OQOTECH

TECH & QUALITY

Validación de Sistemas en entornos cloud

Mayte Garrote Gallego

CTO, Oqotech

@Mayte Garrote Gallego

CURSOS GRATUITOS ONLINE 2023

19 ABRIL — Análisis de requisitos y enfoque de validación para los Sistemas Informatizados. Revisión del anexo 11, CSA y segunda edición GAMP5.

17 MAYO — Mantenimiento del estado de control.

14 JUNIO — Sistema de calidad híbrido (digital / papel).

12 JULIO — Digitalización documental en ambientes farma.

18 OCTUBRE — Enfoque de validación para el desarrollo de software agile.

15 NOVIEMBRE — Validación de sistemas en entornos cloud.

13 DICIEMBRE — Caso Práctico: Recopilación de preguntas y respuestas.

OQOTECH
TECH & QUALITY

www.oqotech.com

Índice

01. Entorno Regulatorio

02. Entorno Cloud

03. Actividad delegada

04. Actividad de Validación

OQOTECH
TECH & QUALITY

Entorno Regulatorio

Entorno Regulatorio

Normativas y guías aplicables.

AEMPS

- Anexo 11, Sistemas informatizados.
- Anexo 15, Cualificación y Validación.
- Capítulo 4, Documentación
- ICH guideline Q9 on quality risk management

FDA

- 21 CFR Part 11, Electronic Records; Electronic Signatures — Scope and Application
- Computer Software Assurance for Production and Quality System Software Food and Drug Administration Staff

ISPE

- GAMP5, A Risk-Based Approach to Compliant GxP Computerized Systems. Second Edition.
- Good Practice Guide, Enabling Innovation. Critical Thinking, Agile, IT Service Management.

MHRA

- 'GXP' Data Integrity Guidance and Definitions

WHO

- Annex 5. Guidance on good data and record management practices

Principio GxP

Este anexo aplica a todas las formas de sistemas informatizados usados como parte de las actividades reguladas por las GxP. Un sistema informatizado es un set de componentes de software y hardware que juntos satisfacen ciertas funcionalidades.

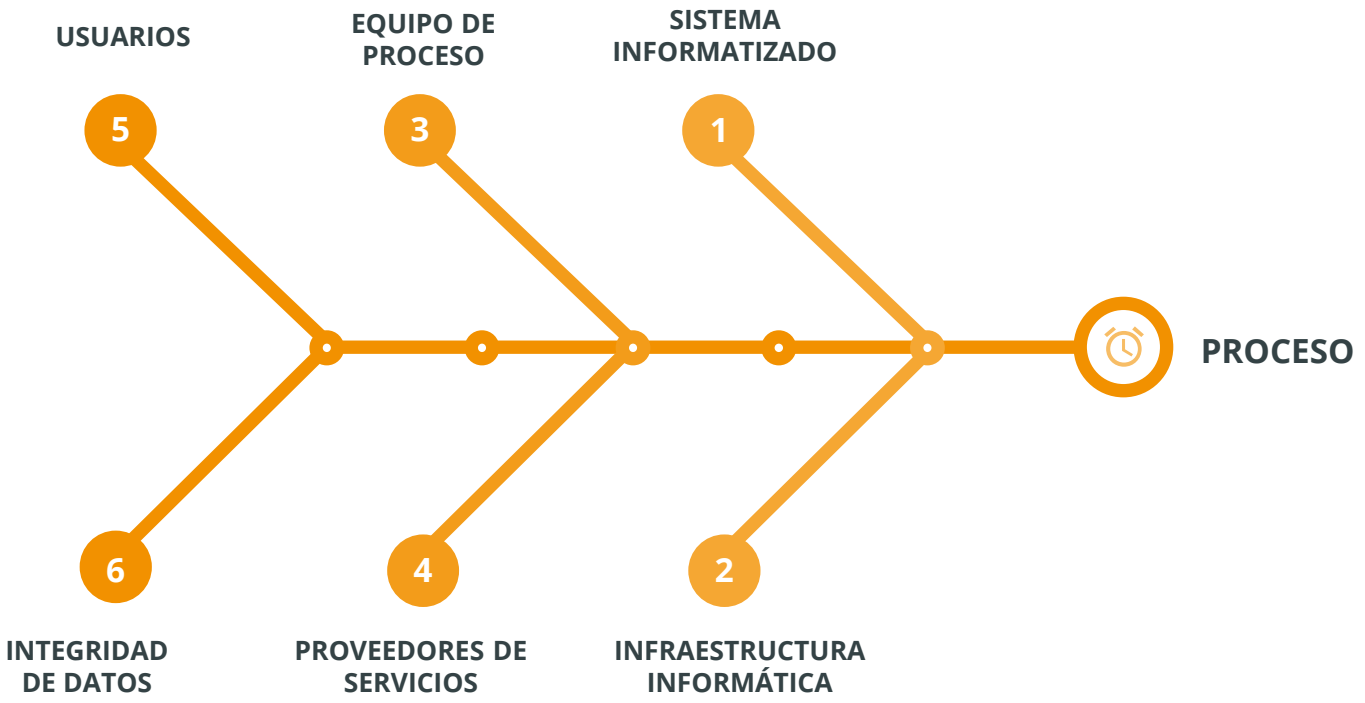
La aplicación debe validarse; la infraestructura informatizada (IT) debe cualificarse.

