

**UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS**

**FACULTAD 4**

**Informe Técnico de SBDII - Seguridad**

Autores: Joaquin Rivas Sánchez

Tutor: Luis Manuel Valera Perez

**La Habana, marzo 2024**

**“Año 65 de la Revolución”**

**Introducción**

El presente Informe Técnico de Seguridad de la Base de Datos de la Biblioteca Nacional José Martí tiene como objetivo principal desarrollar una política integral que garantice la seguridad, confidencialidad y disponibilidad de la información almacenada en la base de datos de esta institución. La seguridad de los datos es fundamental para el correcto funcionamiento de la biblioteca, ya que almacena información crítica sobre los recursos bibliográficos, los miembros, los préstamos y la informacion referente a los procesos internos. En este informe, se abordarán buenas prácticas, controles de acceso, protección de la red y requisitos para garantizar la seguridad de la base de datos, con el fin de protegerla de posibles amenazas internas y externas

**Desarrollo**

**Contexto Organizacional**

La Biblioteca Nacional José Martí es una institución pública que alberga una vasta colección de recursos bibliográficos y multimedia. La base de datos es esencial para el funcionamiento eficiente de la biblioteca, ya que almacena información sobre los recursos disponibles, los miembros de la biblioteca, los préstamos y las transacciones.

Se ha detectado un aumento en los incidentes de acceso no autorizado a la base de datos, lo que ha generado preocupación en cuanto a la seguridad de la información almacenada. Se ha identificado que algunos usuarios han logrado acceder a recursos bibliográficos restringidos y han realizado modificaciones no autorizadas en los registros de préstamos, lo que pone en riesgo la integridad de los datos y la confidencialidad de la información de los miembros de la biblioteca. Ante esta situación, es imperativo revisar y reforzar la estructura de roles y accesos en la base de datos para garantizar la seguridad y protección de los datos.

**Requisitos Generales Previos**

- Todos los sistemas operativos del servidor deben estar protegidos

- Se debe asegurar y gestionar las redes y dispositivos de red para garantizar la protección de la información

- Se deben evitar los servicios o protocolos no seguros o sin cifrar (por ejemplo, HTTP, FTP, etc)

- Siempre que sea posible, se deben deshabilitar o eliminar los servicios o puertos innecesarios

- Se deben implementar controles de protección, como sistemas de detección de intrusiones, firewalls, soluciones anti-malware, etc.

- Se deben llevar a cabo evaluaciones de seguridad técnicas, como pruebas de penetración, simulaciones de ataques cibernéticos, ejercicios de respuesta cibernética, evaluaciones de vulnerabilidad, etc.

**Requisitos para garantizar la seguridad de la base de datos**

- Todas las bases de datos deben alojarse en servidores que no realicen ninguna otra función, como la “función de aplicación web”.

- Se deben determinar los riesgos de seguridad asociados con las bases de datos especiales y se deben desarrollar soluciones apropiadas.

- Se deben implementar y desarrollar controles de seguridad adecuados para proteger la información confidencial en las bases de datos.

- Los deberes deben segregarse con diferentes privilegios para que ningún equipo o personal sea completamente responsable de todos los procesos de las bases de datos. Esto implica la implementación del “principio de segregación de deberes”.

**Amenazas Potenciales**

Las amenazas potenciales pueden incluir ataques cibernéticos, como intentos de acceso no autorizado, inyección de SQL, robo de datos y ransomware. También pueden surgir amenazas internas, como el acceso indebido a la información por parte del personal o errores humanos que resulten en la pérdida o corrupción de datos.

**Buenas Prácticas**

Principio del Menor Privilegio: Asigna los permisos mínimos necesarios para cada rol. No otorgues más privilegios de los requeridos

Roles en Lugar de Usuarios Individuales: Agrupa permisos en roles en lugar de asignarlos directamente a usuarios individuales

Roles Basados en Funcionalidad: Crea roles que reflejen funciones específicas (por ejemplo, “Lectura”, “Escritura”, “Administrador”)

Roles de Solo Lectura: Crea roles de solo lectura para usuarios que no necesitan modificar datos.

Auditoría de Roles: Regularmente revisa y actualiza los roles

Documentación Detallada: Documenta claramente los roles, sus responsabilidades y los permisos asociados.

