Hospital Universitario Infanta Cristina

SaludMadrid

Red H s H Hospitales sin Humo

Procedimiento de Contingencias

Ámbito de Laboratorio

Hospital Universitario
Infanta Cristina

Índice

CONTROL DE VERSIONES:

Ver	Fecha	Descripción	Autor(es) Fecha	Aprobado Fecha
1.0	Septiembre 2013	Versión Inicial	Jaime Gil Fombellida	
2.0	Noviembre 2016	Actualización	Jaime Gil Fombellida	
3.0	Septiembre 2020	Actualización	Jaime Gil Fombellida	

1. Introducción

1.1. Objetivos

Los objetivos del presente informe son:

- Analizar el estado de situación del ámbito de Laboratorio del Hospital Universitario Infanta Cristina ante una posible Contingencia en los Sistemas de Información.
- Recomendar las acciones necesarias, en caso en que proceda, para la gestión de posibles contingencias en los Sistemas de Información del ámbito de Laboratorio del Hospital Universitario Infanta Cristina.

1.2. Alcance

El alcance definido para la realización del presente informe son los ***Sistemas de Información así como los diferentes departamentos que integran el ámbito de Laboratorio del Hospital Universitario Infanta Cristina.***

Quedan fuera del alcance de este análisis otros aspectos importantes que deben tenerse en cuenta de cara a la continuidad de negocio, como contingencias de recursos humanos, instalaciones, etc.

El presente informe analiza la criticidad de los Sistemas de Información del Ámbito de Laboratorio del Hospital Universitario Infanta Cristina sito en Parla (Madrid).

La información del Servicio se ha obtenido de los responsables de distintas Áreas implicadas a los que les puede afectar el presente Plan de contingencia:

Área	Área	Área
Laboratorio	Informática y SSII	

1.3. Conceptos básicos

El desarrollo de este análisis toma como referencia el modelo de Gestión de la Continuidad de Negocio plasmado en las normas:

- BS25999-1 “Code of practice for business continuity management”
- BS25999-2 “Business continuity management - Part 2: Specification”
- BS25777, “Information and communications technology continuity management - Code of Practice”

Las actividades del presente proyecto corresponderían a parte de las tareas contempladas en dichos estándares, dentro de las fases de “Comprender la organización” y “Determinar las opciones de GCN” (GCN: Gestión de la Continuidad de Negocio)

Para la definición de las recomendaciones propias de un Plan de Continuidad de Negocio es necesaria la elaboración de un BIA (Business Impact Analysis) o ***Análisis de Impacto en el Negocio***, que tiene como objetivo determinar cuáles serían los efectos sobre una organización de la interrupción de una determinada actividad. Además, el BIA determina cuál debería ser el nivel mínimo de servicio apropiado y con qué recursos podría restaurarse dicho nivel mínimo.

En el caso que nos ocupa se va a realizar una ***aproximación a un BIA***, puesto que dado el alcance y la temporalidad de este estudio, no se realizará un Análisis de Impacto de Negocio exhaustivo y completo de toda la organización.

Una de las consecuencias directas de la aplicación de estos conceptos es conocer los **RTOs, RPOs y MTDs** objetivos de tiempo y de punto de recuperación de los sistemas de información objeto del alcance descrito anteriormente. O lo que es lo mismo:

- RTO (Recovery Point Objective) significa ***saber cuánto tiempo se puede tardar en recuperar un sistema de información***
- *RPO (*Recovery Point Objective) significa ***cuántos datos es admisible perder a consecuencia de un incidente:***
- *MTD (*Maximum Torelable Downtime*)* significa ***el tiempo máximo de caída de un proceso sin que se produzcan efectos desastrosos***

Es importante que la organización tenga claro qué se entiende exactamente por RTO, ya que negocio puede tener una visión concreta (tiempo que transcurre entre que se produce un incidente y se recupera la actividad de negocio), mientras que TI puede pensar en unos plazos diferentes (tiempo transcurrido entre que se autoriza el arranque de la solución de contingencia hasta que ésta es técnicamente operativa).

2. Análisis de Servicios: Caracterización

2.1. Descripción del Servicio

2.1.1 El alcance que nos ocupa es el Ámbito de Laboratorio del Hospital Universitario Infanta Cristina, analizando los procesos que se llevan a cabo en el servicio podremos concluir con los mecanismos alternativos a llevar a cabo en caso de contingencia de los Sistemas de Información.

2.1.2 Laboratorios

Las peticiones de pruebas analíticas al servicio de Laboratorio se realizan desde SELENE y llegan automáticamente al programa SERVOLAB que es el programa con el que se gestionan y se informan las pruebas analíticas.

Una vez realizadas estas pruebas, el resultado de la analítica llega automáticamente a SELENE

2.2. Sistemas

Nombre	Servicio	Área	Criticidad	RTO	RPO	MTD
SELENE	Sistema de información clínica (HIS) del Hospital	Admisión Laboratorio Consultas Etc.	ALTA	3h	30min	24h
SERBOLAB	Sistema de gestión del laboratorio de análisis clínicos,	Laboratorios	ALTA	3h	30min	24h
OPENLINK	Servicio de Mensajería HL7	Integraciones	ALTA	3h	30min	24h

- RTO (Recovery Point Objective) significa ***saber cuánto tiempo se puede tardar en recuperar un sistema de información***
- *RPO (*Recovery Point Objective) significa ***cuántos datos es admisible perder a consecuencia de un incidente:***
- *MTD (*Maximum Torelable Downtime*)* significa ***el tiempo máximo de caída de un proceso sin que se produzcan efectos desastrosos***

2.3. Activos

En el Ámbito de Laboratorio se han detectado los siguientes activos que intervienen en los sistemas de información dedicados al Ámbito de Laboratorio:

- 11 equipos

- 2 impresoras láser

- 1 impresoras etiquetas

2.4. Requerimientos

Este apartado persigue el objetivo de identificar el RTO, RPO y MTD más ajustado posible.

Identificados los Sistemas de Información que soportan el Ámbito de Laboratorio del Infanta Cristina, se estudia y asigna un nivel de impacto en el Servicio en el caso de contingencia en cada uno de los sistemas.

Se ha utilizado la siguiente escala de colores:

BAJO	MEDIO	ALTO	MUY ALTO

CRITICIDAD DE LOS SISTEMAS DE INFORMACIÓN

Sistema	0h	2h	4h	8h	12h	24h
SELENE						
OPENLINK						
SERVOLAB						
TOTALES						

Como conclusión con el fin de mitigar el riesgo de un impacto alto, se debería definir un RTO (tiempo de recuperación) de 2 horas, que debería servir como argumento para habilitar un sistema de recuperación de los sistemas prácticamente instantáneo.

En las entrevistas realizadas se ha identificado que la pérdida de información máxima asumible podría ser como es actualmente de 24 horas, ya que se realiza una copia de seguridad diaria, lo que define nuestro RPO, punto de recuperación.

En los siguientes puntos del documento se abordaran los procedimientos a llevar a cabo en caso de contingencia de cada uno de los sistemas. Además de estos, que afectan a las áreas operativas del Ámbito de Laboratorio, el Área de Informática deberá como área de apoyo transversal disponer de los procedimientos necesarios para la recuperación de cada uno de los sistemas a los que da soporte.

3. Problemas derivados de la caída de uno/varios sistemas en Laboratorio

A continuación detallamos los problemas que pueden llegar a sufrir los usuarios derivados de la caída de todos o de algún sistema de información en el área de Laboratorio.

AREAS y USUARIOS AFECTADOS por los SISTEMAS DE INFORMACIÓN

- Laboratorio Facultativos:
    - Petición/Resultados pruebas laboratorio: SELENE – SERVOLAB
- Laboratorio enfermeras / auxiliares:
    - Impresión etiquetas laboratorio: SELENE - SERVOLAB

4. Activación plan de contingencia y medidas a tomar

El proceso de activación del plan de contingencia de los Sistemas de Información del Ámbito de Laboratorio del Infanta Cristina es prácticamente el mismo, sea cual sea el sistema de información que esté fallando. Es decir, da igual cual sea el sistema de información de Laboratorio afectado el proceso para activar el plan de contingencia será el mismo.

Una vez detectada la necesidad de activar el plan de contingencia habrá que ver cuales son los sistemas y áreas afectados para ver el alcance del problema y activar las partes del plan de contingencia necesarias

Estrategia de Contingencia para los sistemas de información del Ámbito de Laboratorio del Hospital Universitario Infanta Cristina			
Afectados:	Personal de Laboratorio		
Autorizador:	Gerente / Jefe de Hospital / Jefe de Informática y SSII		
Pasos a seguir			
Nº	**Descripción**	**Acciones**	**Responsable**
1	Detección	Se detecta incidencia con desde cualquier equipo informático de Laboratorio	Usuario afectado
2	Notificación	Ponerse en contacto con el CESUS a través del teléfono de contacto correspondiente. (333333) y solicitar el número de incidencia correspondiente	Usuario afectado
3	Comprobación	CESUS realiza las comprobaciones pertinentes in-situ o conectándose en remoto.	Soporte CESUS
3.1	Incidencia solucionada al momento	Cesus soluciona la incidencia al momento y se cierra dicha incidencia una vez verificada con el usuario. **NO se activa plan contingencia**	Soporte CESUS / Usuario afectado
3.2	Incidencia no solucionada al momento de nivel no crítico	Cesus al no poder solucionar la incidencia en el momento, la pasa a los distintos proveedores afectados para que solucione en los tiempos establecidos dicha incidencia. **NO se activa plan contingencia**	Soporte CESUS
3.3	Incidencia no solucionada al momento de nivel crítico	Cesus detecta que la incidencia es grave y avisa al Jefe de Informática / Jefe de Hospital el alcance de la incidencia. **Se debería activar el plan contingencia**	Soporte CESUS
4	Decisión de activación Plan de Contingencia	Por parte del Gerente o del Jefe de hospital se decide activar el Plan de contingencia para el área o áreas afectadas	Gerente / Jefe de Hospital
5	Elección de las partes a activar dentro del plan de contingencia	Según los sistemas afectados se elegirán los partes del plan de contingencia a activar	Gerente / Jefe de Hospital

A continuación se detalla los problemas derivados de la caída de cada uno de los sistemas de información así como las medidas a tomar cuando se activa el plan de contingencia.

4.1. Plan de contingencia SELENE

PROBLEMAS DERIVADOS DE LA CAIDA DE SELENE		
SISTEMA	**PROBLEMAS**	**MEDIDAS**
	- Imposibilidad de petición / resultados pruebas laboratorio: SELENE - SERVOLAB	Petición en papel y traslado de dicha petición al servicio de laboratorio. . Las plantillas están en Z:\Directorio General\Plan de contingencia\laboratorio. Cuando el resultado de la prueba esté completo deberá avisarse a la urgencia para que sigan tratando al paciente

4.2. Plan de contingencia SERVOLAB

PROBLEMAS DERIVADOS DE LA CAIDA DE SERVOLAB		
SISTEMA	**PROBLEMAS**	**MEDIDAS**
	Petición pruebas laboratorio: SELENE – SERVOLAB	Si SERVOLAB está caído las peticiones podrán hacerse en SELENE pero habrá que imprimir la petición y llegarla en mano al servicio de Laboratorio.
ENFERMERAS AUXILIARES	Impresión de etiquetas de laboratorio	Si SERVOLAB no funciona no podrán imprimirse las etiquetas de laboratorio

4.3. Plan de contingencia OPENLINK

PROBLEMAS DERIVADOS DE LA CAIDA DE ALERT (TRIAJE)		
SISTEMA	**PROBLEMAS**	**MEDIDAS**
TODOS	No integración entre aplicaciones, con lo cual no viajan las peticiones, datos administrativos, etc. entre aplicaciones	Según las integraciones que no funcionen deberán activarse los planes de contingencia anteriores

5. Estrategia y diseño de procedimientos de recuperación contingencias

En este punto se trata de desarrollar los procedimientos necesarios para la recuperación de la contingencia en cuanto a los sistemas así como la recuperación del negocio una vez superada la contingencia.

Se tendrán en cuenta y deberán ser desarrollados explícitamente por cada Área los mecanismos de recuperación en caso de contingencias.

5.1. Estrategias de recuperación de los Sistemas de Información

Las estrategias de recuperación de los sistemas son propias de los proveedores de cada sistema de información y deben ser supervisadas y gestionadas por CESUS, que en el caso de los NNHH es el encargado del registro y gestión de todas las incidencias que se producen.

El INFANTA CRISTINA solamente tiene capacidad de supervisar el estado y avance de la recuperación de dichos sistemas.

Dicha supervisión corresponderá al Jefe de Informática y SSII y al Jefe de Hospital.

SISTEMAS DE INFORMACIÓN AFECTADOS

- Recuperación del Sistema SELENE (HCE)
- Recuperación del Sistema Servolab de Laboratorios
- Recuperación del OPENLINK (Mensajería HL7 entre aplicaciones)

5.2. Estrategias de recuperación según Procesos de Negocio

5.2.1 FACULTATIVOS LABORATORIO

PLAN DE RECUPERACION DEL ÁMBITO DE LABORATORIO

SISTEMA	PROBLEMAS	MEDIDAS
FACULTATIVOS	Peticiones no registradas de: - laboratorio	En el momento que funcione Selene cada médico deberá registrar para cada paciente las peticiones que haya ido generando durante el plan de contingencia

5.2.2 SERVICIO DE LABORATORIO

PLAN DE RECUPERACION DEL SERVICIO DE LABORATORIO		
PERSONAL	**PROBLEMAS**	**MEDIDAS**
LABORATORIO	Peticiones	En el momento que funcione Selene y Servolab los técnicos de laboratorio deberán verificar que el SERVOLAB se reciben vía SELENE todas las peticiones generadas durante el plan de contingencia
	Resultados	Una vez comprobado que las peticiones están creadas se deberán devolver los resultados de dichas peticiones a SELENE

6. Listado de contactos

A continuación se despliegan los contactos relevantes en caso de contingencia:

SOPORTE CESUS	333333
Jefe de Hospital	649154315
Jefe Informática y SSII	639856377
Supervisora Guardia	649150789
Guardia Facultativos Radiología	608732346
Guardia Técnicos Radiología	649153521
Guardia Técnicos Laboratorio	608732335
Guardia Facultativos Laboratorio	647323886
Guardia Banco de sangre	
Guardia Farmacia	649150588