Cuando un sistema informatizado reemplace una operación manual, no debe ser en detrimento de la calidad del producto, control del proceso o garantía de calidad. No debe haber un incremento del riesgo total del proceso.

Anexo 11

Riesgos asociados a los Sistemas Informatizados

Asegurar el uso previsto de los sistemas informatizados durante su ciclo de vida.



OQOTECH
TECH & QUALITY

Requisitos / buenas prácticas – Servicios en la nube

En la revisión del Anexo11 se incluye:

- Se deben incluir los sistemas informatizados en nube.

Proveedores IT (MHRA, GMP Data Integrity Definitions and Guidance for Industry)

- Cuando se utilicen servicios "en nube" o "virtuales", debe prestarse atención a la comprensión del servicio prestado, la propiedad, la recuperación, la conservación y la seguridad de los datos.
- Debe tenerse en cuenta la ubicación física donde se conservan los datos, incluido el impacto de cualquier ley aplicable a esa ubicación geográfica.
- Las responsabilidades del proveedor tecnológico y la empresa regulada deben definirse en un acuerdo o contrato técnico. Esto debería garantizar el acceso oportuno a los datos (incluidos los metadatos y las pistas de auditoría) al propietario de los datos y a las autoridades nacionales competentes que lo soliciten. Los contratos con los proveedores deben definir las responsabilidades en materia de archivo y legibilidad continua de los datos durante todo el periodo de conservación.
- Deben existir disposiciones adecuadas para la restauración del software/sistema según su estado validado original, incluida la información de validación y control de cambios que permita esta restauración.
- Los acuerdos de continuidad de la actividad deben incluirse en el contrato y probarse. La necesidad de una auditoría del proveedor de servicios debe basarse en el riesgo.

Requisitos / buenas prácticas – Servicios en la nube

Organizaciones contratadas, proveedores y proveedores de servicio (WHO, Guidance on Good Dara al Record Management Practices)

- La creciente externalización de actividades GXP pone de relieve la necesidad de establecer y mantener firmemente definidas las funciones y responsabilidades para garantizar datos y registros completos y precisos a lo largo de estas relaciones. Las responsabilidades del proveedor y de la empresa regulada deben abordar de forma exhaustiva los procesos de ambas partes que deben seguirse para garantizar la integridad de los datos. Estos detalles deben incluirse en un contrato que describa el trabajo externalizado o a los servicios prestados.
- La empresa regulada que subcontrata el trabajo es responsable de la integridad de todos los resultados comunicados, incluidos los proporcionados por cualquier organización subcontratada o proveedor de servicios. Estas responsabilidades se extienden a cualquier proveedor de servicios informatizados pertinentes. Cuando se subcontraten bases de datos y el suministro de software, el contratante debe asegurarse de que los subcontratistas han sido acordados y están incluidos en el acuerdo de calidad con el contratante, y de que están debidamente cualificados y formados en GRDP. Sus actividades deben supervisarse periódicamente a intervalos determinados mediante una evaluación de riesgos. Esto también se aplica a los proveedores de servicios basados en la nube.

Requisitos / buenas prácticas – Servicios en la nube

Organizaciones contratadas, proveedores y proveedores de servicio (WHO, Guidance on Good Dara al Record Management Practices)

- Para cumplir con esta responsabilidad, además de contar con sus propios sistemas de calidad, la empresa regulada debe verificar la adecuación de los los sistemas de gobernanza del proveedor de servicio, mediante una auditoría u otros medios adecuados. Esto debe incluir la adecuación de los controles de la empresa regulada sobre los proveedores y una lista de terceros autorizados significativos que trabajan para el proveedor.
- El personal que evalúe y valore periódicamente la competencia de un proveedor de servicios debe contar con la formación, las cualificaciones, la experiencia y la formación adecuadas para evaluar los sistemas de gobernanza de la integridad de los datos y detectar problemas de validez. La naturaleza y frecuencia de la evaluación del aceptante del contrato y el enfoque de la supervisión continua de su trabajo deben basarse en una evaluación documentada del riesgo. Esta evaluación debe incluir una evaluación de los procesos de datos pertinentes y sus riesgos.
- Las estrategias previstas de control de la integridad de los datos deben incluirse en los acuerdos de calidad y en los acuerdos contractuales y técnicos escritos, según corresponda y sea aplicable, entre el el proveedor y la empresa regulada. Éstas deben incluir disposiciones para que el proveedor tecnológico tenga acceso a todos los datos en poder de la organización que sean relevantes para el producto o servicio del proveedor, así como a todos los registros relevantes de los sistemas de calidad.

Requisitos / buenas prácticas – Servicios en la nube

Organizaciones contratadas, proveedores y proveedores de servicio (WHO, Guidance on Good Dara al Record Management Practices)

- Cuando la conservación de datos y documentos se contrata a un tercero, debe prestarse especial atención a comprender la propiedad y la recuperación de los datos conservados en virtud de este acuerdo. También debe tenerse en cuenta la ubicación física donde se conservan los datos y el impacto de cualquier ley aplicable a esa ubicación geográfica. Los acuerdos y contratos deben establecer consecuencias mutuamente acordadas en caso de que la empresa regulada deniegue, rechace o limite el acceso del proveedor a sus registros. Los acuerdos y contratos también deben contener disposiciones sobre las medidas que deben tomarse en caso de cierre de la empresa o quiebra del tercero para garantizar que se mantiene el acceso y que los datos pueden transferirse antes del cese de todas las actividades empresariales.
- Cuando se externalicen bases de datos, el contratante debe asegurarse de que, si se utilizan subcontratistas, en particular proveedores de servicios basados en la nube, estos estén incluidos en el acuerdo de calidad y estén debidamente cualificados y formados en GRDP. Sus actividades deben supervisarse periódicamente a intervalos determinados mediante una evaluación de riesgos.

Entorno Cloud

Beneficios de los servicios en la nube

Disminución de riesgos si se selecciona al proveedor tecnológico adecuado y se establecen los acuerdos de calidad de servicio precisos.

- Beneficios de la externalización:
  - **Infraestructura física** a mantener de forma periódica con riesgo de degradación y obsolescencia.
  - **Personal especialista** en el diseño, configuración y mantenimiento de la infraestructura informática.
  - Buenas prácticas asociadas al **sistema de calidad** de la infraestructura informática.
  - Seguridad física y lógica.
  - Plan de remediación ante **ataques de seguridad** en continuo proceso de evolución.
  - **Servicio garantizado y gestión de los datos**.
  - Definición de **planes de continuidad de negocio y tiempos de respuesta** ante contingencias.

Modelos de servicios en la nube

Aplicaciones hospedadas.

Herramientas de desarrollo, administración de bases de datos, análisis de negocios.

Sistema operativo.

Servidores y almacenamiento.

Seguridad/firewalls de red.

Edificio/planta física para el centro de datos.

Infrastructure as a Service (IaaS)

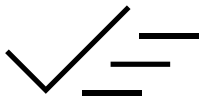
Platform as a Service (PaaS)

Software as Service (SaaS)

OQOTECH
TECH & QUALITY

Aspectos clave de los servicios en la nube

Actividad delegada



Actividad de validación diferente a la tradicional. Ausencia de visibilidad de datos y procesos de administración y mantenimiento.

Actividad delegada

Infraestructura Cloud

- Los proveedores de servicios en la nube no están regulados por GxP, y es responsabilidad de la organización regulada que utiliza dichos servicios garantizar que los procesos de calidad cumplan con los requisitos aplicables al sector.

- Requisitos de la organización regulada:
  - Evaluación de proveedores.
  - Acuerdos contractuales sobre niveles de servicio, calidad y supervisión.
  - Se deben contemplar en los acuerdos procedimientos acordados de gestión de incidencias y aseguramiento de los datos.

- Cuando se externaliza un sistema GxP a un tercero, es vital comprender dónde residen los datos y asegurarse de que el proveedor de servicios ha tomado las medidas adecuadas para garantizar que su prestación es sólida.

Control sobre los proveedores tecnológicos

- Identificación de proveedores tecnológicos críticos.
  - Producto y/o servicio previsto.
  - Evaluación / homologación de proveedores.
  - Gestión del servicio.
  - Evaluación del servicio.

Los contratos y acuerdos adecuados son esenciales para definir las expectativas, responsabilidades y medidas de rendimiento.

Procedimiento de evaluación de proveedores

- Por sistema informatizado identifica los proveedores de servicio tecnológico.
- Facilita la identificación y definición del producto/servicio previsto por parte de los proveedores.
- Confirma su aplicación en todo el ciclo de vida de los sistemas.
- Establece los criterios de aceptación en todo el ciclo de vida.
- Establecer la criticidad de los proveedores de servicio tecnológico.
- Facilita la confirmación de buenas prácticas o certificaciones por parte del proveedor.
- Preparación de un acuerdo de servicio estándar para los proveedores de servicio tecnológico crítico que describa la planificación, implementación y documentación asociada prevista. La extensión de la definición o controles requeridos debe basarse en el riesgo y la complejidad de los sistemas informatizados administrados.
- Identifica roles y responsabilidades.
- Establece los procedimientos para la revisión periódica de proveedores críticos.
- Facilita el mantenimiento del estado de control.

Acuerdos de calidad del producto / servicio prestado

Los acuerdos deben concretar el nivel de la calidad y gestión del servicio contratado. Recomendación:

- Descripción de la empresa proveedora de servicios y equipo de proyecto asociado.
- Descripción de los productos proporcionados y/o servicios prestados.
- Documentación del sistema informatizado requerido.
- Documentación de procedimientos internos del proveedor de servicios requerida.
- Especificación de entornos de trabajo disponibles y uso previsto de los mismos.
- Política de versionado y actualización del software a seguir.
- Gestión de control de cambios.
- Gestión de incidencias.
- Servicio garantizado.
- Ubicación, disponibilidad y recuperación de los datos garantizados.
- Acceso a monitorización y métricas de los servicios delegados.

Quedando reflejados en los puntos anteriormente citados los roles y responsabilidades de cada una de las partes.

Acuerdos de calidad del producto / servicio prestado

Los acuerdos deben concretar el nivel de la calidad y gestión del servicio contratado. Recomendación:

- Protección de datos de carácter personal.
- Propiedad de los trabajos y propiedad intelectual.
- Confidencialidad y acceso a la información

- Revisión periódica del servicio prestado. Auditorías.

- Periodo de aplicación de los servicios.
- Modificaciones o ampliaciones de los servicios
- Precio y modalidades de pago.

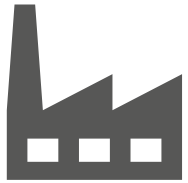
Quedando reflejados en los puntos anteriormente citados los roles y responsabilidades de cada una de las partes.

Gestión de proveedores

- Gestión del proveedor durante el servicio.
  - Mejora continua de la colaboración
  - Seguimiento
  - Gestión de incidencias y no conformidades
  - Reclamaciones
- Evaluación periódica según la actividad delegada.

Actividad de Validación

Infraestructura IT físico vs nube



La infraestructura informática se encuentra alojada en las instalaciones de la organización y es evaluada a través de una cualificación formal.

La infraestructura es responsabilidad del proveedor. No se dispone de visibilidad a nivel de características de la arquitectura informática ni el mantenimiento establecido.

CSA

- El programa Computer Software Assurance (CSA) refuerza la importancia de adoptar un enfoque basado en los riesgos y centrado principalmente en el impacto para la seguridad y calidad del producto.
- El enfoque descrito se basa en la definición clara del uso previsto del sistema y en la determinación de un enfoque basado en el riesgo en función del impacto del sistema en la seguridad y la calidad del producto.
- Incluye el aprovechamiento de las actividades existentes y los datos del proveedor, las herramientas automatizadas y la captura de datos, y el uso de métodos de prueba ágiles.
- Cualquier registro producido debe ser de valor para la organización.

Pensamiento crítico

- El pensamiento crítico se define como "un proceso sistemático, racional y disciplinado de evaluación de la información desde una variedad de perspectivas para obtener una respuesta equilibrada y bien razonada".
- El pensamiento crítico está en consonancia con la aplicación de los principios de la gestión de riesgos de calidad de la norma ICH Q9.
- Puede y debe convertirse en una mentalidad/estrategia habitual basada en el conocimiento y experiencia del equipo multidisciplinar de validación para guiar en el enfoque y ejecución de las actividades a desarrollar a lo largo del ciclo de vida del sistema.

Riesgos asociados a entornos cloud

- Análisis de riesgos considerando:
  - Infraestructura informática
  - Procesos
  - Datos
  - Servicios aplicados
  - Personal
  - Sistema de calidad
  - Normativa
  - Documentación
  - Reclamaciones y defectos de calidad

Riesgos asociados a entornos cloud

Item	Posible modo de fallo	Efectos potenciales del fallo	Causa potenciales del fallo	Criticidad C	Probabilidad L	Clasificación del riesgo RC	Detectabilidad D	IPR	Acción mitigadora del riesgo
1	**Infraestructura informática**								
1.1	Menor o ningún control sobre el centro de procesamiento de datos	Pérdida de servicio y/o integridad de datos. Puede afectar a registros y gestión del proceso GxP relevantes.	Ante la ausencia de control sobre el procesamiento de datos, no haber determinado un acuerdo, entre compañía regulada y el proveedor, que especifique el servicio y datos garantizado por el proveedor tecnológico.	3	1	**3**	1	**3**	-
1.2.1	Incompatibilidad de la infraestructura informática con la infraestructura informática anterior (para cambios)		Ausencia de especificación técnica requerida por los sistemas informatizados a gestionar en la nube por parte de compañía regulada.	3	2	**6**	1	**6**	Definir y aprobar las especificaciones técnicas requerida por los sistemas informatizados a gestionar en la nube.
1.2.2			Ausencia de un acuerdo de calidad del servicio, entre compañía regulada y el proveedor, que garantice el cumplimiento de los requisitos técnicos especificados por compañía regulada.	3	2	**6**	1	**6**	Generar, aprobar y firmar de un acuerdo de calidad del servicio, entre compañía regulada y el proveedor, que garantice el cumplimiento de los requisitos técnicos especificados por compañía regulada.
1.3.1	Diseño, cualificación, configuración y mantenimiento de la infraestructura informática dependiente del proveedor deficiente.		Ausencia de especificación técnica y mantenimiento requerido por parte de compañía regulada.	3	2	**6**	2	**12**	Definir y aprobar las especificaciones técnicas y mantenimiento requeridos para los sistemas informatizados a gestionar en la nube.
1.3.2			Ausencia de un acuerdo de calidad del servicio, entre compañía regulada y el proveedor, que garantice el cumplimiento de los requisitos técnicos y mantenimiento especificados por compañía regulada.	3	2	**6**	1	**6**	Generar, aprobar y firmar de un acuerdo de calidad del servicio, entre compañía regulada y el proveedor, que garantice el cumplimiento de los requisitos técnicos y mantenimiento especificados por compañía regulada.
1.3.3			Mala práctica en el diseño, configuración y mantenimiento por parte del proveedor.	3	1	**3**	3	**9**	Acuerdo de servicio y datos garantizados por el proveedor. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor.
1.4.1	No se dispone de acceso físico o muy limitado a los servidores		Ante la ausencia de acceso a los servidores, no haber determinado un acuerdo, entre compañía regulada y el proveedor, que especifique el servicio y datos garantizado por el proveedor tecnológico.	3	1	**3**	1	**3**	Generar, aprobar y firmar de un acuerdo de calidad del servicio, entre compañía regulada y el proveedor, que garantice el cumplimiento de los requisitos técnicos especificados por compañía regulada.
1.4.2			Mala práctica en el diseño, configuración y mantenimiento de la seguridad física de los servidores por parte del proveedor.	3	1	**3**	3	**9**	Acuerdo de servicio y datos garantizados por el proveedor. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor.

Riesgos asociados a entornos cloud

Item	Posible modo de fallo	Efectos potenciales del fallo	Causa potenciales del fallo	Criticidad C	Probabilidad L	Clasificación del riesgo RC	Detectabilidad D	IPR	Acción mitigadora del riesgo
1	**Infraestructura informática**								
1.5.1	Configuración y mantenimiento de los servidores dependiente del proveedor deficiente.	Pérdida de servicio y/o integridad de datos. Puede afectar a registros y gestión del proceso GxP relevantes.	Ausencia de especificación técnica y mantenimiento requerido por parte de compañía regulada.	3	2	**6**	2	**12**	Definir y aprobar las especificaciones técnicas y mantenimiento requeridos para los sistemas informatizados a gestionar en la nube.
1.5.2			Ausencia de un acuerdo de calidad del servicio, entre compañía regulada y el proveedor, que garantice el cumplimiento de los requisitos técnicos y mantenimiento especificados por compañía regulada.	3	2	**6**	1	**6**	Generar, aprobar y firmar de un acuerdo de calidad del servicio, entre compañía regulada y el proveedor, que garantice el cumplimiento de los requisitos técnicos y mantenimiento especificados por compañía regulada.
1.5.3			Mala práctica en el diseño, configuración y mantenimiento por parte del proveedor.	3	1	**3**	3	**9**	Acuerdo de servicio y datos garantizados por el proveedor. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor.
1.6	Tiempos de servicio del proveedor ante alta, modificación o baja de servicios delegados no definidos. Retrasos y configuración incorrecta.		Ausencia de un acuerdo de calidad del servicio, entre compañía regulada y el proveedor, que garantice el cumplimiento de los tiempos de servicio del proveedor.	3	2	**6**	2	**12**	Generar, aprobar y firmar de un acuerdo de calidad del servicio, entre compañía regulada y el proveedor, que garantice el cumplimiento de los tiempos de servicio del proveedor.
1.7.1	Servicios y datos se encuentran fuera de la empresa.		Mala práctica en el diseño, configuración y mantenimiento por parte del proveedor.	3	1	**3**	3	**9**	Acuerdo de servicio y datos garantizados por el proveedor. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor.
1.7.2			Ausencia de un acuerdo de calidad del servicio, entre compañía regulada y el proveedor, que garantice el cumplimiento de los requisitos técnicos y mantenimiento especificados por compañía regulada.	3	2	**6**	1	**6**	Generar, aprobar y firmar de un acuerdo de calidad del servicio, entre compañía regulada y el proveedor, que garantice el cumplimiento de los requisitos técnicos y mantenimiento especificados por compañía regulada. Asegurar la recuperación de datos GxP relevantes ante una finalización de servicio.

Riesgos asociados a entornos cloud

Item	Posible modo de fallo	Efectos potenciales del fallo	Causa potenciales del fallo	Criticidad C	Probabilidad L	Clasificación del riesgo RC	Detectabilidad D	IPR	Acción mitigadora del riesgo
2	**Procesos**								
2.1	No se dispone de acceso a los sistemas informatizados en nube.	Pérdida de servicio. Puede afectar a la gestión del proceso GxP relevante o la consulta o registro de su información asociada.	Acceso al sistema dependiente del servicio del proveedor	3	1	**3**	3	**9**	Generar, aprobar y firmar un acuerdo, entre compañía regulada y el proveedor, que especifique el servicio y datos garantizado por el proveedor tecnológico.
2.2			Acceso al sistema dependiente del servicio de internet de compañía regulada	3	2	**6**	3	**18**	Contratación de dos líneas, con operadores independientes, para el servicio de internet.
2.3			Acceso al sistema dependiente del tunel de seguridad establecido entre el proveedor y la compañía. Acceso al sistema dependiente de la configuración del proveedor	3	1	**3**	3	**9**	Acuerdo del tipo de conexión, determinar la configuración aplicable al proveedor y compañía regulada, implementar configuración y verificar su funcionamiento. Acuerdo de servicio y datos garantizados por el proveedor.
2.4			Acceso al sistema dependiente del tunel de seguridad establecido entre el proveedor y la compañía. Acceso al sistema dependiente de la configuración de compañía regulada	3	1	**3**	3	**9**	Acuerdo del tipo de conexión, determinar la configuración aplicable al proveedor y compañía regulada, implementar configuración y verificar su funcionamiento. Aplicar seguridad para que únicamente sea accesible por el director de IT la configuración de estos parámetros.
2.5	Tiempos de servicio del proveedor ante alta, modificación o baja de servicios delegados no definidos. Retrasos.		Ausencia de un acuerdo de calidad del servicio, entre compañía regulada y el proveedor, que garantice el cumplimiento de los tiempos de servicio del proveedor.	3	1	**3**	3	**9**	Generar, aprobar y firmar de un acuerdo de calidad del servicio, entre compañía regulada y el proveedor, que garantice el cumplimiento de los tiempos de servicio del proveedor.

Riesgos asociados a entornos cloud

Item	Posible modo de fallo	Efectos potenciales del fallo	Causa potenciales del fallo	Criticidad C	Probabilidad L	Clasificación del riesgo RC	Detectabilidad D	IPR	Acción mitigadora del riesgo
3	**Datos**								
3.1	No se dispone de acceso a la información.	Incumplimiento de la integridad de datos. Puede afectar a registros y procesos GxP relevantes.	Acceso a los datos dependiente del servicio del proveedor	3	1	**3**	1	**3**	Generar, aprobar y firmar un acuerdo, entre compañía regulada y el proveedor, que especifique el servicio y datos garantizado por el proveedor tecnológico.
3.2			Acceso a los datos dependiente del servicio de internet de compañía regulada	3	2	**6**	1	**6**	Contratación de dos líneas, con operadores independientes, para el servicio de internet.
3.3			Acceso al sistema dependiente del tunel de seguridad establecido entre el proveedor y la compañía. Acceso al sistema dependiente de la configuración del proveedor	3	1	**3**	1	**3**	Acuerdo del tipo de conexión, determinar la configuración aplicable al proveedor y compañía regulada, implementar configuración y verificar su funcionamiento. Acuerdo de servicio y datos garantizados por el proveedor.
3.4			Acceso al sistema dependiente del tunel de seguridad establecido entre el proveedor y la compañía. Acceso al sistema dependiente de la configuración de compañía regulada	3	1	**3**	1	**3**	Acuerdo del tipo de conexión, determinar la configuración aplicable al proveedor y compañía regulada, implementar configuración y verificar su funcionamiento. Aplicar seguridad para que únicamente sea accesible por el director de IT la configuración de estos parámetros.
3.5	Acceso a la información por parte del proveedor.		Los datos no se encuentran cifrados.	3	2	**6**	3	**18**	Cifrado de datos en movimiento y reposo. Acuerdos de calidad con el proveedor.
3.6	Datos no disponibles.		Ausencia de mantenimiento requerido, copias de seguridad, por parte de compañía regulada.	3	2	**6**	2	**12**	Definir y aprobar las especificaciones técnicas y mantenimiento requeridos para los datos a gestionar en la nube.
3.7			Diseño, configuración y monitorización de copias de seguridad dependientes del proveedor	3	2	**6**	3	**18**	Acuerdo de servicio, datos y mantenimiento garantizados por el proveedor. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor.
3.8			Ausencia de mantenimiento requerido, restauración de datos, por parte de compañía regulada.	3	2	**6**	2	**12**	Definir y aprobar las especificaciones técnicas y mantenimiento requeridos para los datos a gestionar en la nube.
3.9			Diseño, configuración y monitorización de la restauración de datos dependientes del proveedor	3	2	**6**	3	**18**	Acuerdo de servicio, datos y mantenimiento garantizados por el proveedor. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor.
3.10	Modificación o borrado de datos.		Mala práctica en el diseño, configuración y mantenimiento por parte del proveedor.	3	2	**6**	3	**18**	Acuerdo de servicio, datos y mantenimiento garantizados por el proveedor. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor.

Riesgos asociados a entornos cloud

Item	Posible modo de fallo	Efectos potenciales del fallo	Causa potenciales del fallo	Criticidad C	Probabilidad L	Clasificación del riesgo RC	Detectabilidad D	IPR	Acción mitigadora del riesgo
4	Servicios aplicados								
4.1	No cumplimiento de la disponibilidad del servicio	Pérdida de servicio y/o integridad de datos. Puede afectar a registros y gestión del proceso GxP relevantes.	Ausencia de definición del requisito por parte de compañía regulada y posterior acuerdo con el proveedor.	3	2	**6**	1	**6**	Generar, aprobar y firmar un acuerdo, entre compañía regulada y el proveedor, que especifique el servicio y datos garantizado por el proveedor tecnológico.
4.2			Dependencia de las buenas prácticas del proveedor.	3	1	**3**	1	**3**	Acuerdo de servicio, datos y mantenimiento garantizados por el proveedor. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor. Gestión de incidencias y no conformidades.
4.3	No cumplimiento de al política de copias de seguridad y recuperación de datos		Ausencia de definición del requisito por parte de compañía regulada y posterior acuerdo con el proveedor.	3	2	**6**	2	**12**	Definir y aprobar las especificaciones técnicas y mantenimiento requeridos para los datos a gestionar en la nube.
4.4			Dependencia de las buenas prácticas del proveedor.	3	1	**3**	2	**6**	Acuerdo de servicio, datos y mantenimiento garantizados por el proveedor. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor. Realización de simulacros. Gestión de incidencias y no conformidades.
4.5	No cumplimiento de la política de recuperación ante desastres		Ausencia de definición del requisito por parte de compañía regulada y posterior acuerdo con el proveedor.	3	2	**6**	2	**12**	Definir y aprobar las especificaciones técnicas y mantenimiento requeridos para los datos a gestionar en la nube.
4.6			Dependencia de las buenas prácticas del proveedor.	3	2	**6**	2	**12**	Acuerdo de servicio, datos y mantenimiento garantizados por el proveedor. Definición del RTO y RPO. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor. Realización de simulacros. Gestión de incidencias y no conformidades.
4.7	No cumplimiento de los mantenimientos programados		Ausencia de definición del requisito por parte de compañía regulada y posterior acuerdo con el proveedor.	3	2	**6**	3	**18**	Definir y aprobar las especificaciones técnicas y mantenimiento requeridos para los datos a gestionar en la nube.
4.8			Dependencia de las buenas prácticas del proveedor.	3	2	**6**	3	**18**	Acuerdo de servicio, datos y mantenimiento garantizados por el proveedor. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor. Realización de simulacros. Gestión de incidencias y no conformidades.
4.9	No cumplimiento de la exploración de vulnabilidades y pruebas de penetración de terceros.		Ausencia de definición del requisito por parte de compañía regulada y posterior acuerdo con el proveedor.	3	2	**6**	3	**18**	Definir y aprobar las especificaciones técnicas y mantenimiento requeridos para los datos a gestionar en la nube.
4.10			Dependencia de las buenas prácticas del proveedor.	3	2	**6**	3	**18**	Acuerdo de servicio, datos y mantenimiento garantizados por el proveedor. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor. Gestión de incidencias y no conformidades.

OQOTECH
TECH & QUALITY

Riesgos asociados a entornos cloud

Item	Posible modo de fallo	Efectos potenciales del fallo	Causa potenciales del fallo	Criticidad C	Probabilidad L	Clasificación del riesgo RC	Detectabilidad D	IPR	Acción mitigadora del riesgo
4	**Servicios aplicados**								
4.11	No cumplimiento de la gestión de solicitudes de servicios	Pérdida de servicio y/o integridad de datos. Puede afectar a registros y gestión del proceso GxP relevantes.	Ausencia de definición del requisito por parte de compañía regulada y posterior acuerdo con el proveedor.	3	2	**6**	2	**12**	Definir y aprobar las especificaciones técnicas y mantenimiento requeridos para los datos a gestionar en la nube.
4.12			Dependencia de las buenas prácticas del proveedor.	3	1	**3**	2	**6**	Acuerdo de servicio, datos y mantenimiento garantizados por el proveedor. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor. Gestión de incidencias y no conformidades.
4.13	No cumplimiento de la gestión de solicitudes de cambio		Ausencia de definición del requisito por parte de compañía regulada y posterior acuerdo con el proveedor.	3	2	**6**	2	**12**	Definir y aprobar las especificaciones técnicas y mantenimiento requeridos para los datos a gestionar en la nube.
4.14			Dependencia de las buenas prácticas del proveedor.	3	1	**3**	2	**6**	Acuerdo de servicio, datos y mantenimiento garantizados por el proveedor. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor. Gestión de incidencias y no conformidades.
4.15	No cumplimiento de tiempos de reacción		Ausencia de definición del requisito por parte de compañía regulada y posterior acuerdo con el proveedor.	3	2	**6**	2	**12**	Definir y aprobar las especificaciones técnicas y mantenimiento requeridos para los datos a gestionar en la nube.
4.16			Dependencia de las buenas prácticas del proveedor.	3	1	**3**	2	**6**	Acuerdo de servicio, datos y mantenimiento garantizados por el proveedor. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor. Gestión de incidencias y no conformidades.
4.17	No disponibilidad del panel de monitorización y métricas de los servicios delegados		Ausencia de definición del requisito por parte de compañía regulada y posterior acuerdo con el proveedor.	3	2	**6**	2	**12**	Definir y aprobar las especificaciones técnicas y mantenimiento requeridos para los datos a gestionar en la nube.
4.18			Dependencia de las buenas prácticas del proveedor.	3	1	**3**	2	**6**	Acuerdo de servicio, datos y mantenimiento garantizados por el proveedor. Acceso a un panel de monitozación o informes del servicio delegado. Sistema de calidad y certificaciones del proveedor. Gestión de incidencias y no conformidades.

OQOTECH
TECH & QUALITY

Riesgos asociados a entornos cloud

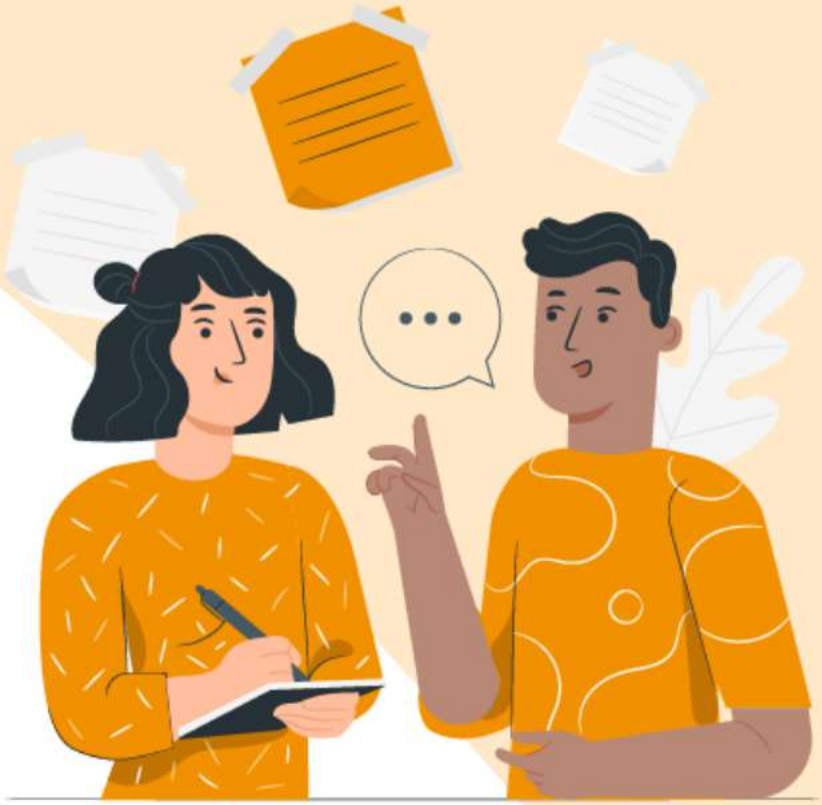
Item	Posible modo de fallo	Efectos potenciales del fallo	Causa potenciales del fallo	Criticidad C	Probabilidad L	Clasificación del riesgo RC	Detectabilidad D	IPR	Acción mitigadora del riesgo
4	**Servicios aplicados**								
5	**Personal**								
5.1	El personal es responsabilidad del proveedor. Falta de supervisión.	Pérdida de servicio y/o integridad de datos. Puede afectar a registros y gestión del proceso GxP relevantes.	Protocolos de gestión del proveedor que no cubren las necesidades de compañía regulada.	3	2	**6**	3	**18**	Sistema de calidad y certificaciones del proveedor.
5.2	Personal no formado.		Personal no cualificado	3	2	**6**	3	**18**	Sistema de calidad y certificaciones del proveedor.
5.3	No registro de actividades críticas		Protocolos de gestión del proveedor que no cubren las necesidades de compañía regulada.	3	2	**6**	3	**18**	Sistema de calidad y certificaciones del proveedor. Acceso a un panel de monitozación o informes del servicio delegado.
6	**Sistema de calidad**								
6.1	Enfoque de cualificación y validación diferente	Pérdida de servicio y/o integridad de datos. Puede afectar a registros y gestión del proceso GxP relevantes.	El alcance de los procedimientos no contemplan este modelo de servicio.	3	1	**3**	2	**6**	Revisión del alcance de los procedimientos.
7	**Normativa**								
7.1	Producto no cumple con normativa aplicable	Resultados no fiables	Diseño incorrecto del producto	3	2	**6**	1	**6**	Determinación inicial de los requerimientos regulatorios del producto para el uso previsto.
8	**Documentación**								
8.1	Deficiencias en la documentación	No cumple con los requerimientos de compañía regulada	Protocolos de gestión del proveedor que no cubren las necesidades de compañía regulada.	2	3	**6**	1	**6**	Establecer conjuntamente criterios de aceptación.
8.2		Documentación mal cumplimentada o incorrecta	Personal no cualificado	3	2	**6**	1	**6**	Revisión documentación por parte de compañía regulada. Solicitud formación al personal en buenas prácticas de documentación.
9	**Reclamaciones y defectos de calidad**								
9.1	Incorrecta gestión reclamaciones o desviaciones	Retraso en la respuesta	Personal insuficiente	3	2	**6**	1	**6**	Acordar tiempos máximos de respuesta.
9.2.1		Insuficiente investigación	Personal no cualificado	3	2	**6**	1	**6**	Inclusión de la gestión de cambios. Solicitud evidencias capacitación del personal que interviene en el proceso. Aprobación final del registro por compañía regulada.
9.2.2			Proceso de investigación no estandarizado	3	2	**6**	1	**6**	Formulario de reclamaciones.
9.2.3			Protocolos de gestión del proveedor que no cubren las necesidades de compañía regulada.	3	2	**6**	1	**6**	Aprobación del formulario de gestión de desviaciones, con probabilidad de uso de formulario propio de compañía regulada.

OQOTECH
TECH & QUALITY

¡Gracias!

Grupo de LinkedIn

OQOTECH - Validación de Sistemas informatizados e Integridad de Datos



https://www.linkedin.com/groups/8902028/

https://www.linkedin.com/company/oqotech

¿Quieres dejar tus dudas para el siguiente curso?

- En el curso *"Caso Práctico: Recopilación de preguntas y respuestas"* responderemos dudas recopiladas que nos hayáis enviado.

- Puedes enviarnos tus preguntas en el siguiente enlace:

https://www.oqotech.com/cursos/caso-practico-recopilacion-de-preguntas-y-respuestas/

PODCAST - OQOTECH EDUCA

OQOTECH

TECH & QUALITY

EDUCA

PODCAST

WWW.OQOTECH.COM

¿Te ha gustado la clase?

Ayúdanos a poder seguir haciendo
estos contenidos totalmente gratuitos.

¡Comparte y comenta tu experiencia con tus contactos en las redes e invítalos a los cursos!

www.oqotech.com