER_ACTION determina la respuesta del servidor de Oracle a paquetes defectuosos/deformados recibidos del cliente.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL. SELECT UPPER(VALUE) FROM V$SYSTEM_PARAMETER WHERE UPPER(NAME)='SEC_PROTOCOL_ERROR_FURTHER_ACTION';	Alto

		Los paquetes defectuosos recibidos del cliente pueden indicar potencialmente ataques basados en paquetes en el sistema, como ataques "TCP SYN Flood" o "Smurf", que podrían resultar en una condición de denegación de servicio, este valor debe establecerse de acuerdo con las necesidades de la organización.	Asegúrese de que VALUE este establecido en (DROP,3). Para remediar esta configuración, ejecute la siguiente instrucción SQL. ALTER SYSTEM SET SEC_PROTOCOL_ERROR_FURTHER_ACTION = '(DROP,3)' SCOPE = SPFILE;	
4.2.18	Asegurar 'SQL92_SECURITY'	La configuración del parámetro SQL92_SECURITY TRUE requiere que un usuario también tenga el Privilegio de objeto SELECT antes de poder realizar operaciones UPDATE o DELETE en las tablas que tienen cláusulas WHERE o SET.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL. SELECT UPPER(VALUE) FROM V$SYSTEM_PARAMETER WHERE UPPER(NAME)='SQL92_SECURITY'; Asegúrese de que VALUE este establecido en TRUE. Para remediar esta configuración, ejecute la siguiente instrucción SQL. ALTER SYSTEM SET SQL92_SECURITY = TRUE SCOPE = SPFILE;	Alto
4.2.19	Asegurar '_trace_files_public'	La configuración _trace_files_public determina si el archivo de seguimiento del sistema es legible en todo el mundo o no.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL. SELECT VALUE FROM V$SYSTEM_PARAMETER WHERE NAME='_trace_files_public';	Alto

			El VALUE igual a FALSE o la falta de resultados implica el cumplimiento. Para remediar esta configuración, ejecute la siguiente instrucción SQL. ALTER SYSTEM SET "_trace_files_public" = FALSE SCOPE = SPFILE;	

4.3. Conexión y Restricción Login

ITEM	Vulnerabilidad	Descripción	Remediación	Impacto
4.3.1	Intentos de inicio de sesión fallidos	La configuración de PASSWORD_LOCK_TIME determina cuántos días deben pasar para que el usuario cuenta que se desbloqueará después de que se haya producido el número establecido de intentos fallidos de inicio de sesión.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL. SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME='PASSWORD_LOCK_TIME') AND (LIMIT='DEFAULT' OR LIMIT='UNLIMITED' OR LIMIT < 1); La falta de resultados implica el cumplimiento. Corrija esta configuración ejecutando la siguiente instrucción SQL para cada PROFILE devuelto por el procedimiento de auditoría.	Alto

			ALTER PROFILE <profile_name> LIMIT PASSWORD_LOCK_TIME 1;	
4.3.2	Asegurar 'PASSWORD_LIFE_TIME'	La configuración PASSWORD_LIFE_TIME determina cuánto tiempo se puede usar una contraseña antes de que el usuario deba cambiarla.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL. SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME='PASSWORD_LIFE_TIME') AND (LIMIT='DEFAULT' OR LIMIT='UNLIMITED' OR LIMIT > 90); La falta de resultados implica el cumplimiento. Corrija esta configuración ejecutando la siguiente instrucción SQL para cada PROFILE devuelto por el procedimiento de auditoría. ALTER PROFILE <profile_name> LIMIT PASSWORD_LIFE_TIME 90;	Alto
4.3.3	Asegurar 'PASSWORD_REUSE_MAX'	La configuración PASSWORD_REUSE_MAX determina cuántas contraseñas diferentes se deben usar antes de que el usuario pueda reutilizar una contraseña anterior.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL. SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME='PASSWORD_REUSE_MAX') AND (LIMIT='DEFAULT' OR LIMIT='UNLIMITED' OR LIMIT < 20);	Alto

