Ética

Preguntas:

Basándose en los requerimientos funcionales del proyecto y aplicando la legislación

revisada en la cursada:

1. · Describir cómo el grupo se conforma como instrumento legal (Empresa, Socios, CEO,Empleados) y si tendrán un contrato con qué cláusulas.
2. · Describir quiénes y ante quien deben matricularse a nivel provincial para ejercer la Profesión.
3. · Describir que requerimientos deben cumplir el código programado y las bases de datos según la legislación vigente
4. · Enumerar los pasos para que ARGBroker sea parte del Registro Nacional de software.
5. · Si un integrante del grupo no realiza el trámite de matriculación, que pena le corresponde a nivel provincial.
6. · Si el código es replicado, describir como la Ley de Propiedad Intelectual puede salvaguardar a ARGBroker.
7. · Si un integrante del grupo divulga los datos de la base de datos interna, describir como legalmente deberían accionar los demás.
8. · Si otro integrante del grupo reutiliza el código para fines personales, describir como legalmente deberían accionar los demás según la Legislación de la Provincia de Córdoba y el Código Penal Argentino.
9. · Si otro integrante del grupo reutiliza el código para fines personales a nivel nternacional, describir qué instrumento legal respalda a ARGBroker.
10. · Si la base de datos es adulterada de manera externa, a nivel nacional, describir qué instrumento legal respalda a ARGBroker.
11. · Si los datos de la base de datos son adulterados de manera externa, a nivel internacional, describir qué instrumento legal respalda a ARGBroker.
12. · Cuando los programadores de ARGBroker incurren en una negligencia, a que instrumento legal se acude y quien.
13. · Cómo ARGBroker debe implementar seguridad según la Ley de Protección de Datos Personales.
14. · Si el cliente decide reemplazar a ARGBroker por otro proveedor, describir cómo se debe actuar de manera ética ante el cliente y los colegas.

15. · Si un usuario denuncia a ARGBroker por divulgación de sus datos personales, a que legislación recurrió el mismo y como ARGBroker puede respaldarse jurídicamente.

Respuestas:

1- · **Describir cómo el grupo se conforma como instrumento legal (Empresa, Socios, CEO,**

Empleados) y si tendrán un contrato con que cláusulas.

Conformación de la Empresa

1. **Tipo de Empresa: Sociedad Anónima (S.A.)**

- **Fundación:** Debe estar inscripta en el Registro Público de Comercio
- **Capital Social:** Capital Social Mínimo, dividido en acciones
- **Accionistas:** Al menos dos
- **Órganos de Gobierno**

2. **Socios y participaciones:**
    - **Distribución de Acciones**
    - **Derechos y Obligaciones**

3. **CEO y Empleados:**
    - **Nombramiento del CEO:** El Directorio designa al CEO, quien es responsable de la gestión operativa.
    - **Empleados:** Se contratan empleados según las necesidades del proyecto, cumpliendo con las normativas laborales argentinas (Ley de Contrato de Trabajo 20.744).

Contratos y Cláusulas

se establecerán contratos con las siguientes cláusulas:

4. **Contrato de Desarrollo de Software:**

- **Partes:** ISPC Cba (el desarrollador) y el Cliente (empresa que solicita el desarrollo).
- **Objeto:** Desarrollo de una aplicación demo para la compra y venta de acciones en la Bolsa de Valores de Buenos Aires.
- **Plazo:** Período de desarrollo y entrega del software.
- **Precio y Pagos**
- **Propiedad Intelectual:** La propiedad del software desarrollado pertenecerá a ISPC Cba.
- **Confidencialidad:** Obligación de mantener confidencial la información sensible.
- **Soporte y Mantenimiento:** Detalles sobre el soporte técnico y mantenimiento post-implementación.

5. **Contrato de Trabajo para Empleados:**
   - **Partes:** ISPC Cba y el empleado.
   - **Objeto:** Términos y condiciones del empleo.
   - **Duración:** Indefinida o determinada.
   - **Remuneración:** Salario y otros.
   - **Horario de Trabajo**
   - **Confidencialidad:** Protección de la información confidencial de la empresa.
   - **Propiedad Intelectual:** Cesión de derechos sobre el trabajo realizado durante el empleo.
6. **Contrato con el CEO:**
   - **Partes:** ISPC Cba y el CEO.
   - **Objeto:** Nombramiento y responsabilidades del CEO.
   - **Duración:** Plazo del contrato.
   - **Remuneración:** Salario y otros.
   - **Obligaciones:** Responsabilidades y deberes del CEO.

- **Confidencialidad y No Competencia:** Cláusulas para proteger los intereses de la empresa.

2. · **Describir quiénes y ante quien deben matricularse a nivel provincial para ejercer la Profesión.**

Para ejercer como profesionales los integrantes del grupo deberán matricularse en el colegio profesional de Ciencias Informáticas de Córdoba (CPCIPC)

3. · **Describir que requerimientos deben cumplir el código programado y las bases de datos según la legislación vigente**

1. Protección de Derechos de Autor

Ley N.º 11.723 de Propiedad Intelectual:

- **Registro del Software**: El código del programa debe ser registrado en la Dirección Nacional del Derecho de Autor (DNDA). Este registro proporciona una protección formal y facilita la defensa en casos de infracción.
- **Documentación**: Es necesario presentar la documentación técnica del software, incluyendo descripciones funcionales y técnicas, diagramas de flujo, y cualquier otra documentación que describa el funcionamiento y las características del software.
- **Declaración de Autoría**: Debe incluirse una declaración que identifique claramente a los autores y titulares de los derechos del software.

2. Protección de Datos Personales

Ley N.º 25.326 de Protección de Datos Personales:

- **Consentimiento**: La recopilación y el tratamiento de datos personales deben realizarse con el consentimiento explícito de los titulares de esos datos.
- **Finalidad**: Los datos deben ser recopilados para finalidades determinadas, explícitas y legítimas, y no pueden ser tratados de manera incompatible con dichas finalidades.
- **Seguridad**: Se deben implementar medidas de seguridad adecuadas para proteger los datos personales contra el acceso, la modificación o la destrucción no autorizados. Esto incluye tanto medidas técnicas (cifrado, control de acceso, etc.) como organizativas (políticas de privacidad, capacitaciones, etc.).
- **Derechos de los Titulares**: Se debe garantizar a los titulares de los datos el acceso, rectificación, actualización y, cuando corresponda, supresión de sus datos personales.

3. Seguridad Informática

Normativas sobre Ciberseguridad:

- **Seguridad de la Información**: Los sistemas y bases de datos deben cumplir con las buenas prácticas de seguridad de la información, como las establecidas por normas ISO/IEC 27001.
- **Auditorías y Controles**: Realizar auditorías periódicas de seguridad para identificar y corregir vulnerabilidades.
- **Registro de Actividades**: Mantener registros detallados de las actividades de acceso y modificaciones en las bases de datos para permitir la detección de incidentes de seguridad.

4. Requisitos Técnicos Específicos

Código Programado:

- **Estandarización y Documentación**: El código debe seguir estándares de codificación reconocidos y debe estar bien documentado para garantizar la mantenibilidad y la claridad.
- **Licencias de Terceros**: Si el software utiliza bibliotecas o componentes de terceros, se deben respetar las licencias correspondientes, asegurando que su uso sea legal y compatible con la distribución del software.
- **Compatibilidad y Accesibilidad**: Asegurar que el software sea compatible con los entornos operativos para los cuales fue diseñado y que cumpla con normas de accesibilidad, si corresponde.

Bases de Datos:

- **Integridad y Exactitud**: Implementar mecanismos que aseguren la integridad y exactitud de los datos almacenados.
- **Respaldo y Recuperación**: Contar con políticas y procedimientos de respaldo y recuperación de datos para prevenir la pérdida de información.

Acceso Controlado: Implementar controles de acceso estrictos para asegurar que solo personal autorizado pueda acceder a los datos sensibles

4. · Describir que requerimientos deben cumplir el código programado y las bases de datos según la legislación vigente

1. Protección de Derechos de Autor

Ley N.º 11.723 de Propiedad Intelectual:

- **Registro del Software**: El código del programa debe ser registrado en la Dirección Nacional del Derecho de Autor (DNDA). Este registro proporciona una protección formal y facilita la defensa en casos de infracción.
- **Documentación**: Es necesario presentar la documentación técnica del software, incluyendo descripciones funcionales y técnicas, diagramas de flujo, y cualquier otra documentación que describa el funcionamiento y las características del software.
- **Declaración de Autoría**: Debe incluirse una declaración que identifique claramente a los autores y titulares de los derechos del software.

2. Protección de Datos Personales

Ley N.º 25.326 de Protección de Datos Personales:

- **Consentimiento**: La recopilación y el tratamiento de datos personales deben realizarse con el consentimiento explícito de los titulares de esos datos.
- **Finalidad**: Los datos deben ser recopilados para finalidades determinadas, explícitas y legítimas, y no pueden ser tratados de manera incompatible con dichas finalidades.
- **Seguridad**: Se deben implementar medidas de seguridad adecuadas para proteger los datos personales contra el acceso, la modificación o la destrucción no autorizados. Esto incluye tanto medidas técnicas (cifrado, control de acceso, etc.) como organizativas (políticas de privacidad, capacitaciones, etc.).
- **Derechos de los Titulares**: Se debe garantizar a los titulares de los datos el acceso, rectificación, actualización y, cuando corresponda, supresión de sus datos personales.

3. Seguridad Informática

Normativas sobre Ciberseguridad:

- **Seguridad de la Información**: Los sistemas y bases de datos deben cumplir con las buenas prácticas de seguridad de la información, como las establecidas por normas ISO/IEC 27001.
- **Auditorías y Controles**: Realizar auditorías periódicas de seguridad para identificar y corregir vulnerabilidades.
- **Registro de Actividades**: Mantener registros detallados de las actividades de acceso y modificaciones en las bases de datos para permitir la detección de incidentes de seguridad.

4. Requisitos Técnicos Específicos

Código Programado:

- **Estandarización y Documentación**: El código debe seguir estándares de codificación reconocidos y debe estar bien documentado para garantizar la mantenibilidad y la claridad.
- **Licencias de Terceros**: Si el software utiliza bibliotecas o componentes de terceros, se deben respetar las licencias correspondientes, asegurando que su uso sea legal y compatible con la distribución del software.
- **Compatibilidad y Accesibilidad**: Asegurar que el software sea compatible con los entornos operativos para los cuales fue diseñado y que cumpla con normas de accesibilidad, si corresponde.

Bases de Datos:

- **Integridad y Exactitud**: Implementar mecanismos que aseguren la integridad y exactitud de los datos almacenados.
- **Respaldo y Recuperación**: Contar con políticas y procedimientos de respaldo y recuperación de datos para prevenir la pérdida de información.

Acceso Controlado: Implementar controles de acceso estrictos para asegurar que solo personal autorizado pueda acceder a los datos sensibles

5. · Describir que requerimientos deben cumplir el código programado y las bases de datos según la legislación vigente

1. Protección de Derechos de Autor

Ley N.º 11.723 de Propiedad Intelectual:

- **Registro del Software**: El código del programa debe ser registrado en la Dirección Nacional del Derecho de Autor (DNDA). Este registro proporciona una protección formal y facilita la defensa en casos de infracción.
- **Documentación**: Es necesario presentar la documentación técnica del software, incluyendo descripciones funcionales y técnicas, diagramas de flujo, y cualquier otra documentación que describa el funcionamiento y las características del software.
- **Declaración de Autoría**: Debe incluirse una declaración que identifique claramente a los autores y titulares de los derechos del software.

2. Protección de Datos Personales

Ley N.º 25.326 de Protección de Datos Personales:

- **Consentimiento**: La recopilación y el tratamiento de datos personales deben realizarse con el consentimiento explícito de los titulares de esos datos.
- **Finalidad**: Los datos deben ser recopilados para finalidades determinadas, explícitas y legítimas, y no pueden ser tratados de manera incompatible con dichas finalidades.

- **Seguridad**: Se deben implementar medidas de seguridad adecuadas para proteger los datos personales contra el acceso, la modificación o la destrucción no autorizados. Esto incluye tanto medidas técnicas (cifrado, control de acceso, etc.) como organizativas (políticas de privacidad, capacitaciones, etc.).
- **Derechos de los Titulares**: Se debe garantizar a los titulares de los datos el acceso, rectificación, actualización y, cuando corresponda, supresión de sus datos personales.

3. Seguridad Informática

Normativas sobre Ciberseguridad:

- **Seguridad de la Información**: Los sistemas y bases de datos deben cumplir con las buenas prácticas de seguridad de la información, como las establecidas por normas ISO/IEC 27001.
- **Auditorías y Controles**: Realizar auditorías periódicas de seguridad para identificar y corregir vulnerabilidades.
- **Registro de Actividades**: Mantener registros detallados de las actividades de acceso y modificaciones en las bases de datos para permitir la detección de incidentes de seguridad.

4. Requisitos Técnicos Específicos

Código Programado:

- **Estandarización y Documentación**: El código debe seguir estándares de codificación reconocidos y debe estar bien documentado para garantizar la mantenibilidad y la claridad.
- **Licencias de Terceros**: Si el software utiliza bibliotecas o componentes de terceros, se deben respetar las licencias correspondientes, asegurando que su uso sea legal y compatible con la distribución del software.
- **Compatibilidad y Accesibilidad**: Asegurar que el software sea compatible con los entornos operativos para los cuales fue diseñado y que cumpla con normas de accesibilidad, si corresponde.

Bases de Datos:

- **Integridad y Exactitud**: Implementar mecanismos que aseguren la integridad y exactitud de los datos almacenados.
- **Respaldo y Recuperación**: Contar con políticas y procedimientos de respaldo y recuperación de datos para prevenir la pérdida de información.

Acceso Controlado: Implementar controles de acceso estrictos para asegurar que solo personal autorizado pueda acceder a los datos sensibles

6. · Describir que requerimientos deben cumplir el código programado y las bases de datos según la legislación vigente

1. Protección de Derechos de Autor

Ley N.º 11.723 de Propiedad Intelectual:

- **Registro del Software**: El código del programa debe ser registrado en la Dirección Nacional del Derecho de Autor (DNDA). Este registro proporciona una protección formal y facilita la defensa en casos de infracción.
- **Documentación**: Es necesario presentar la documentación técnica del software, incluyendo descripciones funcionales y técnicas, diagramas de flujo, y cualquier otra documentación que describa el funcionamiento y las características del software.

- **Declaración de Autoría**: Debe incluirse una declaración que identifique claramente a los autores y titulares de los derechos del software.

2. Protección de Datos Personales

Ley N.º 25.326 de Protección de Datos Personales:

- **Consentimiento**: La recopilación y el tratamiento de datos personales deben realizarse con el consentimiento explícito de los titulares de esos datos.
- **Finalidad**: Los datos deben ser recopilados para finalidades determinadas, explícitas y legítimas, y no pueden ser tratados de manera incompatible con dichas finalidades.
- **Seguridad**: Se deben implementar medidas de seguridad adecuadas para proteger los datos personales contra el acceso, la modificación o la destrucción no autorizados. Esto incluye tanto medidas técnicas (cifrado, control de acceso, etc.) como organizativas (políticas de privacidad, capacitaciones, etc.).
- **Derechos de los Titulares**: Se debe garantizar a los titulares de los datos el acceso, rectificación, actualización y, cuando corresponda, supresión de sus datos personales.

3. Seguridad Informática

Normativas sobre Ciberseguridad:

- **Seguridad de la Información**: Los sistemas y bases de datos deben cumplir con las buenas prácticas de seguridad de la información, como las establecidas por normas ISO/IEC 27001.
- **Auditorías y Controles**: Realizar auditorías periódicas de seguridad para identificar y corregir vulnerabilidades.
- **Registro de Actividades**: Mantener registros detallados de las actividades de acceso y modificaciones en las bases de datos para permitir la detección de incidentes de seguridad.

4. Requisitos Técnicos Específicos

Código Programado:

- **Estandarización y Documentación**: El código debe seguir estándares de codificación reconocidos y debe estar bien documentado para garantizar la mantenibilidad y la claridad.
- **Licencias de Terceros**: Si el software utiliza bibliotecas o componentes de terceros, se deben respetar las licencias correspondientes, asegurando que su uso sea legal y compatible con la distribución del software.
- **Compatibilidad y Accesibilidad**: Asegurar que el software sea compatible con los entornos operativos para los cuales fue diseñado y que cumpla con normas de accesibilidad, si corresponde.

Bases de Datos:

- **Integridad y Exactitud**: Implementar mecanismos que aseguren la integridad y exactitud de los datos almacenados.
- **Respaldo y Recuperación**: Contar con políticas y procedimientos de respaldo y recuperación de datos para prevenir la pérdida de información.

Acceso Controlado: Implementar controles de acceso estrictos para asegurar que solo personal autorizado pueda acceder a los datos sensibles

7. · **Si el código es replicado, describir como la Ley de Propiedad Intelectual puede salvaguardar a ARGBroker.**

La Ley de Propiedad Intelectual de Argentina nos ofrece múltiples mecanismos para proteger el software ARGBroker contra la replicación no autorizada:

7. **Registro en la DNDA**: Proporciona evidencia de autoría y fecha de creación.
8. **Derechos Morales y Patrimoniales**: Protegen la autoría y controlan la reproducción y modificación del software.
9. **Acciones Legales**: Permiten demandas civiles y penales contra los infractores.
10. **Medidas Cautelares**: Ofrecen soluciones rápidas para detener la infracción.
11. **Prevención Proactiva**: Uso de licencias y medidas técnicas para proteger el software.

8. **Si un integrante del grupo divulga los datos de la base de datos interna, describir como legalmente deberían accionar los demás.**

Si un integrante del grupo divulga los datos de la base de datos interna, legalmente los demás integrantes deberían accionar solicitando la aplicación de las medidas disciplinarias correspondientes según las políticas de confidencialidad y seguridad de la empresa. Además, en caso de una violación que comprometa la privacidad o seguridad de los datos, se podría recurrir al marco legal argentino relacionado con la protección de datos personales como la Ley de Protección de Datos Personales (Ley 25.326) para tomar las medidas legales necesarias contra el infractor.

9. **Si otro integrante del grupo reutiliza el código para fines personales, describir como legalmente deberían accionar los demás según la Legislación de la Provincia de Córdoba y el Código Penal Argentino.**

En caso de que un integrante del grupo use el código sin autorización será considerado una infracción grave y se procederá de acuerdo con la legislación de la provincia de Córdoba y el código Penal Argentino

10. **Si otro integrante del grupo reutiliza el código para fines personales a nivel internacional, describir qué instrumento legal respalda a ARGBroker.**

En caso de que algún integrante reutilice el código a nivel internacional el grupo actuara de acuerdo a lo que dice el Articulo 10 – “Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afine” descripto en el Convenio de Berna

11. **Si la base de datos es adulterada de manera externa, a nivel nacional, describir qué instrumento legal respalda a ARGBroker.**

En caso de ser adulterada a nivel nacional el grupo se respaldará de manera legar en la Ley de Protección de Datos Personales (Ley 25.326), en el código Penal argentino(Articulo 183, 184 y 173), Ley de Delitos Informáticos (Ley 26.388), Ley de Delitos Informáticos (Ley 26.388), y en la ley de Firma Digital(Ley 25.506)

12. **Si la base de datos es adulterada de manera externa, a nivel nacional, describir qué instrumento legal respalda a ARGBroker.**

En caso de ser adulterada a nivel nacional el grupo se respaldará de manera legar en la Ley de Protección de Datos Personales (Ley 25.326), en el código Penal argentino(Articulo 183, 184 y 173), Ley de Delitos Informáticos (Ley 26.388), Ley de Delitos Informáticos (Ley 26.388), y en la ley de Firma Digital(Ley 25.506)

13. ¿Cuándo los programadores de ARGBroker incurren en una negligencia, a qué instrumento legal se acude y quién?

Respuesta: En caso de negligencia de los programadores de ARGBroker, se acude al **Código Civil y Comercial de la Nación Argentina**. Según este código, la negligencia o la falta de diligencia adecuada en el desarrollo de software podría considerarse una falta en el cumplimiento de las obligaciones contractuales o extracontractuales, dependiendo del contexto. Las personas afectadas por esta negligencia pueden iniciar acciones legales en base a este código para reclamar daños y perjuicios.

14. **¿Cómo ARGBroker debe implementar seguridad según la Ley de Protección de Datos Personales?**

Respuesta: ARGBroker debe implementar medidas de seguridad según la **Ley de Protección de Datos Personales N° 25.326**. Esta ley establece que los responsables de bases de datos deben adoptar medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos personales. Estas medidas incluyen:

- **Control de acceso:** Asegurar que solo el personal autorizado tenga acceso a los datos personales.
- **Cifrado de datos:** Implementar cifrado para la transmisión y almacenamiento de datos sensibles.
- **Auditorías y monitoreo:** Realizar auditorías regulares y monitorear los sistemas para detectar y prevenir accesos no autorizados.
- **Formación:** Capacitar al personal sobre las políticas de seguridad y protección de datos.

15. **Si el cliente decide reemplazar a ARGBroker por otro proveedor, describir cómo se debe actuar de manera ética ante el cliente y los colegas.**

Respuesta: Al reemplazar a ARGBroker por otro proveedor, se debe actuar éticamente siguiendo estos principios:

- **Transparencia:** Informar al cliente de manera clara y honesta sobre el proceso de transición y cualquier posible impacto.
- **Cooperación:** Colaborar con el nuevo proveedor para asegurar una transición fluida y sin problemas para el cliente.
- **Confidencialidad:** Mantener la confidencialidad de los datos e información del cliente durante y después de la transición.
- **Respeto:** Tratar a todos los involucrados, incluyendo el nuevo proveedor y el personal de ARGBroker, con respeto y profesionalismo.
- **Documentación:** Proporcionar toda la documentación necesaria y relevante para que el nuevo proveedor pueda continuar con el servicio sin interrupciones.

16. **Si un usuario denuncia a ARGBroker por divulgación de sus datos personales, ¿a qué legislación recurrió el mismo y cómo ARGBroker puede respaldarse jurídicamente?**

Respuesta: Un usuario que denuncia a ARGBroker por divulgación de sus datos personales recurre a la **Ley de Protección de Datos Personales N° 25.326**. Esta ley protege los datos personales y establece derechos para los titulares de los datos, así como obligaciones para los responsables de su tratamiento.

Cómo ARGBroker puede respaldarse jurídicamente:

- **Cumplimiento de la ley:** Demostrar que ha cumplido con todas las obligaciones establecidas en la Ley de Protección de Datos Personales, incluyendo la implementación de medidas de seguridad adecuadas.
- **Consentimiento:** Probar que obtuvo el consentimiento del usuario para el tratamiento y la divulgación de los datos personales.

- **Políticas de privacidad:** Presentar las políticas de privacidad y protección de datos que han sido implementadas y comunicadas a los usuarios.
- **Registro de actividades:** Mantener un registro detallado de las actividades de tratamiento de datos y de las medidas de seguridad adoptadas.