Prof. Paula León A.

Actividad 07. Análisis funcional de riesgos

Nombre(s):_____ **No. Lista** _____ **Fecha:** _____
(Apellido paterno. Apellido materno. Nombre(s) **Grupo:** _____

Objetivo: Conocer concepto de **Buenas Prácticas** (de Ingeniería) y su relación con el **análisis de riesgos** en el desarrollo de la ingeniería de software.

- **Validación de Sistemas Informatizados** Alcanzar y mantener el cumplimiento aplicable a regulaciones BxP/GMP.
  - Adopción de los principios, enfoques y actividades del ciclo de vida en el marco de los planes y reportes de validación
  - Aplicación de los controles operacionales apropiados a lo largo de la vida del sistema
- **Daño:** Pérdida de la calidad del producto o disponibilidad.
- **Peligro:** Fuente potencial de daño.
- **Riesgo:** Combinación de la probabilidad de que ocurra un daño y la gravedad de dicho daño.
- **Severidad:** Una medida de las posibles consecuencias de un peligro.

El **riesgo** se puede definir como la **posibilidad de que no se obtengan los resultados esperados**. Un resultado no deseado puede ser positivo o negativo. Si se espera implementar un sistema informatizado en 180 días y se termina en 290 días, ese no era el resultado esperado aunque sea por un pequeño margen de tiempo. Cuando se hace referencia a riego en cualquier ámbito, siempre se habla de resultados negativos o no deseados distintos al resultado esperado.

En un proyecto de TI los riesgos que pueden presentarse pueden relacionarse con:

- Tiempo de ejecución
- Presupuesto
- Personal
- Funcionamiento del hardware
- Funcionamiento del software
- Seguridad
- Entre otros factores.

Las etapas de identificación, análisis y medidas para evitar y mitigar los riesgos son la base de lo que se conoce como **administración de riesgos** en proyectos de TI. Dichos riesgos se clasifican de la siguiente forma:

- **Amenaza**. Esta se entiende como una condición del entorno sistema de información o informatizado (persona, equipo, suceso o idea) que ante cierta circunstancia pudiera darse lugar a crearse una violación de seguridad (incumplimiento de alguno de los aspectos mencionados) que afecte alguna parte de la TI de la compañía. Cuando se ha determinado que una amenaza puede afectar un activo hay que estimar cuán vulnerable es éste en dos sentidos: **degradación**, que significa el grado que resultaría perjudicado el activo y la **frecuencia**, que se refiere al grado en que se materializa la amenaza.

- **Vulnerabilidad.** Hecho o actividad que permite concretar una amenaza. Se es vulnerable en la medida que no hay suficiente protección para evitar por completo que llegue a suceder una amenaza. Hay ataques intencionados y no intencionados.

Hay ataques intencionados y no intencionados.

- **Ataques no intencionados:** Es cuando un hecho simplemente sucede pero perjudica al proyecto o a la compañía, por ejemplo: inundación, falta de suministro de energía eléctrica por tiempo prolongado, falla en el satélite de comunicación, errores o equivocaciones de usuarios, inadecuado registro de actividades, difusión no intencional de software dañino o de virus y espías, entre otros.
- **Ataques intencionados.** Acceso no autorizado al sistema en el que el atacante consigue acceso a los recursos del sistema sin previa autorización.

1. Gestión del riesgo

La gestión del riesgo es una de las tareas centrales para un administrador de proyecto. La gestión del riesgo implica anticipar riesgos que pudieran alterar el calendario del proyecto o la calidad del software a entregar, y posteriormente tomar acciones para evitar dichos riesgos. Podemos considerar un riesgo como algo que es preferible que no ocurra. Los riesgos pueden amenazar el proyecto, el software que se desarrolla o a la organización. Por lo tanto, existen tres categorías relacionadas de riesgo:

1. **Riesgos del proyecto**. Los riesgos que alteran el calendario o los recursos del proyecto. Un ejemplo de riesgo de proyecto es la renuncia de un diseñador experimentado. Encontrar un diseñador de reemplazo con habilidades y experiencia adecuadas puede demorar mucho tiempo y, en consecuencia, el diseño del software tardará más tiempo en completarse.
2. **Riesgos del producto**. Los riesgos que afectan la calidad o el rendimiento del software a desarrollar. Un ejemplo de riesgo de producto es la falla que presenta un componente que se adquirió al no desempeñarse como se esperaba. Esto puede afectar el rendimiento global del sistema, de modo que es más lento de lo previsto.
3. **Riesgos empresariales**. Riesgos que afectan a la organización que desarrolla o adquiere el software. Por ejemplo, un competidor que introduce un nuevo producto es un riesgo empresarial. La introducción de un producto competitivo puede significar que las suposiciones hechas sobre las ventas de los productos de software existentes sean excesivamente optimistas.