**Control de Acceso**

| Rol | Descripción | Nivel | Operaciones | Objetos |
| --- | --- | --- | --- | --- |
| dba | El Administrador/a define la estructura de la base de datos, controla los niveles de acceso y garantiza la seguridad. También se encarga de la recuperación y el respaldo de datos | Muy Alto | all | database |
| audit | El Auditor supervisa la seguridad y detecta posibles vulnerabilidades | Medio | select | audit tables |
| director | El director toma decisiones estratégicas y supervisa el funcionamiento general. | Alto | select, update, delete | library, room |
| librarian | El Bibliotecario/a Gestiona y organiza los recursos bibliográficos. | Medio | all | collection, collection\_document, document, manuscript, map, picture, paint, media, music, reference, magazine, book  service, loan, fine |
| cataloger | El Catalogador/a cataloga y clasifica los materiales bibliográficos | Medio | update | collection, collection\_document, document, manuscript, map, picture, paint, media, music, reference, magazine, book |
| public\_usr | El Usuario General consulta materiales | Bajo | select | igual que cataloger  adicionalmente:  room, phone, email, service |
| membership  \_manager | Es el encargado/a de registrar a los miembros que desean unirse a la biblioteca. | Moderado | all | member |
| member | Puede acceder a su información y los préstamos que solicite así como multas en la que incurra | Medio | select | restringido:  member, loan, fine |

Ver anexos para la creación de estos roles: , , ,

**Protección de la red**

Se restringe el acceso al servidor de base de datos y para eso se modificaron los siguientes parámetros del archivo de configuración **postgres.conf**

#------------------------------------------------

# CONNECTIONS AND AUTHENTICATION

#------------------------------------------------

max\_connections = 10

reserved\_connections = 3

authentication\_timeout = 1min

password\_encryption = scram-sha-256

Se hizo un mapeo del usuario del sistema operativo al usuario de postgres usando el archivo **pg\_ident.conf**

# PostgreSQL User Name Maps

# =========================

# MAPNAME SYSTEM-USERNAME PG-USERNAME

god admin dba

Se configuro las direcciones que podían tener acceso a la base de datos usando el archivo pg\_hba.conf

1. debe ser posible las conecciones desde el mismo servidor

2. debe ser posible la coneccion desde todas las subredes de 10.10.4 con contraseña cifrada

3. debe ser posible la coneccion desde otros centros de datos a la base de datos mediante una conexión cifrada y con contraseña cifrada con el usuario 'remote'

| TYPE | DATABASE | USER | ADDRESS | METHOD |
| --- | --- | --- | --- | --- |
| local | all | all | 127.0.0.1/32 | trust |
| host | all | all | 10.10.4.0/24 | md5 |
| hostssl | all | remote | 10.23.8.0/24 | md5 |

**Otras protecciones**

Copia de seguridad y recuperación:

Realiza copias de seguridad de tu base de datos con regularidad y prueba el proceso de restauración.

Almacena las copias de seguridad de forma segura, lejos del entorno de producción.

Gestión de parches:

Mantén actualizado el software de tu base de datos aplicando los parches de seguridad de manera oportuna.

Revisa periódicamente los avisos de seguridad proporcionados por el proveedor de la base de datos.

Seguridad física:

Asegura el acceso físico a los servidores que alojan la base de datos.

Limita el acceso solo al personal autorizado.

**Herramientas para Manejar la seguridad de PostgreSQL**

pgcrypto: Una extension de PostgreSQL para funciones criptograficas

CipherStash: Aumenta la seguridad proporcionando funciones adicionales

PGAudit: Audita la actividad de la base de datos y los eventos registrados

**Conclusiones**

En conclusión, la implementación de una política de seguridad integral es crucial para proteger la base de datos de la Biblioteca Nacional José Martí. Mediante la aplicación de buenas prácticas, como el principio del menor privilegio, la auditoría de roles y la segregación de deberes, se puede reducir el riesgo de accesos no autorizados y garantizar un uso adecuado de los recursos. Además, la protección de la red y la implementación de controles de seguridad adecuados son fundamentales para prevenir amenazas cibernéticas y garantizar la confidencialidad de la información almacenada en la base de datos.

**Bibliografía Consultada**

“Seguridad de la base de datos: una guía de introducción.” *IBM*, <https://www.ibm.com/mx-es/topics/database-security>.

**Anexos**

****

Figura 1:

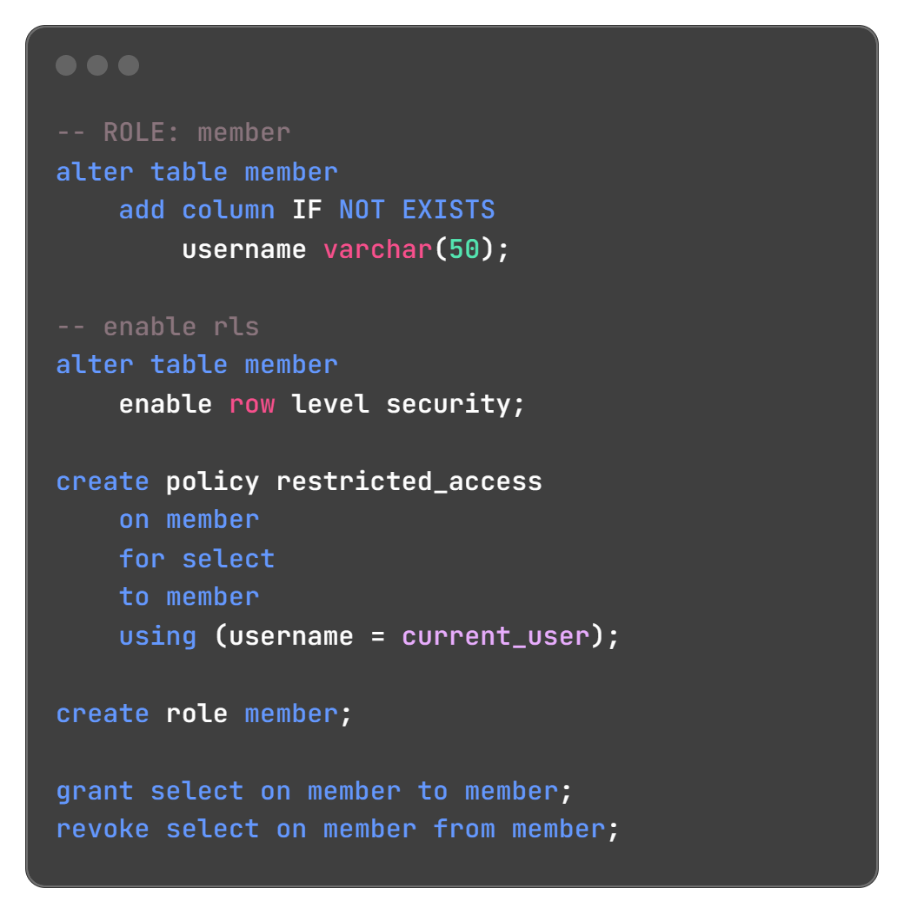
****

Figura 2:

