EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO

Instituto Tecnológico de Aguascalientes

INGENIERÍA _TIC´S____

Nombre de la Asignatura

AUDITORIA EN TECNOLOGIA DE INFORMACION

Bitacora

Profesor: Juan Carlos Sánchez Gaytán

Alumnos:

Edith Marisol Ramírez González 21150988

Jesús Uriel Flores Zavala 21151007

González Mena Emit Alfredo 21151057

Gabriel Alejandro Corona Moreno 21151028

Roberto Bravo Juárez 21150996

Fecha:16/04/2025

Instituto Tecnológico de Aguascalientes

Nombre de la organización: Ejemplo S.A.
Fecha de auditoría: 2025-04-20
Duración estimada: 1 día
Alcance: Seguridad de la información en la administración y operación de la base de datos del SGSI
Norma de referencia: ISO/IEC 27001

1. Objetivo de la Auditoría

- Verificar cumplimiento y efectividad de los controles de seguridad en la base de datos.
- Asegurar la confidencialidad, integridad y disponibilidad de la información.
- Identificar deficiencias, riesgos y oportunidades de mejora.

2. **Estructura Orgánica (Roles y Responsabilidades)**

Rol	**Nombre / Cargo**	**Responsabilidad**
Auditor líder	Edith Marisol Ramírez Gonzalez (Auditor interno)	Coordinación general, entrevistas, informe final
Auditor auxiliar	Roberto Bravo Juarez (Auditor interno)	Revisión técnica, análisis de evidencias, registros
Auditado 1	Jesús Uriel Flores Zavala (DBA)	Proveer evidencias y explicar configuraciones
Auditado 2	González Mena Emit Alfredo (Responsable SGSI)	Proveer políticas y controles documentales
Auditado 3	Gabriel Alejandro Corona Moreno (Soporte TI)	Apoyo en accesos, respaldos y eventos técnicos

3. **Recursos Humanos y Capacidades**

Persona	**Habilidad / Especialidad**
Edith Marisol Ramírez González	**Conoce la norma ISO 27001 y sabe hacer auditorías**
Roberto Bravo Juárez	**Sabe revisar bases de datos y sistemas de seguridad**
Jesús Uriel Flores Zavala	**Administra la base de datos y conoce los accesos**
González Mena Emit Alfredo	**Maneja los documentos del sistema de seguridad**
Gabriel Alejandro Corona Moreno	**Apoya con temas técnicos y copias de seguridad**

4. **Presupuesto Financiero Estimado**

Concepto	**Costo estimado (MXN)**
Horas de personal (auditores)	$4,000
Horas de auditados (participación)	$2,500
Herramientas de auditoría	$1,000
Documentación final e impresión	$500
Total estimado	**$8,000**

5. Metodología de Auditoría

- Revisión documental
- Entrevistas técnicas y administrativas
- Verificación de controles y configuraciones
- Análisis de registros y evidencias
- Informe de hallazgos y recomendaciones

6. **Actividades y Cronograma**

Hora	**Actividad**	**Responsables**
09:00 – 09:30	Reunión de apertura	Edith, Roberto, Gabriel, Emit, Uriel
09:30 – 10:30	Revisión de accesos y roles	Roberto, Uriel
10:30 – 11:30	Evaluación de respaldos y restauraciones	Edith, Emit
11:30 – 12:30	Análisis de registros y eventos de seguridad	Uriel, Emit
12:30 – 13:00	Verificación documental del SGSI	Edith, Gabriel
13:00 – 14:00	Entrevistas técnicas y operativas	Edith, Roberto, Uriel, Gabriel, Emit
14:00 – 15:00	Redacción de hallazgos preliminares	Edith, Roberto
15:00 – 16:00	Reunión de cierre y entrega de observaciones	Todos

7. **Bitácora de Resultados**

Fecha	Actividad Realizada	Evidencia Recabada	Observaciones / Hallazgos
2025-04-20	Revisión de accesos y roles	Listado de usuarios y permisos	Usuarios con privilegios sin justificación
2025-04-20	Validación de respaldos	Reporte de backups	Falta política clara de restauración
2025-04-20	Revisión de logs de eventos	Archivos de log	Eventos sin clasificación o respuesta
2025-04-20	Verificación de políticas y documentación	Manuales y procedimientos	Documentos desactualizados
2025-04-20	Entrevistas	Minutas	Personal no capacitado en control de accesos

8. **Seguimiento y Cierre**

- **Informe final:** 2025-04-21 (entregado a Dirección de TI y SGSI)
- **Revisión de hallazgos críticos:** antes del 2025-04-30
- **Plan de acción correctiva:** elaborado por Laura, Mario y Andrea
- **Seguimiento de mejoras:** 2025-05-21 (auditoría de seguimiento)

2. Objetivo de la Auditoría

Evaluar de manera integral la eficacia de los controles de seguridad implementados en el sistema de gestión de bases de datos, con el propósito de garantizar la **confidencialidad, integridad y disponibilidad** de la información institucional.

La auditoría también tiene como fin identificar **deficiencias, riesgos potenciales y oportunidades de mejora**, así como verificar el cumplimiento de buenas prácticas en la administración y protección de los datos.

