UNIVERSIDAD GERARDO BARRIOS

SEDE CENTRAL SAN MIGUEL /CENTRO REGIONAL USULUTAN

Datos Generales	
Facultad	Ciencia y Tecnología
Asignatura	Administración de base de datos II
Docente	
No. de Unidad	2
Contenido a desarrollar	Generalidades de la seguridad de los datos.

COMPETENCIAS DE LA ASIGNATURA
Crear bases de datos no relacionales y consistentes para almacenar la data empresarial aplicando la metodología del diseño, gestión de base de datos, lenguaje NoSQL y considerando las reglas de negocios desarrolladas de manera individual y colaborativa.

SEMANA 7

GENERALIDADES DE LA SEGURIDAD DE LOS DATOS

En el contexto informático, hablar sobre la seguridad de los datos se refiere a las diversas medidas que toman las organizaciones para garantizar que sus bases de datos estén protegidas de amenazas internas y externas. Esta seguridad de los datos incluye proteger la propia base de datos, los datos que contiene, su sistema de administración de bases de datos y las diversas aplicaciones que acceden a ella. En general, hoy en día las organizaciones debieran proteger las bases de datos de ataques deliberados, como amenazas a la seguridad haciendo uso de internet (ataques automatizados), así como del uso indebido de datos y bases de datos por parte de quienes pueden acceder a ellos.

En los últimos años, el número de accesos no autorizados de los datos en las empresas ha aumentado considerablemente. Además del daño inmenso que estas amenazas representan para la reputación y la base de clientes de una empresa, existe un número creciente de regulaciones y sanciones por violaciones de datos que cada país debe de trabajar, reglamentos con los cuales basarse para crear políticas internas de trabajo para protección de los datos, siendo esto el primer paso para lograr una seguridad efectiva de la base de datos, la cual es clave para seguir cumpliendo, protegiendo la reputación de las organizaciones y permitirles mantener a sus clientes.

Sobre la seguridad de los datos.

La seguridad es la protección de activos (como edificios, equipos, carga, inventario y, en algunos casos, personas) de las amenazas. La seguridad de los datos (o seguridad de la información) se ha descrito generalmente como "la protección de la información de una amplia gama de amenazas con el fin de garantizar la continuidad del negocio, minimizar riesgo empresarial y maximizar el rendimiento de las inversiones y las oportunidades de negocio", y como "el proceso porque una organización protege y asegura los sistemas, medios e instalaciones que procesan y mantienen información vital para sus operaciones ".

Riesgos de privacidad y seguridad de datos.

Descuidar la privacidad y la protección de los datos puede traer consecuencias adversas que son importantes, tales como:

- Sanciones civiles y penales impuestas por los gobiernos, incluidas multas y sanciones.
- Importantes multas e indemnizaciones por daños resultantes de demandas privadas, incluidas las acciones colectivas (permitidas en algunas leyes de privacidad y seguridad de datos, esto a partir de la legislación en este aspecto que tengan los países).
- Daño a la reputación de la empresa y la pérdida de la confianza de los clientes, lo que resulta en la pérdida de ventas, participación de mercado y valor de marca y accionistas.

> **Nota**: Es importante recalcar que los riesgos no pueden ser totalmente eliminados, pero es crítico demostrar que se implementan buenas prácticas y que además sean razonables, para poder reducir a un nivel aceptable esos riesgos.

Seguridad de la base de datos.

En cuanto a la seguridad de la base de datos, se refiere al conjunto de estándares y tecnologías, que proveen de una gama de herramientas, controles y medidas diseñadas para establecer y preservar la confidencialidad, integridad y disponibilidad de la base de datos. Siendo la intención que las empresas siempre consideren a este elemento, como el que continuamente se verá comprometido en la mayoría de las filtraciones de datos y, por lo tanto, deberá ser protegido de la destrucción, modificación o divulgación intencional o accidental.

La seguridad de los datos, aborda y protege lo siguiente:

- Los datos en la base de datos.
- El sistema de gestión de bases de datos (DBMS).
- Cualquier aplicación asociada a esta.

- El servidor de base de datos físico y/o el servidor de base de datos virtual y el hardware subyacente.
- La infraestructura de red utilizada para acceder a la base de datos.

Procurar la seguridad de la base de datos es un esfuerzo complejo y desafiante que involucra todos los aspectos de las tecnologías y prácticas de seguridad de la información, y no termina ahí, pues debe de haber un constante monitoreo y actualización de los recursos informáticos y también, se considerará la usabilidad de la base de datos. Cuanto más accesible y utilizable sea la base de datos, más vulnerable será a las amenazas a la seguridad; cuanto más invulnerable es la base de datos a las amenazas, más difícil es de acceder y utilizar. (Esta paradoja se conoce como regla de Anderson en informática).

Importancia de la seguridad de los datos.

Una violación de datos es una falla en mantener la confidencialidad de la información en una base de datos. El daño que inflige a una empresa, depende de una serie de consecuencias o factores:

- **Propiedad intelectual comprometida**: la propiedad intelectual (secretos comerciales, invenciones, prácticas patentadas) puede ser fundamental por la capacidad de mantener una ventaja competitiva en el mercado. Si esa propiedad intelectual es robada o expuesta, su ventaja competitiva puede ser difícil o imposible de mantener o recuperar.
- **Daño a la reputación de la marca**: los clientes o socios pueden no estar dispuestos a comprar productos o servicios (o hacer negocios con una empresa), si no sienten que pueden confiar para proteger sus datos o los de ellos. Una encuesta Harris Poll de 2018 patrocinada por IBM a adultos mayores de 18 años, reveló que el 63% califica la calidad de la protección de datos contra los ciberataques como "extremadamente importante" en la decisión de compra de una empresa.
- **Continuidad del negocio** (o falta de ella): algunos negocios no pueden seguir funcionando hasta que se resuelva una infracción.
- **Multas o sanciones por incumplimiento**: el impacto financiero por no cumplir con las regulaciones globales, así como regulaciones locales, pueden ser devastadoras, con imposición de multas por violación.

- **Costos de reparar infracciones y notificar a los clientes**: además del costo de comunicar una infracción al cliente, una organización violada debe pagar las actividades de informática forense y de investigación, la gestión de crisis, la clasificación, la reparación de los sistemas afectados y otros.

Amenazas y desafíos comunes.

Muchos de los problemas que recaen en la inseguridad de los datos, pueden ser por alguna de las causas siguientes:

1. **Amenazas internas**. es una amenaza a la seguridad de cualquiera de las tres fuentes con acceso privilegiado a la base de datos:

    - Infiltración malintencionada que tiene la intención de hacer daño.
    - Un informante negligente que comete errores que hacen que la base de datos sea vulnerable a ataques.
    - Un infiltrado: un forastero que de alguna manera obtiene credenciales a través de un esquema como el phishing o al obtener las credenciales de acceso a la base de datos.

    Las amenazas internas se encuentran entre las causas más comunes de violaciones de la seguridad de las bases de datos y, a menudo, son el resultado de permitir que demasiados empleados tengan credenciales de acceso de usuario privilegiado.

2. **Error humano**.

    Aquí caben los accidentes, las contraseñas débiles, el uso compartido de contraseñas y otros comportamientos de usuarios imprudentes o desinformados. Estos continúan siendo la causa de casi la mitad de todas las filtraciones de datos.

3. **Vulnerabilidades de las bases de datos**.

    Nunca se debe perder de vista que los piratas informáticos, buscan o apuntan a las vulnerabilidades de software, el cual incluye indudablemente las bases de datos. Es por ello que todos los proveedores de bases de datos comerciales y plataformas de bases de datos de código abierto, emiten parches de seguridad regulares para

abordar estas vulnerabilidades, aunque en oportunidades dichos parches no son aplicados de forma oportuna.

4. **Explotaciones de desbordamiento de búfer.**

   El desbordamiento de búfer se produce cuando un proceso intenta escribir más datos en un bloque de memoria de longitud fija de los que puede contener. Los atacantes pueden utilizar el exceso de datos, almacenados en direcciones de memoria adyacentes, como base desde la cual lanzar ataques.

5. **Software malicioso.**

   El malware es software escrito específicamente para explotar vulnerabilidades o causar daños a la base de datos. El malware puede llegar a través de cualquier dispositivo terminal que se conecte a la red de la base de datos.

6. **Ataques de denegación de servicio (DoS / DDoS).**

   En un ataque de denegación de servicio (DoS), el atacante inunda el servidor de destino, en este caso el servidor de la base de datos, con tantas solicitudes que el servidor ya no puede satisfacer las solicitudes legítimas de los usuarios reales y, en muchos casos, el servidor se convierte en inestable o se bloquea.

   En un ataque distribuido de denegación de servicio (DDoS), el diluvio proviene de varios servidores, lo que dificulta la detención del ataque.

7. **Ataques de inyección SQL / NoSQL.**

   Una amenaza específica de la base de datos y que ocupa los primeros lugares entre las amenazas más frecuentes, implica la inserción de cadenas de ataque arbitrarias SQL o no SQL en consultas de base de datos servidas por aplicaciones web o encabezados HTTP. Las organizaciones que no siguen las prácticas de codificación de aplicaciones web seguras y realizan pruebas de vulnerabilidad periódicas están abiertas a estos ataques.

8. **Riesgos a las copias de seguridad.**

   Las organizaciones que no protegen los datos de respaldo con los mismos controles estrictos que se utilizan para proteger la base de datos en sí, pueden ser vulnerables a los ataques a los respaldos.

   Cuando estas amenazas se ven agravadas:

   - No hay un control sobre el volumen de los datos de la empresa. Si esto sucede, el área de TI de la empresa debe implementar prácticas de seguridad o herramientas que permitan ser altamente escalable para satisfacer las necesidades en cualquier momento actual o futuro.

   - Expansión de la infraestructura. Los entornos de red se vuelven cada vez más complejos dentro de las compañías, debido a que las cargas de trabajo aumentan y son trasladas a la nube y esto hace que aplicar soluciones de seguridad sea talvez no imposible pero sí desafiante.

   - Requisitos normativos mundiales que hay que cumplir, más las legislaciones locales.

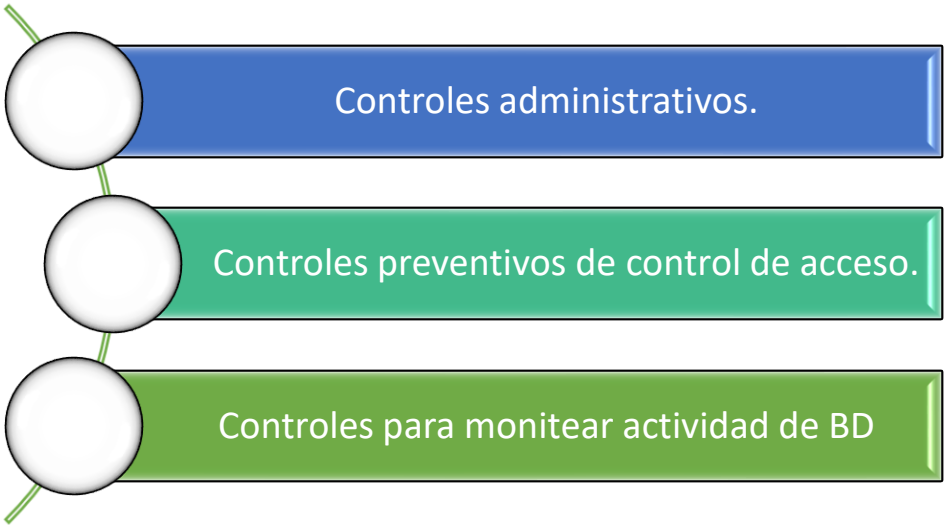
   - Escases de habilidades de seguridad y ciberseguridad.

Mejores prácticas.

Como las bases de datos son casi siempre accesibles desde la red, cualquier amenaza a la seguridad de cualquier componente dentro o parte de la infraestructura de la red también es una amenaza para la base de datos, y cualquier ataque que afecte el dispositivo o la estación de trabajo (PC) de un usuario puede amenazar la base de datos. Por lo tanto, la seguridad de la base de datos debe extenderse mucho más allá de los límites de la base de datos únicamente.

Políticas y controles.

No solo es de implementar controles de seguridad en capas en todo el entorno de red, la seguridad de la base de datos requiere que se establezcan los controles y políticas correctos para acceder a la base de datos en sí. Éstas incluyen:



- Controles administrativos para regular la instalación, los cambios y la gestión de la configuración de la base de datos.
- Controles preventivos para controlar el acceso, el cifrado, el enmascaramiento y otros.
- Controles para monitorear la actividad de la base de datos y las herramientas de prevención de pérdida de datos. Estas soluciones permiten identificar y alertar sobre actividades sospechosas.

ACTIVIDAD DE EVALUACIÓN DE LA SEMANA	
Nombre de la Actividad	Lista de comprobación de seguridad de datos.
Tipo de Actividad	Buzón
Tipo de Participación	Colaborativo (3 estudiantes)
Competencia especifica de la asignatura	Crear bases de datos no relacionales y consistentes para almacenar la data empresarial aplicando la metodología del diseño, gestión de base de datos, lenguaje NoSQL y considerando las reglas de negocios desarrolladas de manera individual y colaborativa.
Instrucciones para la actividad	Luego de haber dado lectura al contenido correspondiente a esta semana, cada equipo deberá trabajar en establecer una lista de verificación que garantice que los datos de una tienda en línea, permanezcan protegidos. Esa lista deberá de incluir aspectos tales como: • Seguridad con respecto al almacenamiento, actualizaciones y los respaldos de información. • Encriptamiento, ya que los métodos de pago manejan tarjetas de crédito y débito, y la información no debiera poder leerse mientras se dirige a su destino. • Usuarios y privilegios en las bases de datos, entre otros. • Y, por último, deberán proponer al menos un programa que permita encontrar problemas de seguridad en la configuración y se obtenga recomendaciones de cómo corregirlos. > **BONUS**: Punto extra por comprobar el funcionamiento del programa propuesto. Al finalizar, deberá enviar su respuesta en un documento en Word, fuente Arial, tamaño de fuente 12, interlineado 1.15. Guarde la tarea con el nombre **Unidad 2- Actividad 1- Lista de comprobación de seguridad de datos** y envíela al espacio correspondiente.

Fecha de Entrega	La fecha límite de participación será el domingo al finalizar la semana , a las 11:55 pm
Instrumento de evaluación	Rúbrica
Ponderación	Evaluación formativa

RECURSOS COMPLEMENTARIOS		
Recurso	**Título**	**Cita referencial**
Sitio Web	**Seguridad de la base de datos - Database security Seguridad de la base de datos**	(Wiki, 2020)
Video	**Fundamentos de la vulneración de seguridad de datos**	(HTML Rules, 2020)
Sitio Web	**La importancia de la seguridad e integridad en base de datos**	(PowerData, 2017)

Rubrica de evaluación

CRITERIOS	**EXCELENTE 10.0 puntos**	**MUY BUENO 8.0 puntos**	**BUENO 6.0 puntos**	**NECESITA MEJORAR 4.0 puntos**	**REPROBADO 0.0 Puntos**
Puntualidad **(2.0 puntos)**	Entrega de tarea en la fecha y hora límite indicada.	Entrega de tarea 6 horas después de la fecha indicada con justificación.	Entrega de tarea un día después de la fecha y hora indicada con previa justificación.	Entrega de tarea dos días después de la fecha indicada sin justificación de fuerza mayor.	No se realizó el envío de la actividad.
Asistencia y participación en video conferencia **(2.0 puntos)**	Asiste puntualmente y participa activamente en la video conferencia	Asiste de forma impuntual a la videoconferencia, pero participa activamente	Asiste de forma impuntual a la videoconferencia, pero tiene poca participación	Asiste de forma impuntual a la videoconferencia, y no participa	No asiste a la video conferencia
Lógica en la resolución del problema **(4.0 puntos)**	La solución planteada tiene un propósito y un tema claros bien planteados y son consistentes.	La solución planteada tiene un propósito y un tema claros, pero tiene uno o dos elementos que no están relacionados.	El propósito y el tema son de alguna forma confusos o imprecisos.	La solución carece de propósito.	No se realiza la entrega
Seguimiento de instrucciones **(2.0 puntos)**	Toda la información provista es precisa y de acuerdo los requisitos de la asignación han sido cumplidos.	Casi toda la información provista es precisa y de acuerdo los requisitos de la asignación han sido cumplidos.	Casi toda la información provista es precisa y de acuerdo con algunos requisitos de la asignación han sido cumplidos.	Hay varias inexactitudes en el contenido provisto o muchos de los requisitos no están cumplidos.	No realiza entrega de tarea
Puntaje final					