			La falta de resultados implica el cumplimiento. Corrija esta configuración ejecutando la siguiente instrucción SQL para cada PROFILE devuelto por el procedimiento de auditoría. ALTER PROFILE <profile_name> LIMIT PASSWORD_REUSE_MAX 20;	
4.3.4	Asegurar FAILED_LOGIN_ATTEMPTS	La configuración FAILED_LOGIN_ATTEMPTS determina cuántos intentos fallidos de inicio de sesión se permiten antes de que el sistema bloquee la cuenta del usuario. Si bien los diferentes perfiles pueden tener configuraciones diferentes y más restrictivas, como USUARIOS y APLICACIONES, los mínimos recomendados aquí deben configurarse en el perfil DEFAULT.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL. SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME=' FAILED_LOGIN_ATTEMPTS ') AND (LIMIT='DEFAULT' OR LIMIT='UNLIMITED' OR LIMIT > 5); La falta de resultados implica el cumplimiento. Corrija esta configuración ejecutando la siguiente instrucción SQL para cada PROFILE devuelto por el procedimiento de auditoría. ALTER PROFILE <profile_name> LIMIT FAILED_LOGIN_ATTEMPTS 5;	Alto
4.3.5	Asegurar 'PASSWORD_GRACE_TIME'	La configuración de PASSWORD_GRACE_TIME determina cuántos días	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL.	Alto

		pueden pasar después de que el usuario la contraseña caduca antes de que la capacidad de inicio de sesión del usuario se bloquee automáticamente. El el valor sugerido para esto es cinco días o menos.	SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME=' 'PASSWORD_GRACE_TIME ') AND (LIMIT='DEFAULT' OR LIMIT='UNLIMITED' OR LIMIT > 5); La falta de resultados implica el cumplimiento. Corrija esta configuración ejecutando la siguiente instrucción SQL para cada PROFILE devuelto por el procedimiento de auditoría. ALTER PROFILE <profile_name> LIMIT PASSWORD_GRACE_TIME 5;	
4.3.6	Asegurar 'PASSWORD_VERIFY_FUNCTION'	PASSWORD_VERIFY_FUNCTION determina los requisitos de configuración de la contraseña cuando se cambia la contraseña de un usuario en el símbolo del sistema SQL. Debe configurarse para todos los perfiles. Tenga en cuenta que esta configuración no se aplica a los usuarios administrados por el archivo de contraseñas de Oracle.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL. SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME='PASSWORD_VERIFY_FUNCTION') AND (LIMIT='DEFAULT' OR LIMIT=NULL); La falta de resultados implica el cumplimiento. Cree una función de verificación de contraseña personalizada que	Alto

			cumpla con los requisitos de contraseña de la organización.	
4.3.7	Asegurar ' SESSIONS_PER_USER '	La configuración SESSIONS_PER_USER determina el número máximo de sesiones de usuario que se se permite estar abierto al mismo tiempo.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL. SELECT PROFILE, RESOURCE_NAME, LIMIT FROM DBA_PROFILES WHERE RESOURCE_NAME=' SESSIONS_PER_USER ') AND (LIMIT='DEFAULT' OR LIMIT='UNLIMITED' OR LIMIT > 10); La falta de resultados implica el cumplimiento. Para remediar esta configuración, ejecute la siguiente instrucción SQL para cada PERFIL devuelto por el procedimiento de auditoría. ALTER PROFILE <profile_name>LIMIT SESSIONS_PER_USER 10;	Alto
4.3.8	Asegurar que a ningún usuario se le asigne el perfil 'DEFAULT'	Tras la creación de la base de datos, los usuarios se asignan al perfil DEFAULT a menos que se especifique lo contrario. No se debe asignar ningún usuario a ese perfil.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL. SELECT USERNAME FROM DBA_USERS WHERE PROFILE='DEFAULT' AND ACCOUNT_STATUS='OPEN' AND USERNAME NOT IN ('ANONYMOUS', 'CTXSYS', 'DBSNMP', 'EXFSYS', 'LBACSYS',	Alto

			'MDSYS', 'MGMT_VIEW','OLAPSYS','OWBSYS', 'ORDPLUGINS', 'ORDSYS', 'OUTLN', 'SI_INFORMTN_SCHEMA','SYS', 'SYSMAN', 'SYSTEM', 'TSMSYS', 'WK_TEST', 'WKSYS', 'WKPROXY', 'WMSYS', 'XDB', 'CISSCAN'); La falta de resultados implica el cumplimiento. Para remediar esta recomendación, ejecute la siguiente instrucción SQL para cada usuario devuelto por la consulta de auditoría utilizando un perfil funcional apropiado. ALTER USER <username> PROFILE <appropriate_profile>;	

4.4. Privilegios Públicos y Objetos

ITEM	Vulnerabilidad	Descripción	Remediación	Impacto
4.4.1	SELECT ANY DICTIONARY	Permite al usuario ver las definiciones de todos los objetos del esquema en la base de datos. Habilitar la opción de auditoría hace que se auditen todas las actividades del usuario relacionadas con esta capacidad.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT AUDIT_OPTION,SUCCESS,FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE USER_NAME IS NULL AND PROXY_NAME IS NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS' AND AUDIT_OPTION='SELECT ANY DICTIONARY';	Alto

			Para remediar esta configuración, ejecute el siguiente SQL REVOKE SELECT_ANY_DIRECTORY FROM <grantee>	
4.4.2	Asegurar de que 'EXECUTE' esté revocado de 'PUBLIC' en DBMS_CRYPTO	La configuración de DBMS_CRYPTO proporciona un conjunto de herramientas que determina la solidez del algoritmo de cifrado utilizado para cifrar los datos de la aplicación y es parte del esquema SYS. Están disponibles DES (clave de 56 bits), 3DES (clave de 168 bits), 3DES-2KEY (clave de 112 bits), AES (claves de 128/192/256 bits) y RC4.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_CRYPTO'; Para remediar esta configuración, ejecute el siguiente SQL REVOKE EXECUTE ON DBMS_CRYPTO FROM PUBLIC;	Alto
4.4.3	Asegurar de que 'EXECUTE' esté revocado de 'PUBLIC' en DBMS_CRYPTO	La configuración de DBMS_CRYPTO proporciona un conjunto de herramientas que determina la solidez del algoritmo de cifrado utilizado para cifrar los datos de la aplicación y es parte del esquema SYS. Están disponibles DES (clave de 56 bits), 3DES (clave de 168 bits), 3DES-2KEY (clave de 112 bits), AES (claves de 128/192/256 bits) y RC4.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND PRIVILEGE='EXECUTE' AND TABLE_NAME='DBMS_CRYPTO'; Para remediar esta configuración, ejecute el siguiente SQL REVOKE EXECUTE ON DBMS_CRYPTO FROM PUBLIC;	Alto
4.4.4	Asegurar de que 'EXECUTE' esté revocado de	El paquete UTL_TCP podría permitir que un usuario no autorizado corrompa el flujo TCP utilizado para	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL	Alto

	'PUBLIC' en UTL_TCP	transportar los protocolos que se comunican con las comunicaciones externas de la instancia.	SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND PRIVILEGE='EXECUTE' AND TABLE_NAME= 'UTL_TCP'; La falta de resultados implica el cumplimiento. Para remediar esta configuración, ejecute el siguiente SQL REVOKE EXECUTE ON UTL_TCP FROM PUBLIC;	
4.4.5	Asegurar de que 'EXECUTE' esté revocado de 'PUBLIC' en UTL_MAIL	El paquete UTL_MAIL podría permitir que un usuario no autorizado corrompa la función SMTP para aceptar o generar correo no deseado que puede resultar en una condición de denegación de servicio debido a la saturación de la red.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND PRIVILEGE='EXECUTE' AND TABLE_NAME= 'UTL_MAIL'; La falta de resultados implica el cumplimiento. Para remediar esta configuración, ejecute el siguiente SQL REVOKE EXECUTE ON UTL_MAIL FROM PUBLIC;	Alto
4.4.6	Asegurar de que 'EXECUTE' esté revocado de 'PUBLIC' en UTL_SMTP	El paquete UTL_SMTP podría permitir que un usuario no autorizado corrompa la función SMTP para aceptar o generar correo no deseado que puede resultar en una condición de denegación de	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND PRIVILEGE='EXECUTE' AND TABLE_NAME= 'UTL_SMTP';	Alto

		servicio debido a la saturación de la red.	La falta de resultados implica el cumplimiento. Para remediar esta configuración, ejecute el siguiente SQL REVOKE EXECUTE ON UTL_SMTP FROM PUBLIC;	
4.4.7	Asegurar de que 'EXECUTE' esté revocado de 'PUBLIC' en UTL_HTTP	El paquete UTL_SMTP podría permitir que un El paquete UTL_HTTP podría usarse para enviar información (sensible) a sitios web externos.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND PRIVILEGE='EXECUTE' AND TABLE_NAME= 'UTL_HTTP'; La falta de resultados implica el cumplimiento. Para remediar esta configuración, ejecute el siguiente SQL REVOKE EXECUTE ON UTL_HTTP FROM PUBLIC;	Alto
4.4.8	Asegurar de que 'EXECUTE' esté revocado de 'PUBLIC' en DBMS_SYS_SQL	El paquete DBMS_SYS_SQL podría permitir que un usuario ejecute código como un usuario diferente sin ingresar credenciales válidas.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND PRIVILEGE='EXECUTE' AND TABLE_NAME= 'DBMS_SYS_SQL'; La falta de resultados implica el cumplimiento.	Alto

			Para remediar esta configuración, ejecute el siguiente SQL REVOKE EXECUTE ON DBMS_SYS_SQL FROM PUBLIC;	
4.4.9	Asegurar de que 'EXECUTE ANY PROCEDURE' esté revocado de 'OUTLN'	Elimine los privilegios de EXECUTE ANY PROCEDURE innecesarios de OUTLN.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT GRANTEE, PRIVILEGE FROM DBA_SYS_PRIVS WHERE PRIVILEGE='EXECUTE ANY PROCEDURE' AND GRANTEE='OUTLN'; Para remediar esta configuración, ejecute el siguiente SQL REVOKE EXECUTE ANY PROCEDURE FROM OUTLN;	Alto
4.4.10	Asegurar de que 'EXECUTE' esté revocado de 'PUBLIC' en UTL_FILE	El uso del paquete UTL_FILE podría permitir a un usuario leer archivos del sistema operativo. Estos archivos pueden contener información confidencial (por ejemplo, contraseñas en .bash_history)	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT PRIVILEGE FROM DBA_TAB_PRIVS WHERE GRANTEE='PUBLIC' AND PRIVILEGE='EXECUTE' AND TABLE_NAME= 'UTL_FILE'; Para remediar esta configuración, ejecute el siguiente SQL REVOKE EXECUTE ON UTL_FILE FROM PUBLIC;	Alto

4.5. Auditoria y Políticas de acceso

ITEM	Vulnerabilidad	Descripción	Remediación	Impacto
4.5.1	Opción de auditoria drop user	Dado que el registro de las actividades de los usuarios que involucran la creación, alteración o eliminación de un usuario puede proporcionar evidencia forense sobre un patrón de actividades sospechosas/no autorizadas, la capacidad de auditoría debe establecerse de acuerdo con las necesidades de la organización.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT AUDIT_OPTION, SUCCESS, FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='DROP USER'AND USER_NAME IS NULL AND PROXY_NAME IS NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS'; Para remediar esta configuración, ejecute el siguiente SQL AUDIT DROP USER	Alto
4.5.2	Habilitar la opción de auditoría de usuario	El objeto USUARIO permite crear cuentas que pueden interactuar con la base de datos de acuerdo con los roles y privilegios asignados a la cuenta. También puede poseer objetos de base de datos.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT AUDIT_OPTION,SUCCESS,FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE USER_NAME IS NULL AND PROXY_NAME IS NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS' AND AUDIT_OPTION='USER'; Para remediar esta configuración, ejecute el siguiente SQL AUDIT USER;	Alto
4.5.3	Habilitar la opción de auditoría ALTER USER	La instrucción ALTER USER se usa para cambiar la contraseña de los usuarios	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL	Alto

		de la base de datos, bloquear cuentas y expirar las contraseñas. Además, esta declaración se utiliza para cambiar las propiedades de la base de datos del usuario. cuentas como perfiles de bases de datos, tablespaces predeterminados y temporales y cuotas de tablespaces. Esta acción de auditoría unificada permite el registro de todas las declaraciones ALTER USER, ya sea con éxito o sin éxito, emitidas por los usuarios, independientemente de los privilegios que tengan los usuarios para emitir dichas declaraciones.	SELECT AUDIT_OPTION,SUCCESS,FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE AUDIT_OPTION='ALTER USER' AND USER_NAME IS NULL AND PROXY_NAME IS NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS'; La falta de resultados implica el cumplimiento. Para remediar esta configuración, ejecute el siguiente SQL AUDIT ALTER USER;	
4.5.4	Habilitar la opción de auditoría PROFILE	El objeto PROFILE permite la creación de un conjunto de límites de recursos de base de datos que se pueden asignar a un usuario, de modo que ese usuario no pueda exceder esas limitaciones de recursos.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT AUDIT_OPTION,SUCCESS,FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE USER_NAME IS NULL AND PROXY_NAME IS NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS'; La falta de resultados implica el cumplimiento. Para remediar esta configuración, ejecute el siguiente SQL AUDIT PROFILE;	Medio

4.5.5	Habilitar la opción de auditoría SYNONYM	La operación SYNONYM permite la creación de un nombre alternativo para un objeto de base de datos, como un objeto de esquema de clase Java, una vista materializada, un operador, un paquete, un procedimiento, una secuencia, una función almacenada, una tabla, una vista, un tipo de objeto definido por el usuario o incluso otro sinónimo. Este sinónimo pone una dependencia en su destino y se vuelve inválido si el objeto de destino se cambia/elimina.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT AUDIT_OPTION,SUCCESS,FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE USER_NAME IS NULL AND PROXY_NAME IS NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS' AND AUDIT_OPTION='SYNONYM'; La falta de resultados implica el cumplimiento. Para remediar esta configuración, ejecute el siguiente SQL AUDIT SYNONYM;	Alto
4.5.6	Habilitar la opción de auditoría 'GRANT ANY OBJECT PRIVILEGE'	GRANT ANY OBJECT PRIVILEGE permite al usuario otorgar o revocar cualquier privilegio de objeto, que incluye privilegios sobre tablas, directorios, modelos de minería, etc.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT AUDIT_OPTION,SUCCESS,FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE USER_NAME IS NULL AND PROXY_NAME IS NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS' AND AUDIT_OPTION='GRANT ANY OBJECT PRIVILEGE'; La falta de resultados implica el cumplimiento. Para remediar esta configuración, ejecute el siguiente SQL	Alto

			AUDIT GRANT ANY OBJECT PRIVILEGE;	
4.5.7	Habilitar la opción de auditoría 'GRANT ANY OBJECT PRIVILEGE'	GRANT ANY OBJECT PRIVILEGE permite al usuario otorgar o revocar cualquier privilegio de objeto, que incluye privilegios sobre tablas, directorios, modelos de minería, etc.	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT AUDIT_OPTION,SUCCESS,FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE USER_NAME IS NULL AND PROXY_NAME IS NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS' AND AUDIT_OPTION='GRANT ANY OBJECT PRIVILEGE'; La falta de resultados implica el cumplimiento. Para remediar esta configuración, ejecute el siguiente SQL AUDIT GRANT ANY OBJECT PRIVILEGE;	Alto
4.5.8	Habilitar la opción de auditoría 'TRIGGER'	Se puede usar un TRIGGER para modificar acciones DML o invocar otras acciones (recursivas) cuando ocurren algunos tipos de acciones iniciadas por el usuario. Habilitar esta opción de auditoría provocará la auditoría de cualquier intento, exitoso o no, de crear, descartar, habilitar o deshabilitar cualquier activador de esquema en cualquier esquema, independientemente del	Para evaluar esta recomendación, ejecute la siguiente instrucción SQL SELECT AUDIT_OPTION,SUCCESS,FAILURE FROM DBA_STMT_AUDIT_OPTS WHERE USER_NAME IS NULL AND PROXY_NAME IS NULL AND SUCCESS = 'BY ACCESS' AND FAILURE = 'BY ACCESS' AND AUDIT_OPTION='TRIGGER'; La falta de resultados implica el cumplimiento.	Alto

		privilegio o la falta del mismo.	Para remediar esta configuración, ejecute el siguiente SQL AUDIT TRIGGER;	

5. Regulaciones

PCI-DSS Estándar de seguridad de datos de la industria de tarjetas de pago.

6. Referencias

- https://benchmarks.cisecurity.org