2. Alcance

Evaluación del control de accesos y autenticación en los sistemas de base de datos
Verificar que se apliquen mecanismos robustos de autenticación, que se eviten cuentas por defecto, y que haya registros de los accesos realizados por los usuarios.
Validación del cumplimiento de políticas de respaldo y recuperación ante incidentes
Asegurar que exista una política documentada y aplicada para respaldos automáticos, restauración periódica, y planes de continuidad del negocio.

Riesgo Identificado	Descripción	Nivel de Riesgo	Controles sugeridos
Pérdida de respaldo	El respaldo lógico no se guarda adecuadamente o se elimina por error	**Alto**	Automatizar respaldo y replicar en diferentes ubicaciones seguras
Falta de cifrado	El respaldo no está cifrado y puede ser accedido por terceros	**Alto**	Implementar cifrado en el respaldo lógico (Transparent Data Encryption, herramientas externas)
Almacenamiento inseguro	El respaldo se guarda en rutas locales no protegidas	**Alto**	Almacenar en servidores seguros o en la nube con autenticación
Acceso no controlado	Personas no autorizadas pueden acceder a los archivos de respaldo	**Alto**	Establecer roles y permisos de acceso, monitorear accesos
Inyección SQL	Vulnerabilidad en aplicaciones permite	**Alto**	Uso de procedimientos almacenados, validación de entradas

	manipular consultas SQL		

Crear una lista de verificación (un checklist) de auditoría

- **Check 1.** Gestión de usuarios, contraseñas robustas y privilegios mínimos necesarios.

Establecer políticas de acceso seguro mediante contraseñas fuertes y asignación de permisos conforme a las funciones del usuario

Acceso no autorizado a sistemas o datos, abuso de privilegios, filtración de información.

Verificar políticas de complejidad de contraseñas y expiración. Validar que los roles tengan permisos mínimos necesarios (principio de menor privilegio). Revisar logs de inicio de sesión. Evaluar si se usa MFA.

- **Check 2.** Estrategia de respaldo y restauración de productos

Asegurar la disponibilidad e integridad de los datos relacionados con productos en caso de pérdida, corrupción o ataque.

Pérdida de información crítica de inventario o productos, impacto en la operación y ventas, fallas en recuperación.

Verificar existencia de respaldos programados (full, incremental). Probar restauración en entorno de prueba. Revisar logs de respaldo. Validar frecuencia de respaldos.

- **Check 3.** Protección de Inyección SQL

Prevenir la ejecución de comandos SQL maliciosos a través de entradas no validadas.

Exposición de datos sensibles, manipulación o borrado de información, escalada de privilegios.

Revisar el código de la aplicación para confirmar uso de sentencias preparadas / parametrizadas. Realizar pruebas de penetración (SQL Injection). Verificar filtros de validación en campos de entrada.

4. Áreas Involucradas

- **Área de Seguridad de la Información**
  Encargada de establecer políticas de seguridad, monitorear incidentes y garantizar el cumplimiento de normas como ISO 27001.
- **Área de Desarrollo o Ingeniería de Software**
  Responsable de codificar los sistemas y aplicar prácticas seguras para evitar vulnerabilidades como inyecciones SQL.
- **Área de Administración de Bases de Datos (DBA)**
  Tiene a su cargo los respaldos, la restauración, la gestión de usuarios en el motor de base de datos y la disponibilidad del servicio.

Hallazgos Preliminares:

1. Se detectaron consultas mySQL dinámicas sin sanitización en algunos módulos de la aplicación, lo cual expone el sistema a inyecciones SQL.
2. No existen evidencias de pruebas de restauración recientes en el sistema de respaldos de la base de datos.
3. Las políticas de contraseñas no exigen requisitos mínimos de complejidad ni vencimiento, y algunos usuarios tienen privilegios innecesarios.

Acciones Inmediatas

1. Implementar procedimientos de respaldo y automáticos, con almacenamiento en medios seguros.
2. Revisar y limitar los accesos administrativos a la base de datos, asignando privilegios mínimos necesarios.
3. Cambiar contraseñas de cuentas privilegiadas y aplicar reglas de complejidad básicas (8+ caracteres, símbolos, números, mayúsculas).

Acciones a Mediano Plazo

1. Establecer una política formal de respaldos y recuperación documentada, alineada con ISO/IEC 27001 y 22301.
2. Desarrollar e impartir una capacitación básica en seguridad para administradores de bases de datos y desarrolladores.
3. Implementar autenticación multifactor (MFA) para el acceso administrativo al sistema de gestión de bases de datos.

Instrumentos a utilizar en la auditoría

phpMyAdmin:

- Propósito: Administración completa de la base de datos.
- Uso:
    - Ejecutar consultas SQL: `SHOW TABLES;`, `DESCRIBE [tabla];`.
    - Exportar/importar datos (SQL/CSV).
    - Verificar relaciones entre tablas y claves foráneas.

LMap:

- Propósito: Detectar inyecciones SQL en la aplicación web.

phpMyAdmin Export/Import:

- Propósito: Generar backups manuales.
- Uso:
    - Exportar backup completo
    - Importar backup

EXPLAIN (vía phpMyAdmin):

- Propósito: Analizar consultas lentas.

SQLMap:

- Propósito: Detectar inyecciones SQL en la aplicación web.
    - Escaneo basico
    - Extraer nombres de bases de datos

Nikto

- Propósito: Detecta vulnerabilidades en servidores web vinculados a la BD.
- Uso:
    - Escaneo basico
    - Vulnerabilidades específicas