Plan de contingencia previo al proceso de Planificación, selección e implantación de un Sistema ERP en un centro deportivo

Fecha	10/05/2020
Realizado por	Rafael Yeray de León Ruiz
Revisado por	José Luis González García

C) Copyright

Índice

1. Introducción

Este plan de contingencia es un anexo a la memoria de la Planificación, selección e implantación de un Sistema ERP en un centro deportivo, por esta razón se ha omitido información que ya estaba desarrollada en el citado documento, como es el organigrama de la empresa, la situación actual, el escenario del futuro, etc.

Por lo tanto, este documento tiene un carácter técnico general de primer uso en caso de incidencia, del que dependerán otros planes más concretos, con información focalizada en cada uno de los problemas a solucionar o mitigar.

2. Motivación

Este plan de contingencia pretende dar continuidad de negocio, garantizando que los servicios que se prestan al ciudadano estén en funcionamiento el mayor tiempo posible, incluso cuando se presenten adversidades.

Para que esto sea posible, es necesario que se evalúen cada uno de los puntos de fallo que podrían afectar al correcto funcionamiento de los sistemas, tratando de anticiparse a estas situaciones e intentando en la medida de lo posible minimizar el tiempo de respuesta de cada una de las situaciones que se podrían presentar.

3. Minimizar los riesgos

Este anexo cubre los aspectos más comunes que podrían desencadenar una contingencia, bien sea por deterioro de los materiales, por causas internas o por causas ajenas a las responsabilidades de la empresa (de terceros).

Se trata de minimizar los riesgos desde tres vertientes o puntos de actuación/respuesta: mediante la redundancia de los elementos y servicios (medidas preventivas), mediante una acción que aminore las consecuencias del fallo (medidas mitigadoras) y que, de una forma definitiva, permita solucionar el origen de la contingencia (medidas correctoras).

4. Tipos de riesgos

Son muchos los riesgos que se encuentran detrás de los procesos de negocio, más aún cuando se pretende un modelo de negocio basado en la nube. Cabe destacar que algunos riesgos debe cubrirlos el proveedor de servicios en la nube, el cual promete una disponibilidad de la solución del 99.9% anual.

4.1 Eléctrico

Se produce un fallo en el sistema eléctrico de origen desconocido: puede ser a causa de un problema planificado por la compañía eléctrica (corte general de zona) o por un problema localizado dentro de las instalaciones deportivas.

Si el corte eléctrico no ha sido planificado por el personal de la empresa, puede que se desconozca la duración de la interrupción del suministro eléctrico y, dependiendo de la duración de éste, será suficiente una medida u otra.

Como **medida preventiva** se cuenta con 3 sistemas de alimentación compatibles: el primero y el segundo están siempre en activo, uno como fuente principal de alimentación (corriente eléctrica) y el otro (SAI) como sistema de protección ante sobrecargas eléctricas y de alimentación en caso de caída eléctrica, por un corto espacio de tiempo, hasta que entre en funcionamiento el Grupo electrógeno.

- *Corriente eléctrica.*
- *Sistema de Alimentación Ininterrumpida (SAI).*
- *Grupo electrógeno.*

Riesgo	Medida	Tipo
Se ha producido un corte en el suministro eléctrico sin previo aviso.	Los equipos informáticos conectados a la SAI no se ven afectados por los cortes de suministro eléctrico durante las primeras 2 horas.	**Mitigadora**
	Los servicios básicos, incluidos los equipos informáticos, pasarán a alimentarse con el grupo electrógeno si transcurrido un minuto después de un corte no se ha recuperado el suministro eléctrico convencional.	**Mitigadora**

4.2 Equipamiento informático

El equipamiento informático no está exento de posibles averías, algunos equipos tienen que estar en funcionamiento las 24 horas de los 365 días del año. Esto produce un desgaste prematuro de sus componentes que, aunque están diseñados para su uso en estas circunstancias, se debe contar con medidas que permitan minimizar al máximo los tiempos de respuesta.

Por esta razón, como **medida preventiva,** el parque informático es homogéneo: existen varios niveles de hardware y cada nivel comparte las mismas características. Es decir,

todos los servidores están dotados de los mismos componentes, al igual que los equipos administrativos, los sistemas de accesos, etc.

De esta forma, no es necesario contar con piezas de reemplazo diferentes que cubran las necesidades de cada uno de los equipos. A medida que se consumen los componentes, se realiza un pedido al fabricante o proveedor para reponer el stock.

Riesgo	Medida	Tipo
Se ha producido un fallo de hardware en un equipo informático.	El fallo está localizado en un componente que ha dejado de funcionar, bien sea por desgaste o por otro motivo. Se sustituye la pieza estropeada por una de reemplazo del stock.	**Correctora**
	No es posible detectar qué componente está generando el mal funcionamiento del equipo, se deriva la incidencia al servicio técnico externo y, cuando vuelva reparado, formará parte del stock. Se sustituye el equipo averiado por uno exactamente igual del stock para, así, no perder información. Además, se intercambiarán los discos duros o, si el disco estuviera en mal estado, se rescatará la información de las copias de seguridad.	**Correctora**

4.3 Comunicaciones

Al apostar por una solución basada en la nube, las necesidades de fortalecer el apartado de las comunicaciones se convierten en prioritarias. Ya que, si se produjera un fallo en las comunicaciones no se tendrá acceso a toda la información de la empresa y de los clientes y, por lo tanto, no se podría ofrecer un servicio de calidad al ciudadano.

Como **medida preventiva,** se han seleccionado minuciosamente cada uno de los elementos que formarán el esquema de red, tratando de que sea lo más homogéneo posible. Igualmente, se ha tratado de hacer lo mismo con el equipamiento informático y, de esta manera, se minimizan los riesgos de comunicaciones, tanto internas como externas.

Del mismo modo, se cuenta con redundancia en las comunicaciones con tres accesos a internet diferenciados: como conexión principal siempre se utilizará la conexión mediante fibra óptica, como segundo elemento de comunicaciones externas e internas, es decir, en caso de caída del principal se utilizará una conexión de Interoperabilidad Mundial para Acceso por Microondas (Wimax) y como última alternativa, en cada uno de los centros se contará con salida a internet 4G:

- *Conexión fibra óptica.*
- *Conexión de Interoperabilidad Mundial para Acceso por Microondas (Wimax).*
- *Acceso a internet 4G.*

Riesgo	Medida	Tipo
Se ha producido un corte de comunicación.	El fallo está localizado en la red interna, uno o más equipos se han quedado incomunicados. Se revisa donde pueda estar el problema, y se procede a solventar la incidencia definitivamente o se buscará una solución temporal.	**Correctora / Mitigadora**
	La red interna funciona con normalidad, no se ha perdido comunicación con los equipos de la empresa, pero no se tiene acceso a la solución de empresa en la nube. Se verifica que todos los elementos de acceso a internet estén funcionando con normalidad, ya que el fallo podría estar localizado en los firewalls, que están balanceados, o en las 3 salidas a internet. Se sustituirá o reparará el elemento que causa la incidencia.	**Correctora**
	Se verifica que aunque hay acceso a internet, no lo hay a la solución de empresa, ni desde dentro de las instalaciones, ni desde cualquier acceso a internet. El fallo debe encontrarse del lado del proveedor del servicio en la nube, se abrirá inmediatamente un ticket de incidencia o se enviará un correo electrónico a la empresa. Si pasados unos minutos no se obtuviera respuesta, se contactará telefónicamente.	**Mitigadora**

4.4 Disponibilidad de la información y control de accesos

El tratamiento y la custodia de los datos de carácter personal de todos los usuarios y la información de la propia organización deben estar sujetos al cumplimiento de las normativas recogidas en la Ley Orgánica de Protección de Datos (LOPD) y en el Reglamento General de Protección de Datos Europeo (GPDR).

Por este motivo, se debe tener especial cuidado con el control de los accesos y el registro de los movimientos de los datos, con el objetivo de que se pueda garantizar que el tratamiento que se le da a la información cumple con los fines por los que ha sido recabada y no para cederlos a terceros o usarlos para actividades delictivas.

Como **medida preventiva,** las claves de acceso caducarán cada 30 días de manera forzosa y, además, se debe establecer un nivel alto de complejidad de las contraseñas. Paralelamente, se realizarán auditorías periódicas de los sistemas, que serán elaboradas por empresas externas especializadas en el sector, con una frecuencia de, al menos, 2 al año.

Por otro lado, no sólo se debe garantizar que la información que están en producción esté protegida, sino que también hay que anticiparse a una posible pérdida de información, ya sea por un fallo técnico o por un borrado de datos, que podría ser intencionado o involuntario.

Para evitar la indisponibilidad de la información y cumplir con la Ley General Tributaria, la cual establece que las organizaciones tienen la obligación de conservar las facturas y los documentos generados durante un plazo de 4 años, se establecerá un robusto plan de copias de seguridad y de recuperación de los datos frente a contingencias.

Este plan de copias de seguridad cumplirá con la regla 3-2-1, es decir, se contará desde el principio al menos 3 sistemas de copias en, por lo menos, 2 soportes diferentes y, al menos, 1 fuera de la sede, en concreto, en un proveedor de servicios en la nube.

Riesgo	Medida	Tipo
Ha existido indisponibilidad de la información, debido a un fallo en los sistemas, o por parte de los usuarios.	Se ha detectado que hay inconsistencia en la información almacenada en los sistemas, se desconoce el origen de esta incidencia. En primer lugar, se debe detectar si ha sido un fallo de los propios sistemas, para tratar de solucionar inmediatamente la causa. Si el problema ha sido causado por parte de algún usuario, se deberá investigar si ha sido un accidente o si ha sido de forma intencionada, para tomar medidas en caso de que haya sido voluntario. Por último, una vez establecidas las causas, para tratar de que no se repita, se realizara una recuperación completa de los datos almacenados en la copia de seguridad más reciente.	**Correctora**
Se ha producido un fallo en el control de los accesos.	Se ha registrado en los sistemas un acceso no autorizado a parte de la información de la empresa. Esta información podría contener datos de carácter sensible, según la tipificación de la ley de protección de datos de carácter personal. Automáticamente, se deben revisar los rastros que ha dejado ese acceso en los logs, para proceder a notificar a la Agencia de Protección de Datos de la situación ocurrida e, inmediatamente, se deben cambiar las claves de acceso de todos los usuarios que se hayan visto implicados en esta incidencia.	**Mitigadora**

4.5 Funcionales y de planificación

A priori, parece que los posibles fallos identificados hasta el momento son los más importantes, pero existen otro tipo de riesgos asociados a un proceso de transformación que podrían generar muchos problemas a la organización si no cuenta con un plan de contingencia que permita abordar estas situaciones de una forma tranquila y sosegada.

Riesgo	Medida	Tipo
Gestión de las resistencias al cambio (órganos directivos y empleados)	No todas las personas entenderán por qué se ha realizado este proceso de transformación, pueden ser múltiple los factores que provoquen la resistencia al cambio. En primer lugar, se ha de conocer que origina el rechazo al cambio, para tratar de transmitir seguridad y tranquilidad a los empleados, explicándoles que esta situación es igual de beneficiosa para todos, no peligran los puestos de trabajo y las condiciones laborales nunca irán a peor, sino a mejor.	**Correctora**
No se ha realizado una correcta verificación y puesta en común de la toma de decisiones	Algunas decisiones se han tomado de forma unilateral, privando al resto de personas implicadas en el proceso del poder de la información, desconociendo éstas, cómo se están llevando a cabo todas las medidas puestas en marcha. Se deberá tomar medidas en el caso de que se intente ocultar información al resto de personas implicadas en el proceso, ya que, todos los procesos deben ser resueltos siempre que se pueda de forma colaborativa y se primará el aprovechamiento de la inteligencia colectiva.	**Correctora**
Verificación del cumplimiento de los objetivos	Al verificar el cumplimiento de los objetivos se detecta que no se han alcanzado los que se han fijado en el estudio de viabilidad de la solución. Dependiendo del porcentaje de cumplimiento de los objetivos, se deberán tomar medidas para tratar de encauzar la situación si está ha sido desfavorable, ya que, es previsible que exista una pequeña variación en los objetivos y, que a largo plazo, cuando los usuarios terminen de adaptarse o se añadan nuevos módulos, los resultados sean mejores.	**Correctora**

5. Seguimiento y actuaciones

Todas las actuaciones, que se realicen en base a las contingencias que se vayan presentando, deberán quedar correctamente grabadas en este documento o se deberán generar nuevos documentos, los cuales quedarán correctamente referenciados en la siguiente tabla, con el objetivo de que se vaya dotando de más información/valor la base de conocimiento de la empresa.

Nº Inc.	Origen	Descripción	Técnico	Fecha

6. Bibliografía

- INCIBE. «Plan de Contingencia y Continuidad de Negocio», 27 de enero de 2016. Accedido 10 de mayo de 2020. https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-contingencia-continuidad-negocio.
- «Cuánto tiempo se deben conservar los documentos de una empresa| DCD». Accedido 10 de mayo de 2020. https://www.dcd.es/conservar-documentos-empresa/.