Desde luego, estos tipos de riesgos se traslapan. Si un programador experimentado abandona un proyecto, esto puede ser un riesgo del proyecto porque, incluso si se sustituye de manera inmediata, el calendario se alterará. En consecuencia, la entrega del sistema podría demorarse. La salida de un miembro del equipo también puede ser un riesgo del producto, porque un sustituto tal vez no sea tan experimentado y, por lo tanto, podría cometer errores de programación. Finalmente, puede ser un riesgo empresarial, porque la experiencia de dicho programador es vital para obtener nuevos contratos.

2. Identificación del riesgo

La identificación del riesgo es la primera etapa del proceso de gestión del riesgo. Se ocupa de identificar los riesgos que pudieran plantear una mayor amenaza al proceso de ingeniería de software, al software a desarrollar, o a la organización que lo desarrolla. La identificación del riesgo puede ser un proceso de equipo en el que este último se reúne para pensar en posibles riesgos. O bien, el administrador del proyecto, con base en su experiencia, identifica los riesgos más probables o críticos.

Como punto de partida para la identificación del riesgo, se recomienda utilizar una lista de verificación de diferentes tipos de riesgo. Existen al menos seis tipos de riesgos que pueden incluirse en una lista de verificación:

1. Riesgos tecnológicos. Se derivan de las tecnologías de software o hardware usadas para desarrollar el sistema.
2. Riesgos personales. Se asocian con las personas en el equipo de desarrollo.
3. Riesgos organizacionales. Se derivan del entorno organizacional donde se desarrolla el software.
4. Riesgos de herramientas. Resultan de las herramientas de software y otro software de soporte que se usa para desarrollar el sistema.
5. Riesgos de requerimientos. Proceden de cambios a los requerimientos del cliente y del proceso de gestionarlos.
6. Riesgos de estimación. Surgen de las estimaciones administrativas de los recursos requeridos para construir el sistema.

La figura siguiente brinda algunos ejemplos de posibles riesgos en cada una de estas categorías. Al concluir el proceso de identificación de riesgos, se tendrá una larga lista de eventualidades que podrían ocurrir y afectar al producto, al proceso y a la empresa. Entonces se necesita reducir esta lista a un tamaño razonable. Si existen demasiados riesgos, será prácticamente imposible seguir la huella de todos ellos.

Tipo de riesgo	Riesgos posibles
Tecnológico	La base de datos que se usa en el sistema no puede procesar tantas transacciones por segundo como se esperaba. (1) Los componentes de software de reutilización contienen defectos que hacen que no puedan reutilizarse como se planeó. (2)
Personal	Es imposible reclutar personal con las habilidades requeridas. (3) El personal clave está enfermo e indispuesto en momentos críticos. (4) No está disponible la capacitación requerida para el personal. (5)
De organización	La organización se reestructura de modo que diferentes administraciones son responsables del proyecto. (6) Problemas financieros de la organización fuerzan reducciones en el presupuesto del proyecto. (7)
Herramientas	El código elaborado por las herramientas de generación de código de software es ineficiente. (8) Las herramientas de software no pueden trabajar en una forma integrada. (9)
Requerimientos	Se proponen cambios a los requerimientos que demandan mayor trabajo de rediseño. (10) Los clientes no entienden las repercusiones de los cambios a los requerimientos. (11)
Estimación	Se subestima el tiempo requerido para desarrollar el software. (12) Se subestima la tasa de reparación de defectos. (13) Se subestima el tamaño del software. (14)

Ejemplos de diferentes tipos de riesgos

3. Análisis de riesgo

Durante el proceso de análisis de riesgos, hay que considerar cada riesgo identificado y realizar un juicio acerca de la probabilidad y gravedad de dicho riesgo. No hay una forma sencilla de hacer esto. Usted debe apoyarse en su propio juicio y en la experiencia obtenida en los proyectos anteriores y los problemas que surgieron en ellos. No es posible hacer valoraciones precisas y numéricas de la probabilidad y gravedad de cada riesgo. En vez de ello, habrá que asignar el riesgo a una de ciertas bandas:

1. La probabilidad del riesgo puede valorarse como muy baja (< 10%), baja (del 10 al 25%), moderada (del 25 al 50%), alta (del 50 al 75%) o muy alta (> 75%).
2. Los efectos del riesgo pueden estimarse como catastróficos (amenazan la supervivencia del proyecto), graves (causarían grandes demoras), tolerables (demoras dentro de la contingencia permitida) o insignificantes.