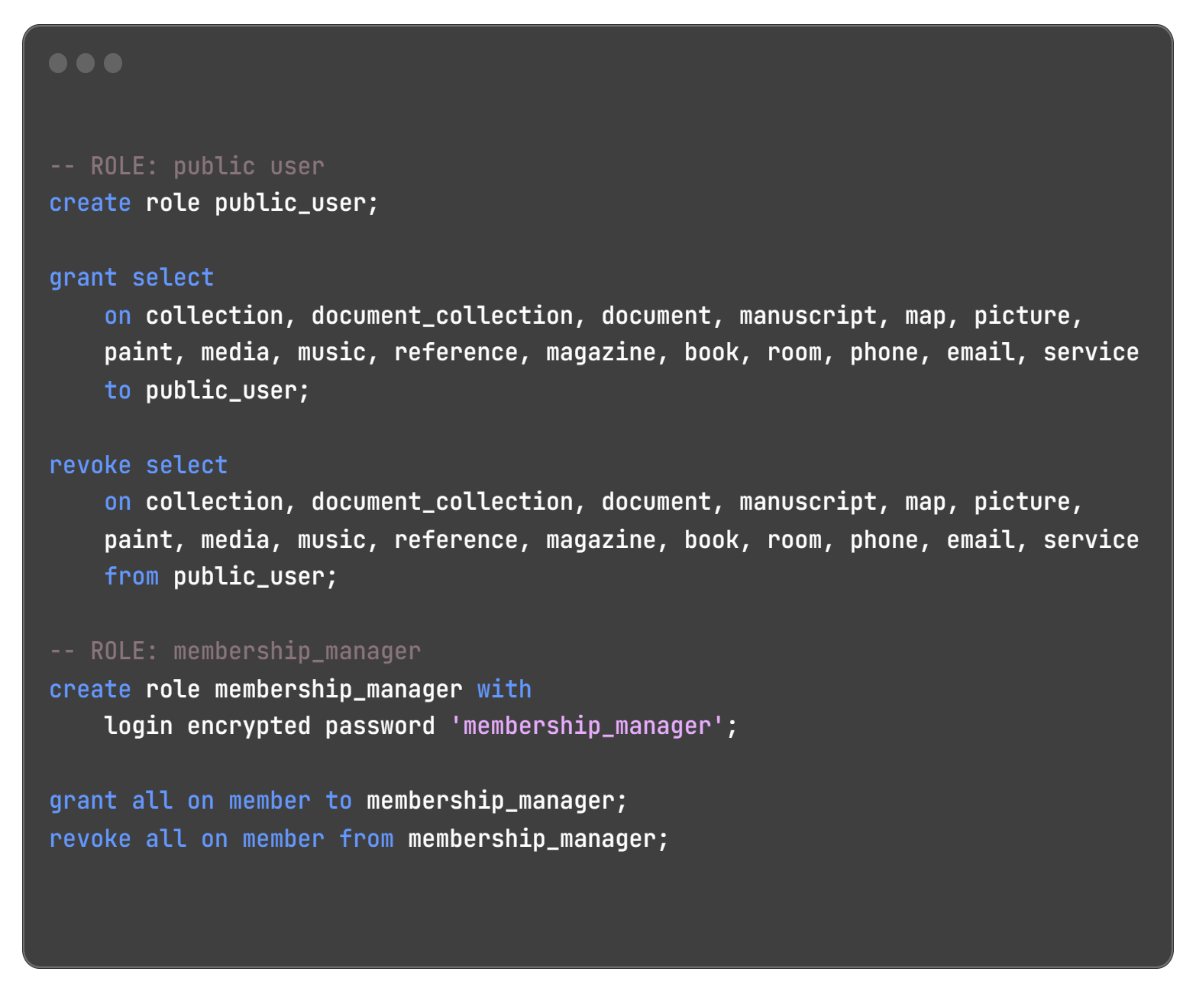
****

Figura 3:

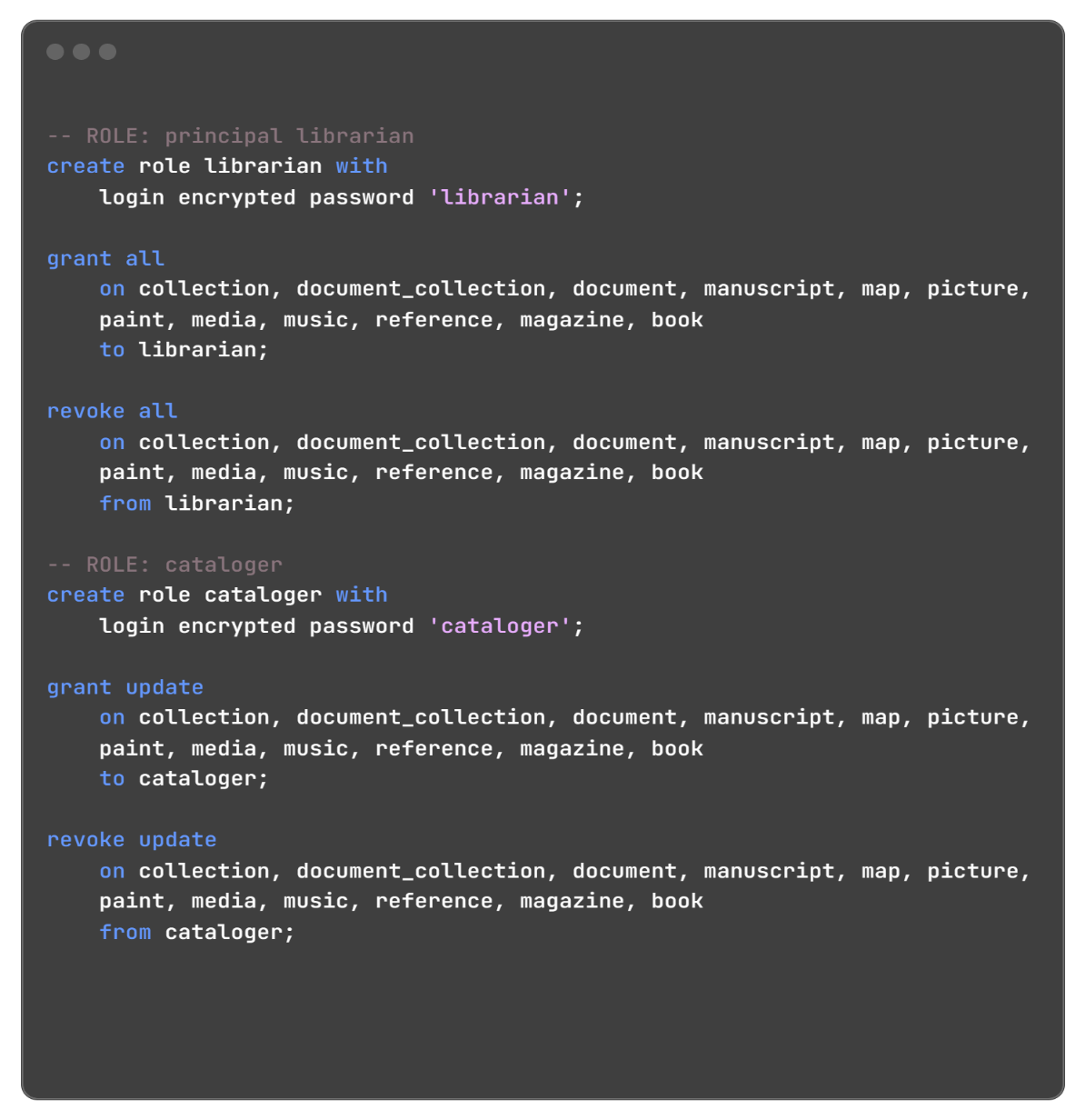
****

Figura 4: