Fundamentos de Ciencia de Datos

PEC2: Los peligros de no gobernar los datos: calidad, seguridad y ética

Criterios de evaluación generales de la PEC.

- Demostrar que se han asimilado correctamente los contenidos teóricos y que se aplican con precisión.
- Razonar todas las respuestas de forma analítica y sintética.
- Estructurar y maquetar correctamente el documento.
- Esquematizar las respuestas mediante el uso de gráficos, infografías y diagramas explicativos.
- Utilizar con precisión las citas y las referencias bibliográficas. No se aceptarán copias textuales de la teoría ni de otras fuentes.
- Ajustar la extensión del documento a un máximo de 20 páginas.

José Alonso Ayllón Gutiérrez

Contexto

Te recordamos el caso de la PEC1:

En 2019 la compañía HM Hospitales inició un plan de transformación digital que también ha supuesto un cambio cultural. En 2020 puso en marcha la iniciativa Covid data save lives, poniendo a disposición de la comunidad científica la información clínica de pacientes atendidos durante la pandemia.

Para esta PEC, vamos a seguir el mismo caso, y la misma metodología: argumenta las respuestas en base a la teoría del bloque 2 y a la información adicional que encuentres referente al caso y los enlaces que te proporcionamos.

Pregunta 1 (30% puntuación)

En la transformación digital de HM Hospitales, además de los cambios tecnológicos, se dieron fundamentalmente cambios culturales. Entre ellos, el gobierno del dato seguramente fue decisivo. Sitúate en el rol del CDO y a partir de ahí, imagina y describe:

- ¿Cómo divulgarías internamente qué es el gobierno del dato en una HM Hospitales y su importancia en la transformación digital?
- Si te basaras en DAMA, ¿qué objetivos principales perseguirías sobre los datos?
- ¿Cuál sería tu planteamiento para la consecución de estos objetivos, en función de las fases que tendrías que implementar para el gobierno del dato?

Antes de empezar, es conveniente establecer qué entendemos por **gobierno de datos** (o **data gorvernace**). Son muchas las posibles definiciones de este concepto, pero la más extendida es la dada por **DAMA**[1], "el ejercicio de autoridad, control y toma de decisiones compartida (planificación, vigilancia y aplicación) sobre la gestión de los activos de datos".

El **CDO** (Chief Data Officier o Director de Datos) tiene por misión **gestionar los datos** y la información como un **activo** de la corporación. Es fundamental que el CDO conozca y entienda las necesidades de la empresa, y disponga de las cualidades necesarias para desarrollar en la empresa el **gobierno de los datos**.

Siendo muchos los retos a los que se enfrenta el CDO, es crucial impulsar la cultura de los datos como un activo estratégico, por lo que debe fomentar y transmitir la importancia del gobierno de los datos en el presente y futuro del negocio.

Para una compañía que quiere una auténtica transformación digital, y convertirse en una empresa orientada al dato, es fundamental disponer del rol del CDO, y que quien lo desempeñe forme parte

de la dirección de la empresa, con competencia en el mando y toma de decisiones, de forma que pueda desarrollar una estrategia en el gobierno de los datos.

En el caso de la necesidad de divulgar el concepto de gobierno de datos en el grupo HM Hospitales, es importante hacer llegar a la dirección de la empresa la importancia de esta transformación digital y lo que supone para la empresa hacer de los datos un activo de presente y futuro. Aunque, probablemente, en el caso de HM Hospitales, la dirección del grupo es la que, habiendo tomado conciencia de esta necesidad, ha impulsado la transformación digital, y ha puesto al frente a la persona adecuada en papel de CDO además de dotar de la financiación adecuada, por lo que la parte más difícil, convencer a la dirección (y a los inversores) ya esté resuelto.

El siguiente paso del CDO es inculcar la cultura del gobierno de datos al resto de la empresa, debiendo llegar a todos los empleados el nuevo punto de vista de la empresa, la necesidad del buen uso de las TICs y las nuevas formas de trabajar.

Para ello es imprescindible disponer de una estrategia, con una hoja de ruta, que incluya acciones formativas, divulgativas y de concienciación de todos los estamentos de la empresa, acorde a las características de cada puesto de trabajo, que ponga de manifiesto el valor que el gobierno del dato aporta al negocio, las mejoras en la organización y al futuro de la compañía.

Hay que tener en cuenta que el gobierno de datos es la aplicación de un conjunto de reglas y buenas prácticas para garantizar el correcto uso de los datos y los procesos sobre estos.

Los objetivos principales del gobierno de los datos son:

- Desde un punto de vista de la gestión de los datos haciendo uso de las TICs:
    - Accesibilidad
    - Seguridad
    - Consistencia
    - Calidad
    - Auditoría
- Desde el punto de vista del valor de negocio de los datos:
    - Definir, validar y comunicar las estrategias del dato, normas, estándares, arquitectura, procedimientos y métricas.
    - Monitorizar las políticas del dato, estándares, arquitectura y procedimientos.
    - Patrocinar y supervisar la entrega de proyectos de gestión de dato y servicios.
    - Gestionar y resolver conflictos relacionados.
    - Entender y promocionar el valor del activo del dato.

Alcanzar con éxito todos los objetivos es necesario para el buen gobierno de los datos. La tarea es difícil y no exenta de complicaciones no solo por la dificultad de conseguir los medios y recursos

necesarios por parte de la empresa, sino por lo que implica en las relaciones humanas dentro de la organización al suponer un cambio en la mentalidad y en romper con las formas de tradicionales de hacer las cosas. Hay departamentos que se sienten importantes e incluso imprescindibles (¡qué error!) y son reacios no al solo al cambio, sino a que vengan otros a imponerle cómo deben hacer su trabajo o que se implanten procesos de información y auditoría sin necesidad de depender de personas concretas o tener que recurrir al departamento o individuo que se siente poseedor de la información.

Por ello, en mi opinión, y por mi experiencia en el sector público, donde cambiar las cosas es un proceso muy lento y supone una batalla tras otra en cambiar aptitudes y más transformación mental que digital, de los objetivos a alcanzar para el gobierno de los datos, pondría especial esfuerza, recursos y dedicación a la definición de la estrategia, su validación y posterior comunicación en toda la compañía, liderando esta comunicación la dirección ("el que manda"), de forma que se transmita un mensaje de cambio hacia el futuro, de auténtica revolución.

Luego, sería necesario hacer visibles resultados de esta transformación, por lo que antes de abordar todo el proyecto de golpe, entiendo conveniente mostrar avances centrando en algún proyecto concreto en el que los beneficios que ofrece el gobierno de los datos pueda servir de referente al resto de la organización, motivando así que el resto de la organización quiera participara de forma proactiva y productiva en los cambios.

En este sentido, se comprueba la buena labor que el grupo HM Hospitales[2] está realizando, al visitar la web del grupo y ver los comunicados y mensajes que ponen muy en valor cómo el cambio de estrategia hacia una organización orientada al dato y la implantación de gobierno de los datos suponen una característica diferenciadora frente a otras empresas del sector.

La siguiente figura muestra las siete fases del ciclo de vida del gobierno del dato según The Data Governance Institute:

Fuente: The Data Governance Institute.

Además de las siete fases, son necesarios dos prerrequisitos:

- Disponer de un **mensaje** del valor del programa **claro** y entendible por todos.
- Disponer de una **hoja de ruta** validada y participada por todos los implicados.

Ya se han comentado algunos de los aspectos más relevantes para conseguir los objetivos del gobierno de los datos, y se ha puesto mucho énfasis en la necesidad de transmitir un mensaje claro y directo dentro de la organización para convencer de la necesidad de participar en el reto que supone la transformación hacia el gobierno del dato. los objetivos en cada fase se pueden resumir de la siguiente forma:

Fase 1.

Describir cómo se ha **desarrollar la estrategia** de transformación hacia el gobierno de los datos, reflejando el valor que aporta al negocio, presente y futuro de la organización, evaluando el estado de la organización, y definir los criterios de éxito, para lo que es necesario establecer las métricas e indicadores que permitan medir el grado de éxito de los programas a ejecutar. En esta fase debe incluirse los análisis de riesgo y debilidades, además de la descripción de oportunidad y mejoras que el cabio hacia el gobierno de los datos supone para la organización.

Fase 2.

Preparar la **hoja de ruta** con un plan detallado de implantación y desarrollo, donde se defina la participación de cada departamento y coordinación, contemplar en lo posible los cambios puntuales que deban incorporarse y los requisitos que hagan sostenible el cambio. Esta hoja de ruta debe incluir el diseño de métricas e informes necesarios para el seguimiento del proceso de transformación.

Las fases 1 y 2 involucran de forma activa a la dirección de la empresa y a los responsables de departamento.

Fase 3.

Esta es la fase de **planificación y financiación.** En esta fase se han de determinar las fuentes de financiación y el alcance de los recursos financieros. Además de posible inversión en recursos humanos propios, hay que prever necesidades de contratación de empresas o profesionales externos y la adquisición de equipamiento o servicios. La planificación debe recoger, además de los medios de financiación con costes y gastos, el retorno de la inversión, tanto desde el punto de vista económico directo del abaratamiento de costes, mejora en implantación de nuevos servicios y clientes, como el impacto futuro en la imagen y confianza en la empresa.

La fase 3 involucra, además de la dirección de la organización, a los responsables financieros y de recursos humanos.

Fase 4.

Fase del **Diseño del Programa,** responsabilidad que recae de forma directa sobre el CDO, quien debe ser capaz de identificar, validar y documentar los procedimientos, establecer los procesos

estándares de negocio, definir los ámbitos y niveles de responsabilidad y, finalmente, exponer el modelo de gobierno del dato para informar al equipo ejecutivo.

Fase 5.

Fase de **Implementación del Programa.** Comienza el gobierno de los datos en la organización. Se inician los procesos de formación y concienciación en el gobierno del dato conforme a la hoja de ruta y se da difusión de las normas y guías sobre los procesos y procedimientos a seguir. Se llevan a cabo las mejoras y cambios necesarios conforme se va realizando el seguimiento del programa conforme a los informes que se generan según las métricas e indicadores previamente definidos.

A partir de esta fase, toda la organización está involucrada de forma directa y activa.

Fase 6.

El **Gobierno del Dato**. Si se logra llagar a esta fase, es que todo el trabajo anterior está dando sus frutos, y ya es posible implantar el diseño del gobierno del dato en el maco de la organización, pudiendo conocer ya en qué niveles y quienes son los encargados de la gestión de los datos como un activo de la empresa. Es determinante la correcta identificación de los responsables y el papel de cada uno en el gobierno del dato.

Fase 7.

Es el momento de la **monitorización, medición y generación de informes.** Esta fase permite disponer de información objetiva sobre la eficacia de la implantación del gobierno del dato en la organización, pudiendo ser necesaria la revisión de algunas métricas o indicadores, así como los modelos de generación de informes.

Para lograr el gobierno del dato en la organización, es necesario iniciar la implantación de cada una de las fases, disponiendo en cada una de ellas de los medios y recursos humanos, técnicos y económicos necesarios. Para ello es imprescindible el estudio de los requisitos previos, y contar con el asesoramiento adecuado, de lo contrario inversiones y esfuerzos puede llevar al fracaso.

Pregunta 2 (35% puntuación)

Después de la lectura del bloque 2, estamos seguros de que el gobierno del dato lo entendemos como un proyecto multifuncional.

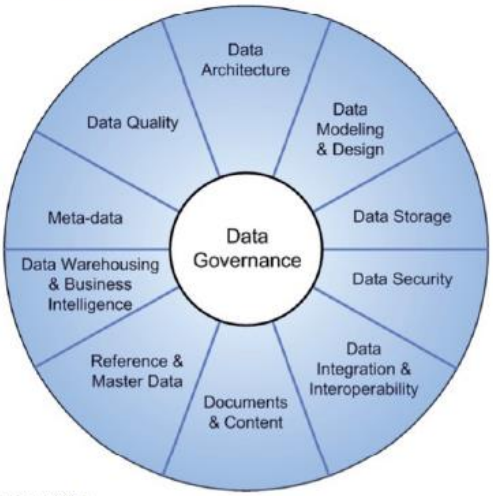
- Define y describe cada una de las funciones según DAMA
- Argumenta para la iniciativa de *Covid data save lives,* qué modelo de gobernanza de datos se habrá adaptado mejor para llevar a cabo dicha iniciativa con éxito, en función de las cuatro dimensiones básicas: personas, tecnología, normas y riesgos/recompensas.

El Diccionario DAMA de Gestión de Datos define **Gobierno de Datos** como "el ejercicio de la autoridad, control y toma de decisiones compartida (planificación, el seguimiento y la aplicación) a través de la gestión de activos de datos.

El gobierno del dato es un área de ámbito multidisciplinar que, siempre desde la perspectiva de los datos, abarca la gestión del negocio, el gobierno de las TICs y la gestión de la administración.

Las responsabilidades derivadas de cada uno de estos ámbitos están entrelazadas, como puede verse en la imagen:

Figura 4. Componentes gobierno del dato.



Fuente: DAMA - DMbok.

El **Gobierno del Dato,** en el centro de la figura, comprende todas las disciplinas relacionadas con la gestión de los datos y los sistemas de datos, ocupándose de los procesos de creación, obtención, transformación, distribución, protección, documentación y preservación de los datos, lo que comprende el **ciclo de vida de los datos** al completo.

El gobierno del dato pretende asegurar que los datos de la organización estén disponibles, protegidos y con calidad.

Según la DAMA, las funciones (o disciplinas) incluidas en el gobierno del dato son:

- **Arquitectura de datos.** Comprende la gestión de los sistemas y estructuras de almacenamientos y procesamiento de datos.
- **Modelos de datos.** Trata de la gestión, análisis, diseño, construcción, verificación y mantenimiento de los modelos de datos.
- **Almacenamiento de datos.** Gestiona las infraestructuras físicas de datos.
- **Seguridad de datos.** Trata los aspectos relativos a garantizar la privacidad y seguridad de los datos.

- **Datos maestros y de referencia.** Gestiona la identificación, mantenimiento, tratamiento, acceso y propagación de datos maestros y de referencia.
- **Inteligencia de negocio y almacenes de datos.** Le compete la gestión de los procesos analíticos y el acceso correcto a la información para la toma de decisiones.
- **Integración e interoperabilidad de datos.** Trata los procesos de adquisición, extracción, transformación, movimiento, propagación, replicación, federación y virtualización de los datos.
- **Contenido y documentos.** Gestiona el almacenamiento, protección, indexación y habilitación de acceso de datos en documentos, facilitando la integración e interoperabilidad con datos estructurados.
- **Metadatos.** consiste en la recopilación, categorización, mantenimiento, integración, control, gestión y distribución de metadatos.
- **Calidad de dato.** Trata la definición, monitorización, mantenimiento y mejora de la calidad e integridad de los datos.

Al diseñar un **plan de gobierno de datos** es clave realizar la elección de **modelos de gobernanza de datos** para determinar las diferentes formas de tomar decisiones de la organización.
Los modelos de madurez de la implantación del gobierno del dato se determinan en función de cuatro dimensiones: **Personas**, **Normas**, **Tecnologías**, y **Riesgos/ Recompensas,** identificándose cuatro modelos:

- **Modelo indisciplinado**
- **Modelo reactivo.**
- **Modelo proactivo**
- **Modelo gobernado**

En el caso del paso dado por HM Hospitales en una **transformación digital** para lograr convertirse en una **organización orientada al dato**, y a la vista de las diversas publicaciones, como ya se comentó en la PEC1 pasada, la compañía está inmersa en una inversión de futuro con una planificación en la que se apuesta por las alianzas tecnológicas de la que se puede deducir que se ha apostado por un **modelo proactivo,** con las siguientes características:

Modelo proactivo

- **Personal**
    - Los órganos de gobierno de la organización han entendido la necesidad del gobierno del dato, y ha destinado los recursos necesarios para iniciar los cambios necesarios.

  - Se considera el dato como un activo estratégico para la toma de decisiones, y se ha puesto en valor el éxito del proyecto.
  - Se ha creado la figura del CDO para implementar la estrategia y trabajar con los distintos equipos funcionales
- **Normas**
  - Se han establecido mecanismos para garantizar la seguridad y calidad de los datos, pasando de la necesidad de corrección de errores a la prevención.
- **Tecnología**
  - Se ha creado un grupo para administrar el dato que mantiene las normas de negocio y las descripciones de los datos de la organización. Además, se realiza un monitorizado de los datos y se han implementado procesos para comprobar la calidad de los datos.
- **Riesgos y Recompensas**
  - El riesgo no es muy alto, gracias a las medidas adoptadas que permiten disponer de mayor información para la toma de decisiones.
  - Las recompensas son altas por la penetración que el modelo está teniendo en la empresa.

Pregunta 3 (20% puntuación)

Los datos de la iniciativa *Covid data save lives:*

- ¿Cómo de privados los consideras? Define qué es privacidad y qué retos de seguridad supone.
- Razona la influencia de la privacidad en la seguridad de los datos. Recuerda definir los conceptos.
- ¿Qué elementos clave de seguridad y privacidad consideras que se han tenido en cuenta en la iniciativa de HM Hospitales?

Privacidad es todo lo relacionado con la vida personal de cada individuo, y que es objeto de mantenerse en secreto. Privacidad puede entenderse como sinónimo de **Intimidad,** y es un derecho de las personas decidir con quién, cómo, cuando y qué compartir con los demás. El **derecho a la privacidad** está contemplado en la declaración mundial de **derechos humanos**, por lo que debe ser respetado por todos, y es obligación de los gobiernos velar por el cumplimiento de este derecho.

En España, el **Código de Protección de Datos de Carácter Personal**[3] recoge la normativa española en materia de la protección de la privacidad de los datos personales. Esta normativa, adaptada a la directiva europea del **GDPR**[4] (General Data Protection Regulation), publicada como

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, contempla los **datos relativos a la salud** de forma explícita en su articulado.

El GDPR define los **datos de salud** como "Datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud." Además, el GDPR califica estos datos como **Especialmente Protegidos**

Así, los datos relativos a la salud de las personas son considerados como privados, y no pueden ser recabados sin el **consentimiento explícito** de la persona, aunque la normativa contempla el posible acceso y tratamiento de estos datos por entidades y profesionales del ámbito de la salud sin necesidad del consentimiento explícito cuando la urgencia por la vida de la persona lo requiera.

La problemática entorno a la privacidad de los datos relativos a la salud de las personas surge cuando entran en colisión **derechos y obligaciones** por parte de las personas y de los centros y profesionales del ámbito de la salud.

Así, todo paciente tiene derecho a que quede constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud, sobre sus datos médicos personales, y la normativa en materia de protección de datos de personales, y en concreto, los relativos a los datos médicos, regula los derechos y las obligaciones en materia de información y documentación clínica en la que se regula el historial del paciente.

La **historia clínica** es el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y evolución clínica de un paciente a lo largo de su proceso asistencial.

La aplicación del GDPR en el ámbito sanitario obliga a la **adopción de medidas** que garanticen la seguridad de sobres los datos y su tratamiento.

- **Veracidad.** Los datos recabados deben ajustarse al principio de veracidad, y ser pertinentes (no hay que recabar datos innecesarios).
- **Secreto.** Es obligatorio guardar el secreto profesional en todo caso.

- **Información.** El paciente debe estar debidamente informado en todo momento.
- **Medidas organizativas y de seguridad.** Es necesario adoptar medidas de seguridad en función del riesgo en el tratamiento de los datos (antes del GDPR las medidas se adoptaban por niveles de seguridad).
- **Evaluación del impacto.** Es el análisis del riego, de forma que los responsables del tratamiento puedan adoptar las medidas adecuadas para minimizar el riesgo, evitando consecuencias negativas para la organización y los pacientes.
- **Elaboración del Documento de Seguridad.** Tanto las medidas de seguridad como los protocolos deben estar recogidos en un Documento de Seguridad, que deberá estar a disposición de la Agencia Española de Protección de Datos,[5] Desde el GDPR no es necesaria la inscripción de ficheros de datos en la AEPD.
- **Registro de actividades del tratamiento.** Es obligatorio mantener un registro de actividades de tratamiento, como mínimo con la siguiente información:
    - Datos del responsable del tratamiento y del DPO
    - Finalidad del tratamiento de los datos
    - Detalle de las categorías de datos e interesados y posibles destinatarios
    - Transferencias internacionales de dados y documentos de garantías.
- **Nombramiento de un Delegado de Protección de Datos (DPO).** Este nombramiento, de carácter obligatorio, debe ser comunicado a la AEPD.
- **Comunicación de datos.** Hay que dar constancia al paciente de la **cesión** de sus datos a terceros, habiendo recabado previamente el consentimiento del paciente.
- **Facilitar los derechos de acceso, rectificación, cancelación y oposición (ARCO)**

Fuente: Grupo Atico34

Todo este marco normativo que regula la privacidad de los datos relativos a la salud de las personas se debe implementar en la organización, para lo que es necesario disponer de **herramientas tecnológicas y personal cualificado** de cara a cumplir los **requisitos de seguridad** derivados de las obligaciones por la **privacidad de los datos**.

En el supuesto de la iniciativa **Covid Data Safe LIves**, ha debido implementarse herramientas que faciliten las obligaciones de conformidad de seguridad y privacidad, y en concreto, sobre los datos que forman parte del conjunto de datos publicado se ha debido aplicar, al menos, las siguientes **técnicas de protección**:

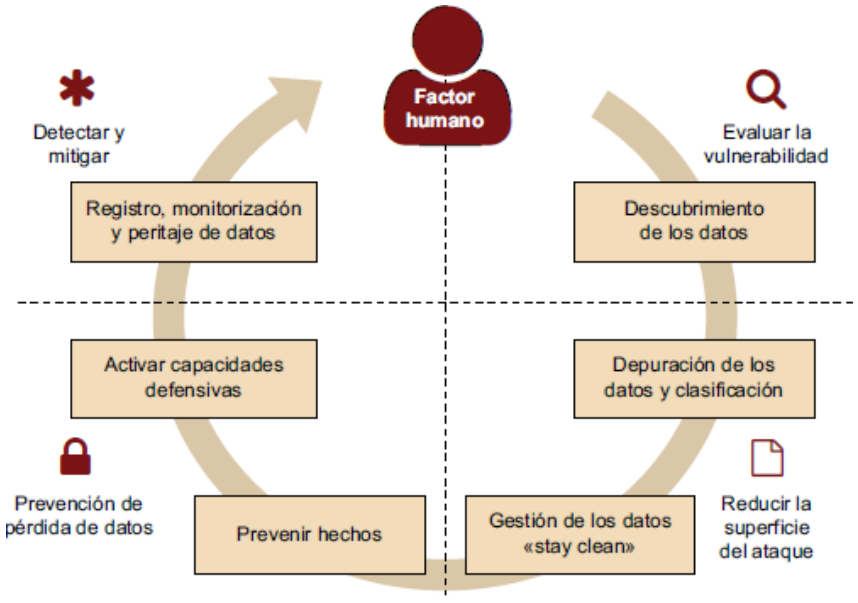
- **Enmascaramiento** de datos, para garantizar que la información original no esté disponible.
- **Anonimización o disociación** de los datos, para impedir la identificación de los interesados.
- **Cifrado** de los datos, lo que dificultará el posible acceso ilegítimo o robo de información.

El conjunto de datos publicado en el proyecto Covid Data Safe Lives, se ha obtenido a partir de las historias clínicas de pacientes de los hospitales del grupo HM Hospitales, por lo que debían formar parte de algún repositorio de datos de la organización. Previo a la aplicación de estos procesos de protección mencionados en el párrafo anterior sobre los datos del repositorio, se ha debido realizar tareas sobre la seguridad de los datos:

- **Clasificación**, para identificar los datos sensibles en los repositorios de datos de la organización, siendo necesario emplear técnicas de autodescubrimiento, catalogación y trazabilidad de datos.
- **Auditoría**, para conocer a qué datos protegidos se accede y quién accede.
- **Protección**, para mantener debidamente protegidos los datos frente a los riesgos contra la seguridad.
- **Monitorización**, para conocer en todo momento qué usuarios, dispositivos o sistemas acceden a los datos.

Todo esto, además, acompañado de tecnologías habituales y bien conocidas en el ámbito de la seguridad de las Tecnologías de la Información y de las Comunicaciones (**TICs**) para proteger las infraestructuras de redes, sistemas, servicios, sistemas de almacenamiento y usuarios, entre otros aspectos de la seguridad (directorios de usuarios y sistemas de autenticación, cortafuegos, antivirus, sistemas perimetrales de seguridad…).

La **seguridad y privacidad** en el ámbito del **Gobierno del Dato** debe estar enmarcada de forma global, como se muestra en la figura:



Fuente: *Infinitive Insights*

Por un lado, la gestión proactiva y gobierno del dato, y por otro la prevención y monitorización activa, y en el centro el factor humano. De esta forma se puede centralizar la **política de seguridad y de privacidad,** y coordinar las técnicas y procesos tradicionales sobre la seguridad de la información, con los requisitos de seguridad del gobierno de los datos.

Además de tratar los datos de forma segura y privada conforme al ordenamiento jurídico y normativo, es necesario ir acompañado de **políticas éticas** para garantizar la **veracidad** de los datos, el deber de **información** al interesado, asegurar el **secreto** y la **seguridad**, así como no almacenar los datos más allá de lo necesario y garantizar su destrucción cuando sea pertinente, y finalmente, determinar la **Responsabilidad** para la garantizar los principios de la protección de la privacidad.

Es relevante la información que figura en el comunicado[6] de HM Hospitales sobre el proyecto Covid Data Safe Lives, en el que se dice "*Para obtener los datos será necesario enviar una solicitud al correo coviddatasavelives@hmhospitales.com para ser evaluada por la Comisión de Data Science y, en su caso, por el Comité de Ética de la Investigación de HM Hospitales*." Se pone de manifiesto la existencia en la organización de una **Comisión de Data Science** y un **Comité de Ética**¸ que son los encargados de validar las peticiones de acceso (o **cesión** a terceros) a los datos, lo que supone garantías de que se han adoptado medidas para proteger la privacidad de los datos de los pacientes conforme a la normativa vigente.
Además, desde la web del grupo HM Hospìtales se puede acceder al documento "Política de Privacidad"[7] en el que figuran el responsable del tratamiento y el DPO.

Pregunta 4 (15% puntuación)

Si analizamos la iniciativa de *Covid data save lives:*

- ¿Ha primado lo bueno, lo justo o lo correcto? Justifica tu respuesta en base a las teorías éticas fundamentales
- Qué principios han de orientar tu ejecución profesional como científico de datos desde la perspectiva de la ética.

Los datos conciernen a las personas, y los científicos de datos, como personas, tenemos valores éticos y morales, lo que hace necesario estar instruidos y conocer las herramientas que ayuden a identificar los problemas éticos relacionados con el gobierno del dato.
Las organizaciones están formadas por personas, y son estas personas, con su cultura y formación, quienes determinarán la responsabilidad u compromiso de la organización con la sociedad.

Las referencias éticas en el ámbito científico suelen estar relacionadas a las cuestiones éticas más mediáticas, como la bioética, la ética sobre la experimentación con animales, la vacunación o la eutanasia, o más reciente, en ámbitos más técnicos, los problemas éticos relacionados con la inteligencia artificial o la robótica, pasando desapercibidos otros aspectos esenciales para los investigadores como es la ética asociada al Big Data.

Como se ha visto en el ejercicio anterior, existe un marco normativo sobre la privacidad y la seguridad de los datos de carácter personal, que debe ser conocido por las entidades de investigación e investigadores y, por ende, por el científico de datos.
Esta normativa, también permite una relajación en la aplicación cuando se trate de proyectos de "**interés público, científico o de investigación histórica o estadística**", por lo que se permite obtener el necesario consentimiento sin necesidad de especificar los tratamientos de que van a ser objeto los datos recopilados y almacenados dentro de un proyecto y que puedan ser de utilidad en otros proyectos, siempre y cuando se aplique las medidas de seguridad reguladas.
La ética científica suele plantearse desde un punto de vista deontológico, bajo el cual, los investigadores se deben a obligaciones morales independientemente de las consecuencias de su incumplimiento.
Los principios básicos que se deben aplicar por los investigadores en general, y los científicos de datos en particular, están recogidos en la **Declaración sobre la Ciencia y el uso del Saber Científico**[8] adoptada en la Conferencia Mundial sobre la Ciencia de la UNESCO del 10 de Julio de 1999[9].

Los **principios éticos profesionales** son principios orientativos con la finalidad de ayudar en las decisiones, permitiendo **evaluar** cuánto bueno y realizable, o malo y evitable hay en las consecuencias de una acción.

- **Principio de beneficencia.** Bajo este principio, una vez identificado el **"bien"**, la finalidad de la acción profesional es la **maximización**. Este principio está fundamentado en la idea de "hacer el bien" y actuar en beneficio de los demás.
- **Principio de autonomía.** Es de origen deontológico por lo que suele estar en conflicto con el anterior, y puede definirse como la capacidad de las personas para decidir sobre sus finalidades personales y actuar bajo las directrices de estas decisiones, por lo que, todos los individuos son tratados como seres autónomos, siendo necesario regular el derecho a la protección de quienes tengan limitada la autonomía.

- **Principio de justicia.** Intenta resolver los conflictos de los dos anteriores, y busca la equidad de cargas y beneficios, incluyendo el rechazo a la discriminación, y suele estar legislado.
- **No maleficencia.** se fundamenta en no producir daño y prevenirlo, y suele estar legislado, sobre todo las penas a imponer por su incumplimiento.

Si hay conflicto en la aplicación de estos principios, los de justicia y no maleficencia deben estar por encima de los de beneficencia y autonomía.
Estos principios deben servir de guía al científico de datos en sus reflexiones ante cuestiones éticas y morales que puedan surgir en el desempeño de sus funciones o en el seno de la entidad donde se realice su trabajo. Es imprescindible conocer los principios éticos para garantizar que la toma de decisiones se puede hacer desde una reflexión centrada en los valores.

En el marco del proyecto Covid Data Save Lifes, y según declaraciones del presidente del grupo HM Hospitales, Dr. Juan Abarca, considera las posibilidades que ofrece la ciencia de datos como "la poderosa arma que tenemos para **ayudar a millones de pacientes de todo el mundo**". Desde luego, puesto que se trata de un proyecto para ayudar en la erradicación de la pandemia mundial por COVID19, el **principio de beneficencia** es claro, justificando la iniciativa en el beneficio para millones de personas en todo el mundo.
El proyecto Covid data Save Lifes ha generado un conjunto de datos disponible para la comunidad científica con historias médicas de pacientes atendidos por covid19. Si la empresa ha seguido las normas en materia de privacidad y seguridad, los riesgos sobre la seguridad de las historias clínicas están en buena medida controlados, por lo no tiene por qué producirse un daño sobre los interesados, que seguramente han debido estar informados y haber prestado su consentimiento.
Por otro lado, los resultados de las investigaciones que se puedan llevar a cabo derivadas del uso de los datos gestionados en este proyecto, serán de utilidad para todo el mundo, no solo para los clientes del grupo HM Hospitales, por lo que el **principio de justicia** también está inherente.
Por último, que una organización privada como HM Hospitales haya decidido invertir esfuerzos y recursos en poner en valor y dar utilidad a sus datos sobre las atenciones por Covid19, no cabe duda, que es actuar de forma correcta, además de ejemplarizante.

Por tanto, basándome en los principios éticos descritos, no encuentro argumentos que me lleven a otra cosa que no sea concluir que en la iniciativa Covid Data Save Lives ha **primado lo bueno, lo correcto y lo justo.**

Referencias:

[1]. DAMA Internacional, Data Management Body of Knowledge (DMbok), www.dama.org

[2]. HM Hospitales, hmhospitales.com

[3] Código de Protección de Datos de Carácter Personal, https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=055_Proteccion_de_Datos_de_Caracter_Personal&tipo=C&modo=2

[4] General Data Protection Regulation, https://eur-lex.europa.eu/legal-content/ES/TXT/?qid=1532348683434&uri=CELEX%3A02016R0679-20160504

[5] Agencia Española de Protección de Datos, https://www.aepd.es/es

[6] https://www.hmhospitales.com/prensa/notas-de-prensa/comunicado-covid-data-save-lives

[7] Política de Privacidad de HM Hospitales, https://www.hmhospitales.com/Documents/politica-de-privacidad.pdf

[8]. Declaración sobre la Ciencia y el uso del Saber Científico, http://www.unesco.org/science/wcs/esp/declaracion_s.htm

[9] Conferencia Mundial sobre la Ciencia de la UNESCO del 10 de Julio de 1999, http://www.unesco.org/science/wcs/index.htm