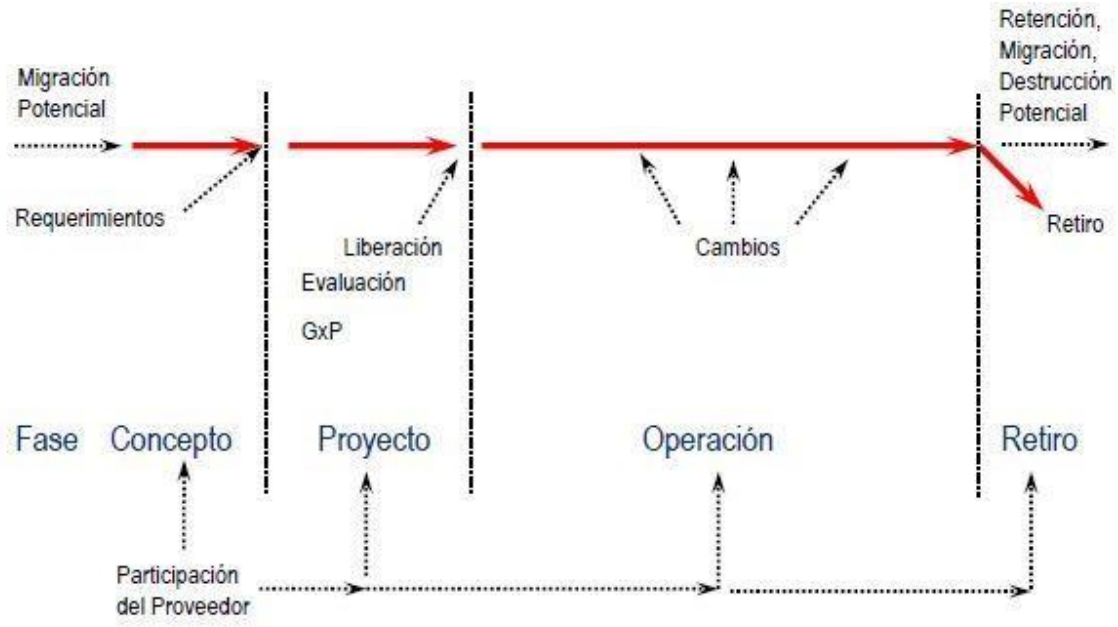
Luego hay que tabular los resultados de este proceso de análisis mediante una tabla clasificada de acuerdo con la gravedad del riesgo.

Riesgo	Probabilidad	Efectos
Problemas financieros de la organización fuerzan reducciones en el presupuesto del proyecto. (7)	Baja	Catastrófico
Es imposible reclutar personal con las habilidades requeridas. (3)	Alta	Catastrófico
El personal clave está enfermo e indispuesto en momentos críticos. (4)	Moderada	Grave
Los componentes de software de reutilización contienen defectos que hacen que no puedan reutilizarse como se planeó. (2)	Moderada	Grave
Se proponen cambios a los requerimientos que demandan mayor trabajo de rediseño. (10)	Moderada	Grave
La organización se reestructura de modo que diferentes administraciones son responsables del proyecto. (6)	Alta	Grave
La base de datos que se usa en el sistema no puede procesar tantas transacciones por segundo como se esperaba. (1)	Moderada	Grave
Se subestima el tiempo requerido para desarrollar el software. (12)	Alta	Grave
Las herramientas de software no pueden trabajar en una forma integrada. (9)	Alta	Tolerable
Los clientes no entienden las repercusiones de los cambios a los requerimientos. (11)	Moderada	Tolerable
No está disponible la capacitación requerida para el personal. (5)	Moderada	Tolerable
Se subestima la tasa de reparación de defecto. (13)	Moderada	Tolerable
Se subestima el tamaño del software. (14)	Alta	Tolerable
El código elaborado por las herramientas de generación de código de software es ineficiente. (8)	Moderada	Insignificante

Tipos de riesgos y ejemplos

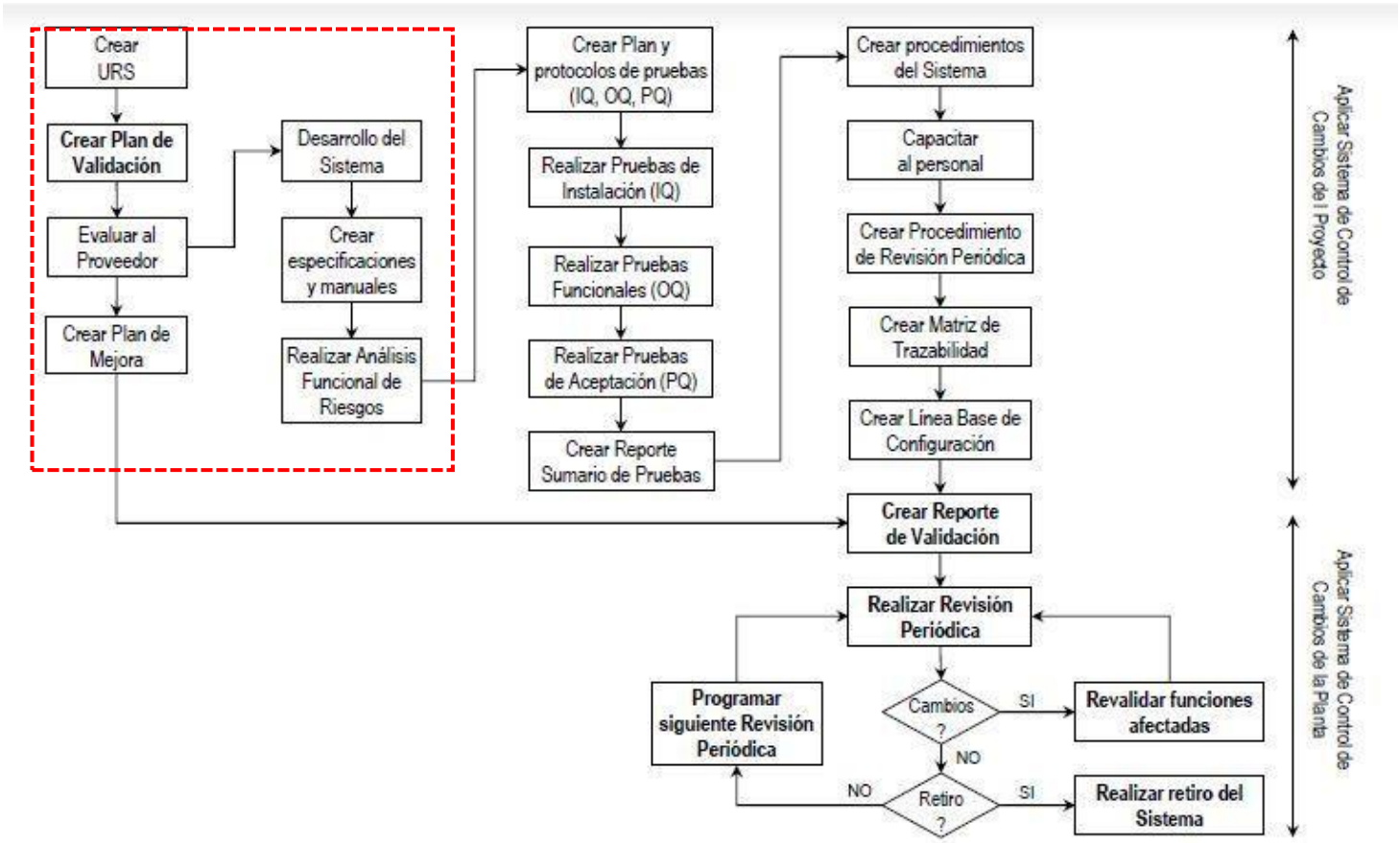
4. Relación del ciclo de vida de un sistema Informatizado y el proveedor (Firma de Ing. Sw)

Abarca todas las actividades, desde el concepto inicial hasta el retiro.



- El proveedor debe proveer conocimiento, experiencia, documentación, y servicios a través del ciclo de vida.

5. ¿Dónde estamos?



6. Administración del riesgo de calidad. Categorías de Software

Categoría 1 – Software de infraestructura

- **Software comercial en capas**
  - Hojas de cálculo
  - Herramientas de programación
  - Bases de datos
- **Software de infraestructura**
  - Software de seguridad
    - Software de monitoreo de red


Categoría 2. Firmware

No se utiliza en GAMP 5

Es un sistema que se desarrolla para establecer un **"Firme"** lazo entre el Hardware y el Software, de ahí proviene su denominación, la cual fue empleada por primera vez en los años 60 para señalar a un conjunto de normas insertado en una tarjeta electrónica para que un aparato más grande ejecutará una función automática.

Los **Firmwares** de los equipos electrónicos son actualizados no para agregar nuevas opciones y alternativas como lo hacen el software de las computadoras, lo hacen para reparar o mejorar la conexión de las funcionalidades del hardware con las indicadas en la ley o **norma** creada. No podemos dejar de mencionar que muchos equipos electrónicos mejoran dentro del Firmware los protocolos de seguridad, por ejemplo: **el firmware de un reproductor de DVD o Blue Ray** actualiza sus protocolos de seguridad para evitar que los discos "piratas" puedan ser reproducidos de una manera eficiente.

Categoría 3 – Productos no configurados

- Sistemas que no se pueden configurar
- Sistemas que realizan configuración determinada

Impresora

Categoría 4 – Software configurado

- Software configurable con interfases
- Módulos de software definidos

ERP- Enterprise Resource Planning

Categoría 5 – Aplicaciones personalizadas

- Software desarrollado para cumplir con los requerimientos específicos de la compañía.

Nombre(s):_____ **No. Lista** _____ **Fecha:** _____
(Apellido paterno. Apellido materno. Nombre(s) **Grupo:** _____

Parte A

RESPONDE

1. Las **actividades del ciclo de vida del sistema informatizado relacionadas con el proveedor** abarcan desde:

2. ¿Qué es la **administración de riesgos**?

3. De acuerdo a la administración del riesgo de calidad categorías de software, **las hojas de cálculo, herramientas de programación y bases de datos** son **categoría**:

4. Defina lo que son **riesgo, amenaza y vulnerabilidad.**

Riesgo	
Amenaza	
Vulnerabilidad	

5. Defina d**año, peligro, riesgo y severidad.**

Daño	
Peligro	
Severidad	

6. De acuerdo a la clasificación de riesgo de calidad en software una **aplicación personalizada** pertenece a la categoría número….

7. **Completa** la Tabla siguiente. Cuando una compañía ha determinado contratar a un proveedor de servicios de ingeniería de software, inicia por (Mencione cuáles son los **primero pasos antes** de llegar al **Análisis Funcional de Riesgos**).

1.	Crear URS	**4.**	
2.		**5.**	
3.		**6.**	

Enfoque práctico

Relaciona **Riesgo-Consecuencia**. **(Color amarillo)**. Consulta la Tabla de Resultados del Análisis de Riesgo para la compañía farmacéutica **CMS,** página 10 inciso a-h

Tabla de Resultados Análisis de Riesgo Actualización Sistema de Control

						EVALUACION INICIAL						RE-EVALUACION			
ASPECTOS PRINCIPALES	Item N°.	Escenario	Riesgo	Consecuencia	Controles (ingenieria y/o administrativos)	G	P	D	R	Recomendaciones	Fecha compromiso y responsables	G	P	D	R
	1	Definición de Requerimientos de Usuario (URS).	Requerimientos de Usuario descritos con un nivel de detalle muy básico.		PNT14-05, experiencia previa en la generación de URS de otros equipos / proyectos.	4	2	4	32	La elaboración de un PNT (14-09 de **CMS**) y capacitación sobre el mismo, referente a la creación de URS's, definir comité / equipo de personas involucradas en la generación de un URS. Consultar fuentes externas de información.	02/09/2016 (R Hidalgo / Rosa H. Luz)	4	1	1	4
	2	Evaluación y selección del proveedor de software.	El proveedor no tiene un sistema de calidad para desarrollo de software y requerimientos documentales.		PNT asociado a la evaluación de proveedores, solicitud de referencias comerciales a terceros.	4	2	3	24	Revisión, actualización y cumplimiento del PNT existente sobre evaluación de proveedores, con el propósito de completar la parte de proveedores de software. Evaluación del proveedor de acuerdo al PNT06-16.	29/08/2016 (R Hidalgo / QA)	4	1	1	4
	3	Adquisición de software/hardware.	El Hardware no tiene la capacidad requerida / incompatibilidad del hardware con el sofware.		Documentos de Especificación de Hardware y Software, apego a las recomendaciones del fabricante del software.	2	1	1	2	NA	NA	4	1	1	4
	4		No se tiene en tiempo y forma el hardware y software requerido para la nueva plataforma		Cronograma del proyecto, comunicación a Dirección General de Planta y el Corporativo sobre el avance del mismo.	3	3	1	9	Establecer una fecha límite para la adquisición de hardware a través de TI **CMS**, en caso se rebasar dicha fecha realizar la compra a través de un proveedor local (incluye HMI's). Se propone establecer un documento llamado Project Charter como herraminenta prinicpal para administración del proyecto.	02/09/2016 (R Hidalgo)	4	1	1	4
	5	Desarrollo del sistema.	El Integrador no tiene estándares de programación adecuados para la intefaz de usuario (navegación de pantallas, códigos de colores de los estados de equipos y alarmas)		PNT asociado a la evaluación de proveedores, solicitud de referencias comerciales a terceros, y manual de operación existente como standard actual de **CMS** para la generación de nuevas pantallas, y revisiones de diseño (formalizar en algún documento dichas revisiones).	4	1	1	4	Revisión, actualización y cumplimiento del PNT existente sobre evaluación de proveedors, con el propósito de completar la parte de proveedores de software. Evaluación del proveedor de acuerdo al PNT06-16.	29/08/2016 (R Hidalgo / QA)	4	1	1	4
	6	Creación de Documentación del sistema (FS, DS y manuales).	El nivel de detalle de las especificaciones y manuales es muy pobre		PNT asociado a la evaluación de proveedores, Protocolos de Calificación de las etapas IQ y OQ del sistema.	4	2	2	16	Establecer revisiones de diseño en el cronograma del proyecto.	14/09/2016 (Integrador / R Hidalgo)	1	1	1	1
	7	Pruebas de Integración del sistema.	El proveedor no realiza pruebas de integración.		No existen controles	3	3	4	36	Incluir en el procedimiento actual de calificaciones la solicitud de un informe de pruebas FAT.	14/09/2016 (Integrador / R Hidalgo)	4	1	1	4
	8	Instalación del Sistema.	Hardware / software mal configurado o instalado.		PNT de evaluación de proveedores, referencias comerciales a terceros.	3	2	3	18	Revisión, actualización y cumplimiento del PNT existente sobre evaluación de proveedors, con el propósito de completar la parte de proveedores de software. Evaluación del proveedor de acuerdo al PNT06-16. Solicitar por escrito la experiencia que se tiene en la configuración del software de control a utilizar, y realizar auditoria presencial sobre algún sistema previamente instalado en alguna otra emrpesa.	14/09/2016 (R Hidalgo)	3	1	1	3

Item #	Riesgo	Consecuencia
1	Requerimientos de Usuario descritos con un nivel de detalle muy básico.	
2	El proveedor no tiene un sistema de calidad para desarrollo de software y requerimientos documentales.	
3	El hardware no tiene la capacidad requerida / incompatibilidad del hardware con el software.	
4	No se tiene en tiempo y forma el hardware y software requerido para la nueva plataforma	
5	El Integrador no tiene estándares de programación adecuados para la interfaz de usuario (navegación de pantallas, códigos de colores de los estados de equipos y alarmas)	
6	El nivel de detalle de las especificaciones y manuales es muy pobre	
7	El proveedor no realiza pruebas de integración.	
8	Hardware / software mal configurado o instalado.	

Retraso en la liberación del sistema validado, con el consecuente retraso en el programa de producción. (a)
Sistema instalado en planta con errores que surjan durante la etapa de validación. (b)
Sistema instalado en planta con errores que surjan durante la etapa de validación, retraso en la implementación e incumplimiento regulatorio. (c)
Desarrollo de un sistema que no cumple con la funcionalidad requerida por CMS, desviaciones de calidad, incumplimiento del plan de producción, incumplimiento en las fechas de entrega de los productos e impacto en el plan de compras (d)
Sistema entregado con errores de programación / documentación críticos. Si la falla / error se presenta después de la validación, el impacto es directo a la calidad del producto y fechas de entrega de los mismos. Incumplimiento regulatorio de las normas vigentes. (e)
Interfaz de usuario confusa que dificulte la operación del sistema y provoque errores de los operadores, impacto a la calidad del producto. (f)
Retraso en la liberación del sistema validado, incumplimiento regulatorio, e incumplimiento con las expectativas del cliente. (g)
Diseño inadecuado de las pruebas, de tal manera que no se detecten durante la validación, errores de configuración o programación y sean detectados durante el uso productivo del sistema. Impacto en la calidad del producto. (h)

Equipo #	Integrantes: